

Entrust Entelligence™

Security Provider 9.3 for Windows®

Administration Guide

Document issue: 2.0

Date of Issue: August 2015



Copyright © 2001-2015 Entrust. All rights reserved.

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

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

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

About this guide17

Revision information	18
Introduction	19
Audience	19
Typographic conventions	19
Note and Attention text	20
Obtaining technical assistance	21
Technical support	21
E-mail address	21
Professional Services	21
Obtaining documentation	23
Documentation feedback	23
Related documentation	24
Security Provider for Windows documentation	24
Security Manager documentation	24
Other related Entrust product documentation	24
Microsoft Windows documentation	24

CHAPTER 1

About Entrust Entelligence Security Provider for Windows25

Security Provider features	26
Security Provider system architecture	31
Entrust Authority Security Manager	32
Directory	32
Other Entrust products	33

CHAPTER 2

About the Microsoft Windows security architecture35

Overview	36
Microsoft CryptoAPI	37
Cryptographic Service Providers (CSPs)	38
Listing the installed CSPs	38
Certificate stores	39
Security stores	40
Revocation providers	40
Applications	42
Microsoft Encrypting File System	42
Microsoft Data Recovery Agent	42
Windows Explorer	42
Microsoft Outlook	43
Internet Information Server (IIS) and Cisco® VPN Client	43

CHAPTER 3

About digital IDs45

Digital ID overview	46
Digital ID categories—Entrust and non-Entrust	47
Digital ID storage locations	48
CSPs that store digital IDs	50
Entrust security store	52
Entrust security store types, location, and contents	52
Logging in to an Entrust security store and authenticating	52
Logging in by right-clicking the taskbar icon	53
Logging in by attempting to perform a secure operation	53
Authenticating by attempting to use a nonrepudiation key	53
Logging out of an Entrust security store	54
Entrust security store certificate processing	54
Entrust security store validation	55
Taskbar status icon	55
Why would I choose not to install the taskbar status icon?	56
Enhanced logout support	57
Configuring Entrust security store settings	57

Third-party security store and mixed digital IDs	58
Third-party security store types, location, and contents	58
Logging in to a third-party security store and authenticating	58
Logging in by attempting to perform a secure operation	58
Authenticating by attempting to use a nonrepudiation key	59
Mixed digital ID	59
Exchanging certificates using email	60
How the certificate exchange works	60
How to send a certificate to another user	61
How to import an encryption certificate	61
Removing and certificates from the Other People certificate store on logout	62

CHAPTER 4

Entrust digital ID features 63

Entrust digital ID enrollment and recovery	64
Enrollment and recovery methods	64
Silent enrollment or recovery	65
Enrollment details with Security Manager	66
Key pair support with Security Manager	66
Enrollment and recovery details with Security Manager 8.x	66
Reasons for recovery	67
How recovery is initiated	68
Manual enrollment and recovery for users	69
Manual enrollment and recovery for computer digital IDs	73
Manual enrollment and recovery for Windows Services	76
Configuring the recovery of archived key pairs	80
Entrust digital ID management	82
What is managed?	82
When management occurs	83
When management does not occur	84
Are key histories maintained?	85
How the user experiences key management	85
Updating a digital ID for a user	85

Updating a digital ID silently if Security Provider's Digital ID Monitor detects that an update is required	86
Updating a Digital ID for computer	86
Updating a Digital ID for Windows service.	87
Other sources of information	87
Additional Entrust digital ID management for smart cards	88
How the Key Access Service works	88
KAS application	89
KAS Certificate Store Provider	89
KAS Cryptographic Service Provider.	89
Internal cache	89
Update and recovery processes	90
Setting the Max key count attribute	90
Calculating maximum keys	91
Communicating with the Certification Authority (CA)	92
Policy certificates for Security Manager	92
V2-key-pair certificate types	94
Relationship between certificate types, certificate definitions, and certificate definition policy	94
Configuring supported key pairs	95
1-key-pair user	96
2-key-pair user	96
EFS User	97
Standalone EFS User	97
Nonrepudiation user	98
Nonrepudiation and EFS User	98
Smart card logon user	98
Selecting supported Security Manager key pairs	98
Automatic additional certificate download	100
How Security Manager's certificates are downloaded	100
Where CA certificates are stored	100
When CA certificates are downloaded	100
Entrust Desktop Solutions migration	101
What is migrated?	101
Address book (PAB)	101

Recipient lists (ERLs)	102
Disabling automatic migration	103
Migrating smart cards from EDS to Security Provider	103
Using smart cards on EDS after migration	104
Importing and exporting the Entrust key file	105
Importing certificates from an Entrust key file	105
Exporting a certificate to an Entrust key file	105
Configuring an enrollment station	106
Entrust Enhanced Cryptographic Provider	106
Smart card vendor Cryptographic Service Provider (CSP).	106
Adding and using the Entrust computer digital ID snap-in	107
Computer Digital ID snap-in functionality	107
Adding the Entrust Digital ID	107
Viewing and managing computer digital IDs	111
Viewing event logs for computer digital IDs	112
Adding and using the Entrust Windows services digital ID snap-in	114
Windows service Digital ID snap-in functionality	114
Adding the Digital ID snap-in	114
Viewing and managing Windows service digital IDs	118
Viewing event logs for Windows service digital IDs	120

CHAPTER 5

CryptoAPI enhancements 123

Importing keys into an Entrust security store	124
About the import process	124
Enabling the import	126
Preconfiguration step	126
Entrust Cryptographic Service Providers	129
Entrust Enhanced Cryptographic Service Provider	129
Entrust Symmetric Cryptographic Service Provider	130
Entrust Key Access Service Cryptographic Service Provider	131
Entrust Elliptic Curve Cryptographic Service Provider	132
Entrust Smart Card Cryptographic Provider	133
Key Storage Providers	134
Entrust Smart Card Key Storage Provider.	134

Entrust Enhanced Key Storage Provider	134
CRL Revocation Provider	136
Supported CRL revocation functionality	136
How CRLs are checked	137
OCSP Revocation Provider	139
OCSP revocation functionality	139
How OCSP Revocation Provider checks certificates	139
Certificate path discovery, validation, and extension checking	141
Path discovery and validation overview	141
About the Certificate Path Discovery feature	142
About the Certificate Path Validation feature	143
About the Certificate Path Critical Extension Policy Provider	143
Customizing certificate path discovery	144
Customizing certificate path validation	145
Customizing the Certificate Path Critical Extension Policy Provider	146

CHAPTER 6

Integrating with other products147

Creating digital IDs in Administration Services	148
Using the Auto-enrollment Service (Administration Services)	149
Enabling auto-enrollment	149
Auto-enrollment for an Entrust digital ID for a user	150
How the user auto-enrollment is initiated	150
Auto-enrollment for an Entrust computer digital ID	151
How the computer auto-enrollment is initiated	152
Auto-recovery	153
How the auto-recovery is initiated	153
Customizing the certificate type and role	154
Responses to auto-enrollment and recovery requests	155
Enrollment and recovery queues for administrator approval	155
Queued responses	155
Silent auto-enrollment and recovery	156
Nonsilent user auto-enrollment and recovery	157
Approved Entrust computer digital ID auto-enrollment and recovery requests	157

Rejected auto-enrollment and recovery response.	158
Resending auto-enrollment requests	158
Why Security Provider for Windows might reject SSL certificates from Microsoft IIS	159
Using an SSL certificate with the Auto-enrollment Service	160
Enabling SSL on Active Directory	160
Creating and updating an SSL Web server certificate	161
Creating an SSL Web server certificate	161
Exporting your Entrust computer digital ID to Microsoft IIS . . .	165
Updating the SSL Web server certificate	167
Using the Roaming Server	170
Enabling roaming users	170
Switching between a roaming and desktop user	171
Configuring roaming certificate settings	172
Allowing users with mixed digital IDs to roam	172
How roaming works with mixed digital IDs	172
Enabling users with mixed digital IDs to roam	172
Working offline as a roaming user	174
Roaming Server problems	175
Support for Entrust Enhanced CSP users only	175
Signing certificate is mandatory.	175
Choosing an algorithm for digital signature	175
Using Entrust TruePass	176
Using an application proxy server	177
How the application proxy server connection works	177
Application proxy server authentication	177
Using Security Manager Proxy	178
Using smart cards	180
Enrolling with a smart card	180
Recovering with a smart card	181
Recovering a credential using the Recover Entrust Digital ID wizard	
181	
Logging in with a smart card	182
Updates with a smart card	182
Configuring the smart card CSP	182

Security Manager 8.x or higher	183
Generating keys within the smart card CSP	183
Configuring Windows Smart Card Logon	185
Moving an Entrust digital ID onto a smart card	185
Using smart cards with Security Provider and EDS	185
Troubleshooting smart card problems	186
Smart card CSP	186
Key or certificate updates fail	187
Smart card only users	187
Smart cards and the nonrepudiation private key	187
Smart cards and Microsoft roaming support	187
Using a Card Management System	188
Functionality not available with a CardMS	188
Integrating Security Provider and a CardMS	189
Using PIV smart cards with Entrust IdentityGuard	191
Managing an Entrust PIV Card	192
Updating a PIV smart card credential	192
Resolving a blocked Entrust smart card	193
Changing a PIN	194
Using the PIV smart card	196
Using Security Provider for Windows with non-Entrust PIV smart card management software	197
Using Microsoft Application Virtualization (App-V)	199

CHAPTER 7

Bundled applications201

File Security application	202
File security functionality, in detail	203
Enabling the File Security application	205
Preconfiguration step	205
Enabling and customizing the File Security application	208
Using the File Security application	210

Password Encrypt application	221
Why use Password Encrypt?	222
Password Encrypt functionality	222
Customizing Password Encrypt	223
Using the Password Encrypt application	224
TrueDelete application	230
Why use TrueDelete?	230
TrueDelete functionality	230
When TrueDelete is not triggered	231
About overwriting methods	231
Customizing TrueDelete	232
Certificate Explorer application	234
Certificate Explorer functionality	235
Customizing the Certificate Explorer	235
Using the Certificate Explorer search functions	236
Viewing archived or expired certificates	238
Grouping certificates in a list	239
Checking the revocation status of a certificate	240
Setting up advanced user and debug modes	242
What is displayed in Advanced mode	243
What is displayed in Debug mode	244
Viewing policy certificates	245
Customer support utility	248
Creating a dump ZIP file	248
Clearing the cache	249

CHAPTER 8

Using Security Manager Administration 251

Configuring user policy	252
Client policy settings	252
Managing login attempts	252
Enabling a suspended security store	253
Logging security store suspensions	254
Configuring password expiry times	254
Setting roaming permission	254

Setting desktop permissions	255
Algorithm for digital signature	255
Configuring the inactivity timeout	255
Auto-associating certificates in Microsoft Outlook	255
Managing key export.	256
Unprotected CAPI key storage.	256
Algorithm for profile protection	257
Security considerations	258
Certificate definition policy settings	259
Policy settings for certificate definitions	259
CSP to manage keys	259
Enable cert update date	261
Cert update date	261
Update cert at percentage of lifetime.	261
Only latest key can sign CMP	262
Key can sign CMP	262
Algorithm for key pair	262
Back up private key	263
Generate key at client	263
Key usage policy	263
Protect key storage for CSP	264
Private key export from CSP	264
Max key count.	264
CSP to export to	264
Configuring the certificate definition policy settings	265
Keys and certificates with no certificate definition policy	265
Configuring an Entrust computer or Windows service digital ID	267
Registering users or computers	268
End user, computer, or Windows Service activation	271
Using other Security Manager features	273
Updating Entrust digital IDs	273
Certificate types that have certificate definition policy	273
Certificate types that do not have certificate definition policy	274
Obsoleting certificate types	274
Moving users from one Entrust Security Manager CA to another	275

Details for Security Manager	276
Changing distinguished names	276
Deactivating users	277
Moving an Entrust digital ID from one security store to another . . .	277

CHAPTER 9

Deploying Security Provider for Windows 281

Deployment worksheet	282
Customizing the installation	285
Selecting application features	285
Adding and removing features	286
Learning what the features do	287
About configuring multiple searchbases.	289
Working with Entrust IdentityGuard	290
Customizing the installation using the wizard	290
Customizing the installation using the wizard and Group Policy . . .	295
Packaging the installation	297
Creating a standard package	298
Creating an administrative package	299
Testing the installation	303
Distributing the installation package	304
Installing Security Provider	305
Upgrading Security Provider	306
Deploying service packs and patches	308
Deploying language packs	310

CHAPTER 10

Troubleshooting 313

Security Provider for Windows logs	314
Setting the logging settings	314
Viewing the log file	315
Setting the log viewing options	315
Security Provider for Windows log file location	315
Windows installer logging	316
Error messages	316
Collecting information for customer support	317
Policy certificate messages	318
Certificate management dump files	318
Enrollment and recovery policy	318
Reading policy certificate dump files	318
Setting the policy certificate dump location	319
Auto-enrollment, CardMS, and OCSP message dump files	319
PKIX-CMP messages	320
Key update dump files	321
Enrollment and recovery dump files	321
Reading PKIX-CMP dump files	321
Setting the PKIX-CMP dump location	321
Configuring hardened desktop environments	322
Security considerations	323
Securing your environment	323
Securing your password	323
Evaluating your cryptographic security	323
Displaying version information	324

APPENDIX A

Security Provider registry settings.....327

What is the ESP registry location?	329
Directory settings	331
Directory connection settings	332
Directory search settings	340
Default directory setting	344

PKI settings	347
General CA settings	348
CA-specific directory setting	352
Roaming Server settings	354
Proxy server settings	357
Auto-enrollment settings	361
CA-specific OCSP Responder settings	367
CardMS settings	368
Entrust IdentityGuard settings	370
Entrust digital ID settings	373
Entrust digital ID for users options settings	373
Entrust Entelligence Windows Service Digital ID settings	389
Entrust computer digital ID settings	392
Entrust security store settings	396
Entrust security store login settings	396
Entrust security store creation settings	405
Entrust security store startup and shutdown settings	416
CRL Revocation Provider settings	419
OCSP Revocation Provider settings	425
Entrust File Security settings	430
Timestamp server settings	445
Password Encrypt settings	451
TrueDelete settings	455
Entrust Certificate Explorer settings	463
Entrust Ready identity device setting	469
Certificate path discovery, validation, download, and extensions settings	470
HTTP connection and timeout settings	476
GUI customization settings	478
Miscellaneous settings	484
Logging settings	489
Entrust email certificate exchange settings	495

APPENDIX B

Entrust digital ID and security store versions and contents.	499
---	------------

How Security Provider upgrades V1 digital IDs and V3 Entrust security stores	500
Glossary501
Index.507

About this guide

This document describes the architecture of Entrust Entelligence™ Security Provider for Windows®, and provides detailed information for administrators to plan, deploy, administer, and troubleshoot Security Provider for Windows for end users.

This chapter contains the following topics:

- [“Revision information” on page 18](#)
- [“Introduction” on page 19](#)
- [“Obtaining technical assistance” on page 21](#)
- [“Obtaining documentation” on page 23](#)
- [“Related documentation” on page 24](#)

Revision information

Table 1: Revisions in this document

Document issue and date	Section	Description
Issue 2.0 August 2015	"File Security application" on page 202	Added a note. A colon in the file name is treated as an illegal character by the File Security Application.
Issue 1.0 August 2015		First release for 9.3.

Introduction

This section describes the intended audience of this document, the typographic conventions used throughout, and explains the note and attention text used throughout this guide.

Audience

The intended audience of this document is administrators who will be deploying and administering Security Provider for Windows.

To use the information in this Guide, you should have a basic understanding of the following:

- cryptography and key management in a PKI
- Microsoft® Windows® security framework
- Microsoft® Windows® Installer

The terms end user and user are used interchangeably throughout this document, and refer to the users of the Security Provider for Windows software.

Typographic conventions

This document uses various typographic conventions to identify objects and syntactic elements. These conventions are used to help you quickly and easily identify particular objects, processes, and names that are used frequently throughout the documentation.

Table 2: Typographic conventions

Convention	Purpose	Example
Bold text (other than headings)	Indicates graphical user interface elements and wizards.	Click Next .
<i>Italicized</i> text	Denotes book or document titles.	For further information on Windows Installer, see the document entitled <i>Windows Installer: Benefits and Implementation for System Administrators</i> .
Blue text	Indicates hyperlinks to other sections in the document when viewed online.	A user is defined as an entity that is identified and approved by a Certification Authority (CA) .
<u>Underlined blue</u> text	Used for Web links	For more information, visit our Web site at www.entrust.com .

Table 2: Typographic conventions

Convention	Purpose	Example
Courier type	Indicates installation paths, file names, Windows registry keys, commands, and text you must enter.	The <code>eespwin32.msi</code> file will be copied to the selected location, in addition to the Security Provider for Windows application files.
Angle brackets using Courier type <code>< ></code>	Indicates variables (text you must replace with your organization's correct values).	Navigate to <code><install_path>\Tools\dvt</code> .
Square brackets using Courier type <code>[]</code>	Indicates optional parameters.	<code>dsa passwd [-ldap]</code>

Note and Attention text

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

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

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

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 Entrust technical support services, visit our Web site at:

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

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

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

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

If you contact Entrust 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, Entrust Professional Services will design and implement the right solution for your organization's needs. For more information about Entrust Professional Services please visit our Web site at:

<http://www.entrust.com>

Obtaining documentation

Entrust product documentation, white papers, technical integration guides, 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://secure.entrust.com/trustedcare>

Documentation feedback

You can rate and provide feedback about Entrust 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 Entrust's PDF documents (see bottom of this page)
- following this link: <http://go.entrust.com/documentation-feedback>

Feedback concerning documentation can also be directed to the Customer Support email address.

support@entrust.com

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.

Security Provider for Windows documentation

- *Entrust Entelligence™ Security Provider for Windows Error Message Guide*
- *Entrust Entelligence™ Security Provider for Windows Release Notes*
- White papers and integration guides for Security Provider for Windows can be viewed on the Entrust TrustedCare Web site at:
<https://www.entrust.com/trustedcare>

Security Manager documentation

- *Entrust Authority™ Security Manager Administration User Guide*
- *Entrust Authority™ Security Manager Operations Guide*

Other related Entrust product documentation

- *Entrust Entelligence™ Security Provider for Outlook Administration Guide*
- *Entrust Authority™ Administration Services Administration Guide*
- *Entrust Authority™ Roaming Server Administration Guide*
- *Entrust Authority™ Security Manager Proxy Administration Guide*

Microsoft Windows documentation

- *Windows Installer: Benefits and Implementation for System Administrators*, white paper published November 2001 by Microsoft Corporation and available from www.microsoft.com
- Additional information about Microsoft® Windows tools and services see the [MSDN Library](#)

About Entrust Entelligence Security Provider for Windows

Entrust Entelligence™ Security Provider for Windows is a lightweight Microsoft® CryptoAPI based application that has three primary functions:

- to deliver managed keys and certificates
- to provide enhanced security features to CryptoAPI applications
- to allow end users to sign, verify, encrypt, and decrypt files on their file system

Security Provider functionality is made available through a set of components that you can enable or disable based on your organization's requirements. It supports flexible enrollment, automatic certificate management, strong key protection, advanced certificate revocation checking, and enhanced security features for a wide range of CryptoAPI applications.

For an overview of Security Provider, see the following sections:

- [“Security Provider features” on page 26](#)
- [“Security Provider system architecture” on page 31](#)

Security Provider features

Table 3 provides an overview of Security Provider's main features. These features are divided into the following categories:

- **Entrust digital ID features**
Entrust digital ID features require an Entrust Certification Authority (CA), namely, Entrust Authority Security Manager.
- **CryptoAPI enhancements**
CryptoAPI features are used internally by Security Provider, but can also be integrated with third-party CryptoAPI applications. They deliver enhanced security features to CryptoAPI applications, and do not require an Entrust CA.
- **Bundled applications**
Bundled applications are included with Security Provider and may require a directory, but do not require an Entrust CA.
- **Other features**
Other features include the leveraging of Windows Installer technology, the integration with Microsoft Group Policy, and the meeting of accessibility standards.

Table 3: Security Provider features

Feature	Description
Entrust digital ID features (Require an Entrust CA.)	
Management of Entrust digital IDs	<p>Security Provider can enroll, recover, update, and continually monitor the keys and certificates in an Entrust digital ID. For details, see:</p> <ul style="list-style-type: none"> • “Digital ID overview” on page 46 • “Entrust digital ID enrollment and recovery” on page 64 • “Entrust digital ID management” on page 82
Automatic additional certificate download	<p>Security Provider can discover Entrust CA certificates, including cross and link certificates, and download them to the user's CA certificate store. Security Provider uses the Entrust CA entry in the user's registry as the starting point from which to discover CA certificates. See “Automatic additional certificate download” on page 100 for details.</p>
Deployment with other Entrust products	<p>You can deploy Security Provider with the following Entrust products to deliver extra features:</p> <ul style="list-style-type: none"> • Security Manager Proxy Server enables the use of Security Provider outside your firewall. • Entrust Authority Roaming Server enables users to access their Entrust security stores from multiple computers. • Entrust TruePass forces users to log in with their Entrust digital IDs to access your Web resources. • Entrust Authority Administration Services enables digital ID enrollment, recovery, and management through the Web. <p>See “Integrating with other products” on page 147 for details.</p>
Integration with a card management system	<p>Security Provider can check for digital ID updates and let a card management system perform the update. See “Using a Card Management System” on page 188 for more information.</p>
Retrieval of past smart card key history	<p>Security Provider can retrieve the encryption key history of a smart card from Security Manager. This gives smart cards access to their full history without needing to store all that data on the smart card itself. See “Additional Entrust digital ID management for smart cards” on page 88.</p>
Automated certificate exchange using email	<p>Security Provider allows users to exchange certificates with other email users by simply clicking a link and following the instructions in a wizard. Security features such as password protection can be incorporated into the exchange.</p>

Table 3: Security Provider features (continued)

Feature	Description
CryptoAPI enhancements. (Can be integrated with other CryptoAPI applications)	
Certificate path discovery, validation, and extension checking	<p>The Certificate path discovery, validation, and extension checking features improve CryptoAPI's native certificate path discovery and validation capabilities:</p> <ul style="list-style-type: none">• The certificate path discovery feature lets CryptoAPI applications find intermediate CA certificates, and cross and link certificates in a directory.• The certificate path validation feature allows CryptoAPI applications to perform improved validation checks on certificate paths.• The certificate extension checking feature allows CryptoAPI applications to check critical certificate extensions when validating certificate paths. <p>See “Certificate path discovery, validation, and extension checking” on page 141 for details.</p>
CRL Revocation Provider	<p>This feature extends CryptoAPIs native Certificate Revocation List (CRL) checking capabilities to support Entrust partitioned CRLs. See “CRL Revocation Provider” on page 136 for details.</p>
OCSP Revocation Provider	<p>This feature provides OCSP checking capabilities to any CryptoAPI-based application. OCSP Revocation Provider communicates with an OCSP server to obtain the most current certificate status. See “OCSP Revocation Provider” on page 139 for details.</p>
CSPs that provide enhanced cryptography	<p>Security Provider includes Cryptographic Service Providers (CSPs) that CryptoAPI applications can use:</p> <ul style="list-style-type: none">• Entrust Enhanced CSP:<ul style="list-style-type: none">- provides a set of asymmetric, symmetric, and hashing algorithms not supported by the default CSPs available with Windows- stores keys and certificates from any CryptoAPI application in an Entrust security store (.epf file)• Entrust Symmetric CSP provides a set of symmetric algorithms not supported by the default CSPs available with Windows.• Entrust Key Access Service CSP lets CryptoAPI applications access a user's old private keys that no longer exist on their smart card due to smart card storage limitations.• Entrust Elliptic Curve CSP provides support for elliptic curve cryptographic (ECC) algorithms. <p>For details, see “Entrust Cryptographic Service Providers” on page 129.</p>

Table 3: Security Provider features (continued)

Feature	Description
Importing to an Entrust security store	This feature allows third-party CryptoAPI applications to import non-Entrust keys and certificates into an Entrust security store (.epf file). See “Importing keys into an Entrust security store” on page 124 .
Bundled applications (Applications within Security Provider. May require a directory.)	
File Security	The File Security application is a Windows application that lets users encrypt, decrypt, sign, verify, and timestamp files on their computers. They can also view the security properties of protected files, such as the digital signature. The application has GUI and command line variants. For details, see “File Security application” on page 202 .
Password Encrypt	The Password Encrypt application is a Windows application that lets users protect a file or files with a password. The password is required to open the file. For details, see “Password Encrypt application” on page 221 .
TrueDelete	The TrueDelete application is a Windows application that lets users remove files from their computers or file servers in a more secure manner than clicking the Delete button. For details, see “TrueDelete application” on page 230 .
Certificate Explorer	The Entrust Certificate Explorer is a Windows application similar to the certificate viewer in Internet Explorer, but with extra functionality. It allows users to view and manage certificates on their computers and create, import, and export Personal Encryption Groups. For details, see “Certificate Explorer application” on page 234 .
Customer support utility	The customer support utility is a command-line tool that you can use when you encounter problems with Security Provider. The tool collects system data and compiles it into a ZIP file which can then be sent to Entrust customer support to help with troubleshooting. For details, see “Customer support utility” on page 248 .
Other features	
Uses the Microsoft Windows installer technology	Security Provider is made available as a Microsoft Windows installer package (.msi file). You can customize this package using a wizard and then make the package available to end users. You may also choose to partially customize the installation package and then push out the remaining configuration information through a Microsoft Group Policy application. See “Customizing the installation” on page 285 for details.
Microsoft Group Policy	You may push out Security Provider configuration information through a Microsoft Group Policy application.

Table 3: Security Provider features (continued)

Feature	Description
Accessibility	Security Provider meets the relevant accessibility standards of Section 508 of the U.S. Disabilities Act.
Certificates from CAs with known problems certificates can be identified and, optionally, removed.	<p>Security Provider has the concept of a known problem certification authority (CA) certificate. A known problem CA certificate may cause certificate chain development issues or some other issue within your environment. Once a CA certificate has been configured as a known problem, Security Provider will skip it when importing certificates to the Intermediate Certification Authorities and Trust Root Certification Authorities certificate stores.</p> <p>Security Provider can also be configured to remove known problem CA certificates from these stores when doing normal management operations.</p> <p>See page 488 for details about these registry settings.</p>

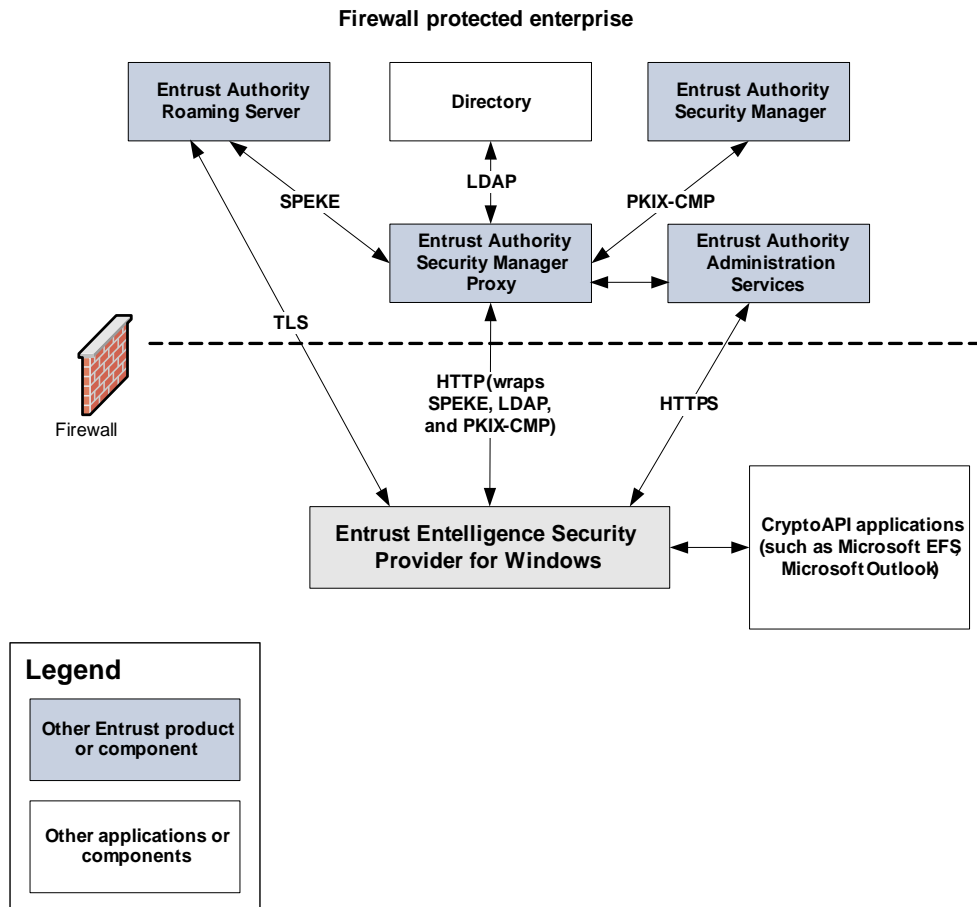
Security Provider system architecture

Figure 1 shows how Security Provider might be deployed in an extended enterprise environment. Details on each component follow the figure.

- If you want to deploy Entrust digital ID features, your architecture must include Security Provider, Security Manager, and a directory, at a minimum.
- If you want to deploy CryptoAPI enhancements, your architecture must include Security Provider, at a minimum.
- If you want to deploy Security Provider's bundled applications, your architecture must include Security Provider and a directory, at a minimum.

For an overview of features, see [“Security Provider features” on page 26](#).

Figure 1: Security Provider for Windows extended enterprise environment architecture



Entrust Authority Security Manager

Security Manager is a Certification Authority (CA) and is an optional component in your deployment. The main functions of Security Manager are to:

- create certificates for any public keys
- create encryption key pairs for users
- provide a managed, secure database of Entrust Authority information containing:
 - the CA signing key pair (this key pair may be created and stored on a separate hardware device rather than the database)
 - user status information
 - the encryption key pair history (including all decryption private keys and encryption public key certificates) for each user
 - the verification public key history (including all verification public key certificates) for each user
 - the validity periods for signing key pairs, encryption key pairs, and system cross-certificates
 - Security Officer and Administrator information
 - CA policy information
 - revocation information
- enforce the security policies defined by your organization
- publish Certificate Revocation Lists (CRLs)
- publish Policy Certificates

Access to Security Manager is provided through:

- Entrust Authority Security Manager Control
- Entrust Authority Security Manager Administration

Directory

The directory is an LDAP-compliant directory service (for example, X.500 directory or a Microsoft Active Directory) where Security Manager or another CA publishes the following publicly-available information:

- user and computer certificates
- lists of revoked certificates (CRLs)
- client policy information

The directory is the most frequently accessed component by client software.

Other Entrust products

You can enhance your Security Provider deployment with additional Entrust products described in Table 4.

Table 4: Entrust Products

Entrust Product	Description
Roaming Server	Roaming Server permits users to store their Entrust digital IDs in a centralized directory so that it can be accessed from any computer at any time to perform encryption and other cryptographic operations. See “Using the Roaming Server” on page 170 for further information.
Security Manager Proxy	Security Manager Proxy is a service that allows Security Provider to communicate with the Security Manager and back-end servers over the Internet. It does not require major changes to existing firewall settings. Security Manager Proxy makes this possible by encapsulating data packets with HTTP so that they can tunnel through firewalls. See “Using Security Manager Proxy” on page 178 for further information.
Auto-enrollment Service	Entrust Authority Administration Services Auto-enrollment Service is one of the Entrust products you can use to transparently register and administer users or computers in Security Manager. Using the Auto-enrollment Service, automatic enrollment and recovery of keys and certificates can be performed for end users or computers. See “Using the Auto-enrollment Service (Administration Services)” on page 149 for further information.
Entrust TruePass	Entrust TruePass is a Web application that can use the Entrust digital IDs created with Security Provider for Web-based authentication, digital signatures, and encryption operations. See “Using Entrust TruePass” on page 176 .
Administration Services	Administration Services is one of the Entrust products you can use to register and administer users in Security Manager. It enables the delivery of managed certificates to users for use with a wide range of enterprise applications, such as file and folder protection, email, e-forms, wireless local area network (WLAN), and virtual private network (VPN) security. See “Creating digital IDs in Administration Services” .

About the Microsoft Windows security architecture

This section provides an overview of the Microsoft Windows security architecture in order for you to understand how Security Provider for Windows integrates with Microsoft Windows native security capabilities.

The Windows security architecture is made up of several major components, described in further detail in the following sections:

- [“Overview” on page 36](#)
- [“Applications” on page 42](#)

Overview

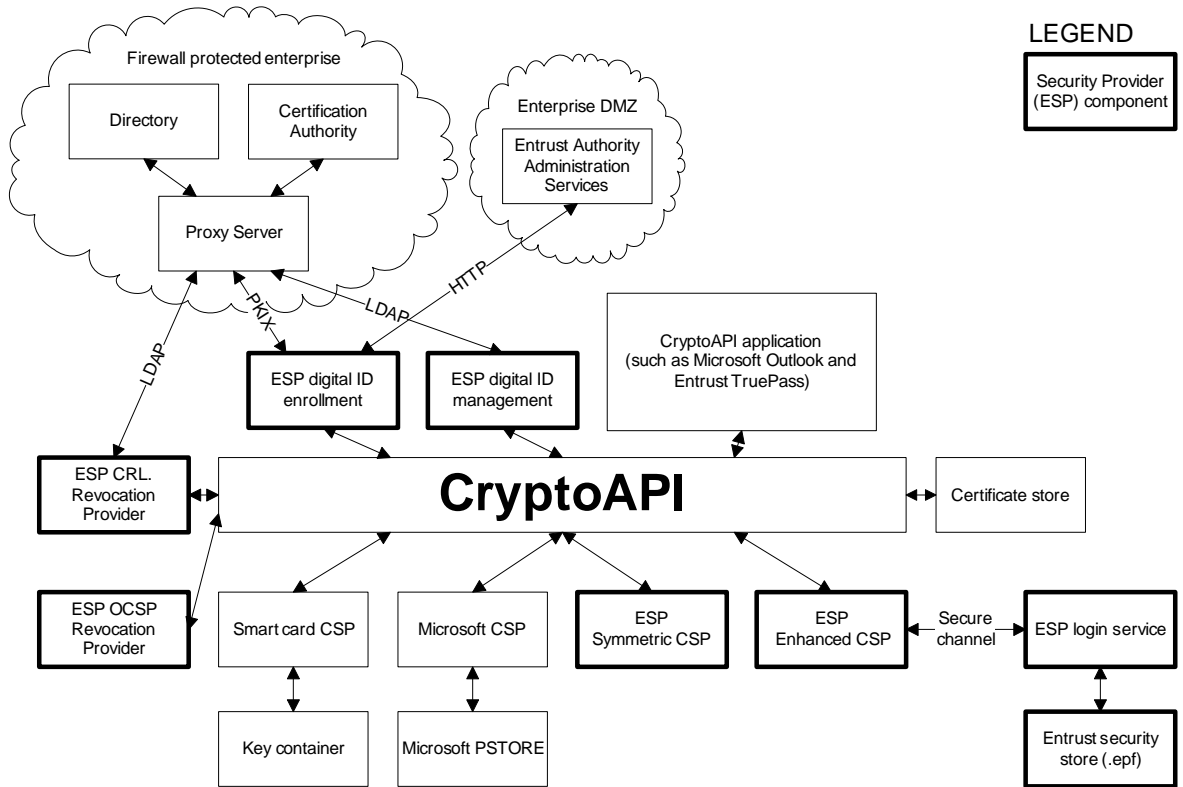
The principal role of Security Provider for Windows is to deliver managed Entrust keys and certificates to the Microsoft Windows security architecture. These Entrust keys and certificates can be used with software applications that are built to take advantage of Microsoft Windows digital signature, authentication, and encryption capabilities.

The principal components of the Microsoft Windows security architecture are described in this chapter.

- ["Microsoft CryptoAPI" on page 37](#)
- ["Cryptographic Service Providers \(CSPs\)" on page 38](#)
- ["Certificate stores" on page 39](#)
- ["Security stores" on page 40](#)
- ["Revocation providers" on page 40](#)

The following figure provides an overview of how all components fit together.

Figure 2: Microsoft Windows security architecture overview



Microsoft CryptoAPI

Microsoft Cryptography Application Program Interface, known as Microsoft CryptoAPI, is a Windows API that provides security capabilities to the operating system. CryptoAPI allows any application to take advantage of cryptographic functionality built in by Microsoft. CryptoAPI is based on standards, such as X.509, PKCS, CMS, and supports a wide range of cryptographic algorithms.

When an application requires an encryption operation, it sends the request through CryptoAPI. CryptoAPI does not actually perform the operation, it passes the request to a **CSP**. CryptoAPI also acts as an interface for the **certificate stores**. When a certificate is required, CryptoAPI sends a query to the appropriate certificate store to return a list of available certificates.

Cryptographic Service Providers (CSPs)

CSPs plug in to CryptoAPI and perform all cryptographic operations, such as encrypting and decrypting data, verifying signatures, and signing data. When an application requires a cryptographic operation, CryptoAPI routes the request to the applicable CSP.

CSPs also act as an interface with the private security store, where users' private keys are securely held. The private security store is stored locally or on a device such as a smart card.

Microsoft provides a number of CSPs with its operating systems. For example, Microsoft Base Cryptographic Service Provider is a general purpose provider that supports digital signatures and data encryption, and uses RSA public-key algorithms for all public key operations. Other Microsoft CSPs support the same capabilities as the Microsoft Base Cryptographic Provider, using stronger security through longer key lengths and additional algorithms.

Similarly, the Microsoft Base Smart Card Cryptographic Service Provider is a general purpose CSP for smart cards. Security Provider supports smart cards that use this CSP provided that the smart card vendor has verified that their smart card or token integrates with the mini driver.

If you are having issues with the third party hardware and software, please call that vendor first, unless it is a specific Entrust error.

Third parties can also write their own CSPs in order to support different algorithms, or to allow the CSP to utilize a private security store other than the one provided by Microsoft. For example, the private security store for the Entrust Enhanced Cryptographic Provider is called the Entrust security store. Another example is in smart card deployments where users store their private keys directly on the smart card. Each smart card vendor writes their own CSP for use by CryptoAPI. The non-Entrust private security stores, such as smart cards, are referred to as third-party security stores.

There are usually several CSPs on each computer. Each certificate is indirectly associated through its private key to one CSP, although one CSP can be associated with many certificates. The [certificate stores](#) keep track of the CSP associated with each certificate.

Listing the installed CSPs

To determine what CSPs are installed on a computer with a Windows operating system, check the Windows registry.

To locate the list of CSPs in your Windows registry

- 1 From the **Start** menu, select the **Run** command.
- 2 Type `regedit` in the **Open** text box.

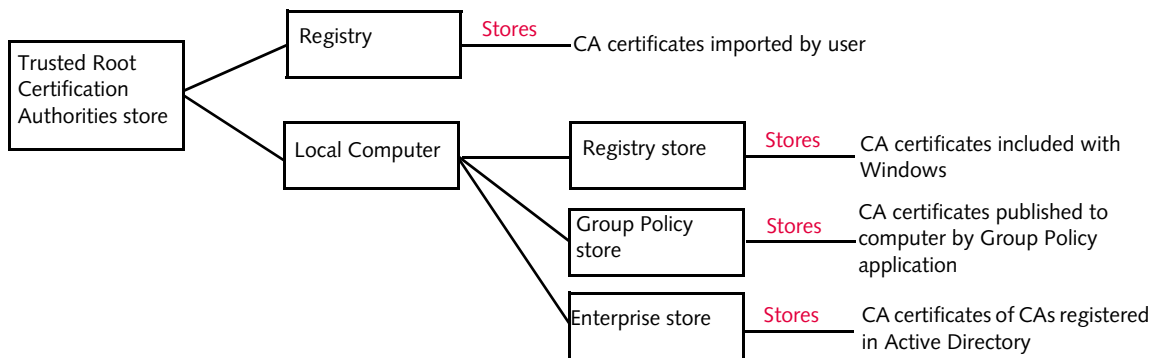
- 3 Click **OK**.
- 4 In the Registry Editor tree view, open
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Defaults\Provider\.

Certificate stores

Certificate stores plug in to CryptoAPI and store certificates and CRLs. Common certificate stores include the Personal, Other People, Intermediate Certification Authorities, and Trusted Root Certification Authorities.

The common certificate stores mentioned above are collections of physical certificate stores. For example, the Trusted Root Certification Authorities certificate store for a typical Windows user is a collection of certificates stored in the registry and local computer. The registry contains CA certificates imported by the user. The local computer contains certificates and settings that apply to the entire computer—every user inherits these certificates. The local computer store is itself a collection of multiple physical stores: registry, Group Policy, and enterprise. The registry store contains CA certificates included with Windows. The Group Policy store contains CA certificates published to the computer through Group Policy and thus, are centrally managed. The enterprise store contains CA certificates from CAs registered in Active Directory as enterprise CAs.

Figure 3: Where CA certificates are stored



Most collection certificate stores follow a similar design; the user's store is composed of a registry store, the computer store, and maybe a Group Policy store.

In addition to storing the certificate itself, a certificate store includes a collection of properties with each certificate. These properties define extra information, such as the CSP associated with a certificate, the archived state, the friendly name, and the description.

The following table provides detailed information on common certificate stores.

Table 5: User, Certification Authorities (CAs), and Publishers certificate stores

Certificate store	Description	Uses
Personal	Holds certificates issued to the user	-decrypting incoming email -signing of outgoing email -used in SSL for client authentication
Other People	Holds certificates for individuals other than the user	-encrypting outgoing email -validating incoming signed email
Trusted Root Certification Authorities	Holds self-signed root certificates for trusted CAs	-establishes trust anchors for validation of certificates
Intermediate Certification Authorities	Holds certificates for trusted subordinate CAs	-establishes trust shortcuts for validation of certificates
Trusted Publishers	Holds certificates for trusted software publishers	-allows verification of Authenticode-signed software

Security stores

Security stores (also called key stores) hold private keys for both users and computers. This includes the [decryption private key](#), the [signing private key](#), and may also contain a history of archived decryption private keys.

A security store is managed by its associated [CSP](#) and is only accessible to the CSP that provided its keys. The CSP determines where the security store is located, and therefore where the private keys are stored. The CSP also determines what algorithm is used to protect the security store.

Microsoft CSPs store private keys in the Windows protected store. An encrypted Windows user profile protects the information. The key is renewed periodically and is used to encrypt each file in the Windows protected store as the file is created.

Smart card CSPs use the card or token itself as a security store, rather than storing the keys on the local machine.

Revocation providers

Revocation providers plug in to CryptoAPI and perform all certificate revocation checks. When a CryptoAPI-enabled application needs to know if a certificate is revoked, CryptoAPI routes the request to the first revocation provider.

Revocation providers are in an ordered list, with the first revocation provider always getting the request first. If the first provider can determine that a certificate is valid or

revoked, the operation ends. If the revocation provider cannot make this determination, the next revocation provider in the list gets the request. This way, revocation providers that use different methods to determine the status can all be used if one provider's method is not appropriate for the given certificate.

Applications

The applications are responsible for calling CryptoAPI functions to request public key and symmetric key operations. Each call must be written into the application or it will not occur. The CryptoAPI calls are passed to the CSP, which performs the actual cryptographic operations. For example, if an application needs to digitally sign a piece of information, the digital signature CryptoAPI call must be triggered from the application itself and functionality built into the user interface. The CryptoAPI calls are then passed to the CSP, which does the actual cryptographic operations. Regardless of which CSP is used, the same CryptoAPI calls are made.

Microsoft applications and any third-party applications that are properly built on the Windows security architecture can list which certificates are available and allow the user to select which certificate to use. Applications can also list the CSPs that are available, or they can automatically select the required CSP for users.

Microsoft Encrypting File System

Microsoft Windows supports the use of Entrust digital IDs with Encrypting File System (EFS). Local and network files and folders can be encrypted using Entrust digital IDs through EFS.

Note: If you move an EFS-encrypted file from an encrypted folder to an unencrypted folder on the same physical drive, it remains encrypted. If you move the file to another drive or a network share, it is decrypted. For more information, consult article 248723, *Understanding Encrypted Directories*, in the Microsoft knowledge base.

Microsoft Data Recovery Agent

The Microsoft Data Recovery Agent is not necessary when using EFS with Security Provider for Windows. Security Manager performs encryption key backups, providing the ability to recover files.

Windows Explorer

The EFS encryption menu option enables you to add Microsoft EFS encryption and decryption menu items to the Microsoft Explorer shortcut menu. The **Encrypt** and **Decrypt** menu items appear when a user right-clicks a file or folder in **My Computer**. Windows Explorer may require a reboot before the menu options are selected.

You can enable the EFS encryption menu through the `EncryptionContextMenu` setting. For details, see [Table 51 on page 432](#).

Microsoft Outlook

You can use Entrust digital IDs created with Security Provider for Windows with Microsoft Outlook S/MIME message security features. For example, Entrust digital IDs can encrypt and digitally sign email messages in Microsoft Outlook.

When necessary, certificates are automatically associated with Microsoft Outlook during enrollment, updates, recovery, and change DN operations. See [“Auto-associating certificates in Microsoft Outlook” on page 255](#) for details.

Internet Information Server (IIS) and Cisco® VPN Client

IIS and Cisco VPN Client are other examples of CryptoAPI-enabled applications that can use Entrust digital IDs. Security Provider manages these digital IDs, as well as any internal information that the application stores about the digital ID. For more information, see [“What is managed?” on page 82](#).

About digital IDs

A digital ID is a set of cryptographic data that defines an entity. The cryptographic data contains, in particular, private keys and public key certificates, which can verify one's identity, much like a driver's license or passport.

This chapter provides detailed information on the types of digital IDs available in a Security Provider environment, and where these digital IDs can be stored.

See the following sections:

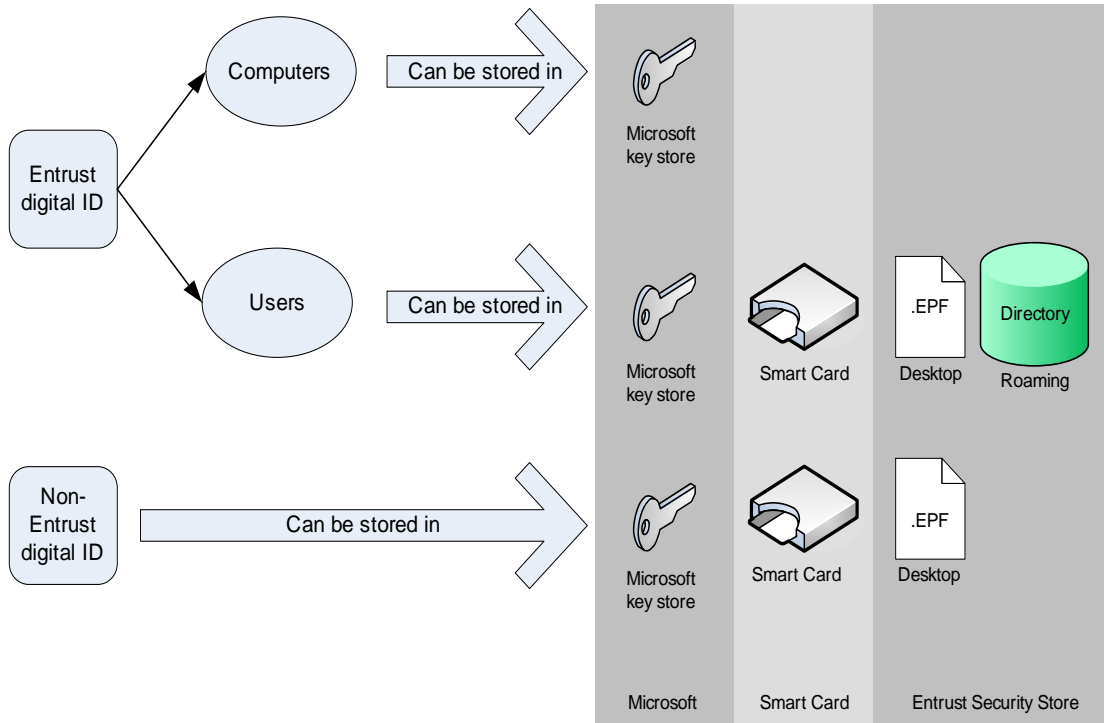
- [“Digital ID overview” on page 46](#)
- [“Entrust security store” on page 52](#)
- [“Third-party security store and mixed digital IDs” on page 58](#)
- [“Exchanging certificates using email” on page 60](#)
- [“Removing and certificates from the Other People certificate store on logout” on page 62](#)

Digital ID overview

Figure 4 shows how digital IDs are categorized, as well as where they are stored. The figure is explained in detail in the following sections:

- [“Digital ID categories—Entrust and non-Entrust” on page 47](#)
- [“Digital ID storage locations” on page 48](#)
- [“CSPs that store digital IDs” on page 50](#)

Figure 4: Digital ID types and where they are stored



Digital ID categories—Entrust and non-Entrust

Table 6 describes the two categories of digital ID: Entrust and non-Entrust.

Table 6: Types of digital ID

Digital ID type	Details
Entrust digital IDs	<p>Entrust products, such as Security Provider, create and manage these IDs. There are two types of Entrust digital ID:</p> <ul style="list-style-type: none">digital ID for a user Used by users to perform cryptographic operations.digital ID for a computer Used by a server—a Web server, for instance—to authenticate to a client. <p>For details on Entrust digital ID features, see “Entrust digital ID features” on page 63.</p>
Non-Entrust digital IDs	<p>These IDs are created by third-party products and are not managed by Entrust.</p>

Digital ID storage locations

Digital IDs are stored in security stores. These are essentially secure places to put keys and certificates belonging to the digital ID. Applications can store both Entrust and non-Entrust digital IDs in the security stores listed in Table 7.

[Table 8 on page 49](#) provides the exact storage locations for the various security stores.

Table 7: Overview of security stores

Storage location	Details
Entrust security store	<p>There are two types of Entrust security stores:</p> <ul style="list-style-type: none">desktop security store The digital ID is stored in an .epf file located on a user's computer. The user must be at this computer to access the security store.roaming security store The digital ID is stored in a directory, allowing users to access their security store from any computer. You must use Entrust Authority Roaming Server to enable roaming Entrust security stores. See "Using the Roaming Server" on page 170 for details. <p>Note: Non-Entrust digital IDs cannot be stored in a roaming security store.</p>
Third-party security store	<p>There are many types of third-party security stores. Among them are:</p> <ul style="list-style-type: none">smart card security stores The digital ID is stored on a smart card.Microsoft key stores The digital ID is stored in the Windows registry. <p>Note: Entrust digital IDs for computers or for Windows services can be stored only in the Microsoft security store.</p>

Table 8: Exact location of certificates and keys in a digital ID

Security store	User's public key certificates stored here	CA certificate and other root certificates stored here	Private keys stored here
Entrust security store—desktop*	on local computer, in an .epf file and Personal certificate store under HKEY_CURRENT_USER in the registry	on local computer, in an .epf file and Trusted Root and Intermediate certificate store under HKEY_CURRENT_USER in the registry	on local computer, in an .epf file
Entrust security store—roaming*	Security Manager's directory and Personal certificate store under HKEY_CURRENT_USER in the registry	Security Manager's directory (through Roaming Server) and Trusted Root and Intermediate certificate store under HKEY_CURRENT_USER in the registry	Security Manager's directory (through Roaming Server)
Third-party—smart card	Personal certificate store under HKEY_CURRENT_USER in the registry	Trusted Root and Intermediate certificate store under HKEY_CURRENT_USER in the registry	on a smart card
Third-party—Microsoft	Personal certificate store under one of these registry keys: <ul style="list-style-type: none"> HKEY_CURRENT_USER (for users) or <ul style="list-style-type: none"> HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates (for computers) or HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Services\ServiceName\SystemCertificates (for Windows services)	Trusted Root and Intermediate certificate store under HKEY_CURRENT_USER in the registry (Users and Windows Services) HKEY_LOCAL_MACHINE (Computers and Windows Services)	on local computer, in protected key store in the Windows registry

Table 8: Exact location of certificates and keys in a digital ID

Security store	User's public key certificates stored here	CA certificate and other root certificates stored here	Private keys stored here
Third-party—other	Personal certificate store in the registry and possibly in other location specified by CSP	Trusted Root and Intermediate certificate store under HKEY_CURRENT_USER in the registry	in a location specified by the CSP

*Of the various Entrust products capable of storing Entrust digital IDs in Entrust security stores, only Security Provider stores the public portion of the Entrust security store in the Microsoft certificate store in addition to the .epf or directory. Having the certificates in the Microsoft certificate store allows other CryptoAPI-based applications to use them.

CSPs that store digital IDs

CSPs are in charge of storing digital IDs, among other tasks. The CSPs that store digital IDs are described in Table 9.

Table 9: CSP overview

CSP	Details
Entrust Enhanced Cryptographic Provider	This CSP is installed with Security Provider and stores digital IDs in Entrust desktop and roaming security stores.
Microsoft CSPs	Microsoft CSPs are made available with the Windows operating system. They store digital IDs in the Microsoft security store.
Smart card CSPs	Several smart card CSPs are made available with the Windows operating system. They store digital IDs on smart cards.

Entrust digital IDs for computers and Windows services must be stored using one of the Microsoft CSPs:

- Microsoft Enhanced Cryptographic Provider v1.0
- Microsoft Strong Cryptographic Provider
- Microsoft Base Cryptographic Provider v1.0
- Microsoft RSA SChannel Cryptographic Provider

Only Microsoft CSPs let administrators disable password prompts. This disabling is necessary to allow computer and Windows services digital ID management to occur without dialog boxes appearing.

For details on the other tasks for which CSPs are responsible, see [“Cryptographic Service Providers \(CSPs\)” on page 38](#).

Note: Three other CSPs are installed with Security Provider for use by other CryptoAPI applications. For details, see [“Entrust Cryptographic Service Providers” on page 129](#).

Entrust security store

Entrust and non-Entrust digital IDs can be stored in an Entrust security store. Entrust security stores are password-protected. See the following sections for details on Entrust security stores:

- [“Entrust security store types, location, and contents” on page 52](#)
- [“Logging in to an Entrust security store and authenticating” on page 52](#)
- [“Logging out of an Entrust security store” on page 54](#)
- [“Entrust security store certificate processing” on page 54](#)
- [“Entrust security store validation” on page 55](#)
- [“Taskbar status icon” on page 55](#)
- [“Enhanced logout support” on page 57](#)
- [“Configuring Entrust security store settings” on page 57](#)

Entrust security store types, location, and contents

For details on the types of Entrust security store available and their location, see [“Digital ID storage locations” on page 48](#).

The Entrust security store may contain varying numbers of keys and certificates, and may contain a full certificate history. For details on the Entrust security store contents, see:

- [“Configuring supported key pairs” on page 95](#)
- [“Entrust digital ID and security store versions and contents” on page 499](#).

Logging in to an Entrust security store and authenticating

From the end user's perspective, the login is the same for users with Entrust and non-Entrust digital IDs. What differs is the underlying processing. For example, if a user has an Entrust digital ID:

- Security Provider checks for updates immediately following the login.
- Security Provider applies any certificate definition policy changes to archived key pairs.

These processes do not occur if the user has a non-Entrust digital ID.

The login occurs in one of these ways:

- [“Logging in by right-clicking the taskbar icon” on page 53](#)
- [“Logging in by attempting to perform a secure operation” on page 53](#)
- [“Authenticating by attempting to use a nonrepudiation key” on page 53](#)

Logging in by right-clicking the taskbar icon

Users can log in by right-clicking the Entrust taskbar status icon and selecting **Log In**. They then select an Entrust security store and submit a password to log in. Users can then perform cryptographic operations using their digital ID, without logging in again, unless the login timeout period is exceeded.

Logging in by attempting to perform a secure operation

From within an application enabled for CryptoAPI or Entrust, users can attempt to perform a signing or decryption operation using the corresponding private keys in their Entrust security store. For example, users might try to sign an email in Microsoft Outlook (a CryptoAPI-enabled application). When the application tries to access the private keys to perform the operations, the Entrust security store login dialog box automatically appears. Users select an Entrust security store and submit a password, and the appropriate private key is made available to the application to perform the desired operation. Once users are logged in, they can perform cryptographic operations without resubmitting their login information.

Occasionally, certain background applications may need to access the Entrust security store to accomplish their routine tasks. For example, Windows Search might periodically need to access your decryption private key in order to decrypt email messages that it wants to index. This may cause the login dialog box to appear when you don't necessarily expect it.

Attention: After logging in, the requesting application will be able to sign, decrypt, and authenticate on your behalf. This is not a concern if you instigated the action, such as when you double-click an encrypted file or encrypted email. However, if you are unaware of what application or what action is about to be performed, you should consider clicking 'Cancel' unless you are comfortable letting the application have access to your digital ID.

Note: Encrypting and verifying are public key operations. Therefore, the user is not prompted to log in to their security store to perform encryption or signature verification operations.

Authenticating by attempting to use a nonrepudiation key

From within a CryptoAPI or Entrust-enabled application, users can attempt to sign information using a nonrepudiation key in their Entrust security store. When the application tries to access the private nonrepudiation key to perform the operation, the Entrust security store authentication dialog box automatically appears. This dialog box appears each time the user uses the key to sign information.

Logging out of an Entrust security store

When a user logs out, Security Provider removes the Entrust security store contents from memory. The logout occurs in one of the following ways:

- Users right-click the Entrust taskbar status icon and select **Log out**.
- Users can press their logout hot key. Users can set this hot key by right-clicking the Entrust taskbar status icon and selecting **Options**.
- After a period of mouse or keyboard inactivity on a computer, Security Provider automatically logs users out. Users can set the login timeout by right-clicking the Entrust taskbar status icon and selecting **Options**.
- The computer goes into suspended mode.
- The Windows session ends.

If an application holds on to a session for longer than the timeout period, configured in Security Manager or on the user's desktop, the Entrust security store becomes locked. This prevents the application from holding on to a session and avoids the authorization password prompts. For more information, see ["Configuring the inactivity timeout" on page 255](#).

Entrust security store certificate processing

The Entrust security store includes the user's certificates and keys in both version 3 (v3) and version 4 (v4). With v4, the full certificate history is available. After the CA certificates are imported as necessary, the user's certificates are imported to the Microsoft Personal certificate store. For each key pair in the Entrust security store, the certificate is extracted if available and imported. If the certificate is not available, the key pair is skipped. Certificate properties such as the archived flag are set on the certificate as necessary.

Security Provider for Windows checks each certificate it processes to see if it is an EFS certificate. If so, Security Provider for Windows checks to ensure that the computer supports EFS. The decryption private key is then exported to the Microsoft Enhanced Cryptographic Provider V1.0. If this is not an archived EFS certificate, the certificate is configured for future EFS operations.

Security Provider for Windows imports certificates to the Personal certificate store and may also mark them archived if they are archived in the Entrust security store. The possibility exists that all the certificates are archived, in which case a warning dialog box appears notifying the user that this Entrust security store only contains archived certificates and thus no updates will be performed. A user can choose to never see this warning again and that selection is saved in the Entrust security store.

If the digital ID contained in the store is an Entrust digital ID, Security Provider performs the following tasks after it processes the Entrust security store's certificates:

- Loads and validates the Entrust policy certificates that are saved to the local disk. This gives Security Provider for Windows access to Entrust policy in case

attempts to contact the directory later to load updated policy certificates fail and to process a few policy-related steps during login.

- Checks the Entrust security store password for expiry. Entrust policy specifies the lifetime of the Entrust security store password in weeks.
- Checks the Entrust policy to see if it should auto-associate the user's Entrust security store with Microsoft Outlook during login.

Once the user logs in successfully, the taskbar status icon changes to show that the user is logged in to the Entrust security store.

If the digital ID contained in the store is an Entrust digital ID, Security Provider performs the following tasks:

- Checks to ensure that the user's current certificates and associated certificate histories are listed in the Personal certificate store, so that old encrypted files can be decrypted. Security Provider performs any necessary updates to the Entrust digital ID.
- Checks the user's current certificates to see if any digital ID management is required. See the section [“Entrust digital ID management” on page 82](#) for further information.




Once users log in, they can use their certificates and keys with multiple applications that use the private keys protected by the Entrust Enhanced Cryptographic Provider, such as Microsoft Outlook, for as long as they remain logged in.

Entrust security store validation

The Entrust security store is validated to ensure that the correct password was given and no tampering occurred. The Password Token section of the Entrust security store is protected by a cyclic redundancy check (CRC) to detect tampering. If the CRC is valid, the password is converted to a symmetric key and a message authentication code (MAC) of a known buffer is created. The MAC is compared to the token entry in the Password Token section to validate the password. Important sections of the Entrust security store are also MACed to prevent against tampering, and other sections have their individual entries encrypted using the symmetric key. The MAC on the Options section of the Entrust security store must be valid for a login to succeed. The MAC on the User X.500 Name is checked, but since it is in an unused section of the Entrust security store only a warning is written to the log if a failure is detected. If the Entrust security store is v4, the MAC on the Keys section is also checked. The MAC on this section must be valid for a login to succeed.

Taskbar status icon

The taskbar status icon is available when you enable Entrust security stores. The icon can appear in one of three ways:

-  —the end user is logged in to their Entrust security store
-  —the end user's Entrust security store is locked
-  —the end user is logged out of their Entrust security store

Users can right-click the icon to display a menu with the following options:

- **Log In** and **Log Out** (see [“Entrust digital ID management”](#) on page 82 for further information)
- **Help**
- **Enroll for Entrust Digital ID** and **Recover Entrust Digital ID Wizard** links
- **Entrust Certificate Explorer**, if installed (see [“Certificate Explorer application”](#) on page 234)
- **Options** which launches the **Entrust Security Store Options** dialog box. It includes the following:
 - a wizard to change the Entrust security store password
 - a setting to configure an inactivity timeout
 - a setting to configure a logout hot key
 - a wizard to help users exchange certificates by email
 - a setting to configure switching from working as a desktop to a roaming user (this is disabled when the roaming feature is not available)
 - a setting to configure switching from working as a roaming to a desktop user

Note: You can hide some of these options. See [“GUI customization settings”](#) on page 478 for details.

Why would I choose not to install the taskbar status icon?

You may decide that the taskbar status icon does not provide your end users with any benefit in the following situations:

- when users will never use the Entrust Enhanced Cryptographic Provider to enroll for their Entrust digital ID; therefore, they will not use the **Entrust Security Store Login** dialog box to log in
- when you want your end users to perform a secure transaction before logging in to their Entrust security store
- when you do not want your users to choose when they want to log in or log out of their Entrust security store

- when you do not want or do not require users to set options in the **Entrust Security Store Options** dialog box

Enhanced logout support

Enhanced logout support is available for Entrust security stores to provide for an orderly logout. The user is automatically logged out or the login sequence is discontinued if the Entrust security store detects the following:

- a screen saver is activated
- users lock their computer
- users cancel a login sequence before completion (no error message is displayed)

By default, enhanced logout support is active. To deactivate it, use the registry setting `DisableEnhancedLogout`. See page 400 for information about disabling the feature.

Configuring Entrust security store settings

Entrust security store settings are available in two locations:

- the Security Manager user policy, configurable through a Security Manager client such as Security Manager Administration
See [“Using Security Manager Administration” on page 251](#) for details. These settings are only used if you are deploying Entrust digital IDs.
- in the registry, configurable through the **Custom Installation** wizard or Group Policy
See:
 - [“Entrust digital ID settings” on page 373](#)
 - [“Entrust security store settings” on page 396](#)
 - [“Entrust Ready identity device setting” on page 469](#)

Third-party security store and mixed digital IDs

Applications can store Entrust and non-Entrust digital IDs in a third-party security store, or in a combination of third-party stores and the Entrust security store.

Third-party security store types, location, and contents

A third-party security store contains public and private information. The third-party CSP used to create the security store determines whether the public key certificates and private keys are password-protected. Consult your third-party vendor's documentation for further information.

For details on the types of third-party security store available and their location, see [“Digital ID storage locations” on page 48](#).

Logging in to a third-party security store and authenticating

From the end user's perspective, the login to a third-party security store is the same for users with Entrust and non-Entrust digital IDs. What differs is the underlying processing. For example, if a user has an Entrust security store digital ID, Security Provider attempts to update the ID immediately after the login. This processing does not occur if the user has a third-party security store digital ID.

The login occurs in one of two ways:

- [“Logging in by attempting to perform a secure operation” on page 58](#)
- [“Authenticating by attempting to use a nonrepudiation key” on page 59](#)

Logging in by attempting to perform a secure operation

From within a CryptoAPI-enabled application (Security Provider, for example), users can attempt to perform a signing or decryption operation using the corresponding private keys in their third-party security store. When the application tries to access the private keys to perform the operations, a login dialog box may or may not appear, depending on whether the security store is password-protected. If the login dialog box does appear, it corresponds to the third-party CSP. For example, if a smart card CSP is used, a smart card dialog box appears.

Users specify a user name and password, and the appropriate private key is made available to the application to perform the desired operation. Once users are logged in, they can perform cryptographic operations without resubmitting their login information.

Note: Encrypting and verifying are public operations. Therefore, the user is not prompted to log in to their security store to perform encryption or signature verification operations.

Authenticating by attempting to use a nonrepudiation key

From within a CryptoAPI or Entrust-enabled application, users can attempt to sign information using a nonrepudiation key in their third-party security store. When the application tries to access the private nonrepudiation key to perform the operation, a login dialog box may appear. In theory, this dialog box should appear each time the users use the key to sign information; however, this is not always the case, even for smart card CSPs. Contact your third-party CSP vendor for details.

Mixed digital ID

Mixed digital IDs occur when keys and certificates in a digital ID are contained in more than one security store. For example, a single digital ID can have its keys and certificates stored in a desktop Entrust security store, on a smart card, and in the Microsoft security store. In this case, the user must log in to three different vendors' dialog boxes—one for Entrust, one for the smart card, and one for Microsoft (if you selected password protection).

If Security Provider needs to manage a mixed Entrust digital ID stored across various security stores, all security stores must be present for the management to occur.

Exchanging certificates using email

Topics in this section include:

- [“How the certificate exchange works” on page 60](#)
- [“How to send a certificate to another user” on page 61](#)
- [“How to import an encryption certificate” on page 61](#)

Entrust Entelligence Security Provider provides a feature for easily exchanging certificates with other certificate users. By clicking a link and following the instructions in the dialog, a user can exchange certificates with another user as email attachments. If the recipient of the certificates is also using Security Provider or Entrust Entelligence Solo, the feature also provides software to assist in adding the certificates to their certificate store. Features include:

- the optional ability to check for tampering using an automatically generated **“thumbprint”** with out-of-band communication
- a customizable, automatically generated email message used to exchange the certificates
- the certificates can be sent in P7C (default) or CER format
- optional password protection using a zipped file attachment for the certificates
- dialog aided addition of exchanged certificates to the user’s certificate store

How the certificate exchange works

The certificate exchange works in the following way:

- 1** The sender selects a digital ID (public certificates only—the user’s private key is not included in the exchange) to attach to the email and send to the person with whom they want to exchange secure email.
- 2** Optionally, the sender records the thumbprint of the digital ID for out-of-band confirmation that the certificates are free of in-transit tampering.
- 3** When the email recipient opens the email they are prompted:
 - a** (optionally) to using an alternate method (such as a telephone conversation with the sender), compare the calculated thumbprint with the one recorded by the sender

If the user enters a matching thumbprint, the **Import** button will remain active. If the thumbprints do not match, the **Import** button will become inactive.
 - b** to add the certificates attached to the email to their certificate store

Attention: For better security, users should always verify the thumbprint. By verifying the thumbprint, the recipient can be confident that the email has not been subject to tampering during transit and the digital ID is genuine.

- c** to send their digital ID certificates back in exchange
If the original sender's email address is included in their certificate, it automatically appears in the return email.
- 4** The recipient attaches their certificates to an email reply and sends it to the person who initiated the exchange.
- 5** Optionally, the person who initiated the exchange verifies the authenticity of the certificates that they received in exchange, using the thumbprint.
- 6** The person who initiated the exchange adds the certificates that they have received to their certificate store.
The software recognizes that this completes the exchange and does not prompt the user to continue.

How to send a certificate to another user

To initiate a certificate exchange follow these instructions:

To send an encryption certificate

- 1** Right-click the Service Provider icon in the system tray and select **Email certificates**.
- 2** From the **Select a digital ID** list, select your digital ID.
If multiple digital IDs appear, select the one that you want to send. Be sure that check that it contains unexpired certificates. You can view details about a certificate by selecting it from the **Digital ID's certificates** list and clicking **View Certificate**.
- 3** Click **OK**.
Your email application opens with a standard email message. One or more certificates (in .p7c format, by default) are attached to the message.
- 4** Send the email to the people with whom you want to exchange encrypted email messages and files.

How to import an encryption certificate

Follow the instructions in the email to import the attached certificates. More information is available in the on-line help.

Removing and certificates from the Other People certificate store on logout

Security Provider can be configured to remove the certificates from the Other People certificate store when the user logs out. This feature helps to clean-up the machine on logout. This feature is controlled by the `DeleteOtherPeopleCertsAtLogout` registry setting (see [page 485](#)).

Enhanced logout support is required by this feature (see [“Enhanced logout support” on page 57.](#))

Entrust digital ID features

This chapter provides detailed information on Entrust digital ID features and processing. Entrust digital ID features are defined as features that only take effect if your users have Entrust digital IDs issued by an Entrust Authority Security Manager CA.

Topics in this chapter:

- [“Entrust digital ID enrollment and recovery” on page 64](#)
- [“Entrust digital ID management” on page 82](#)
- [“Additional Entrust digital ID management for smart cards” on page 88](#)
- [“Communicating with the Certification Authority \(CA\)” on page 92](#)
- [“Configuring supported key pairs” on page 95](#)
- [“Automatic additional certificate download” on page 100](#)
- [“Entrust Desktop Solutions migration” on page 101](#)
- [“Importing and exporting the Entrust key file” on page 105](#)
- [“Configuring an enrollment station” on page 106](#)
- [“Adding and using the Entrust computer digital ID snap-in” on page 107](#)
- [“Adding and using the Entrust Windows services digital ID snap-in” on page 114](#)

Note: Security Provider can be integrated with other Entrust products or a CardMS to deliver extra features to users with Entrust digital IDs. For details, see [“Integrating with other products” on page 147](#).

Entrust digital ID enrollment and recovery

Enrollment and recovery functionality is automatically installed when you select the **Entrust Digital ID for Users**, **Entrust Digital ID for Computers** or **Entrust Digital ID for Services** option in your custom installation package.

Enrollment is the process by which an enterprise delivers managed Entrust keys and certificates to an end user or computer in the form of an [Entrust digital ID](#).

Users or computers must have an existing Entrust digital ID before any secure transactions can be performed. If they do not, they can use Security Provider for Windows to enroll with Entrust Authority Security Manager to create an Entrust digital ID. The enrollment process also creates one or more storage containers, known as security stores, for the Entrust digital ID. A user or computer is defined as an entity that is identified and approved by a [Certification Authority \(CA\)](#).

Recovery is the operation performed when users lose or corrupt their Entrust digital ID.

See one of the following sections for more on enrollment and recovery:

- [“Enrollment and recovery methods” on page 64](#)
- [“Silent enrollment or recovery” on page 65](#)
- [“Enrollment details with Security Manager” on page 66](#)
- [“Reasons for recovery” on page 67](#)
- [“How recovery is initiated” on page 68](#)
- [“Manual enrollment and recovery for users” on page 69](#)
- [“Manual enrollment and recovery for computer digital IDs” on page 73](#)
- [“Manual enrollment and recovery for Windows Services” on page 76](#)

Enrollment and recovery methods

You can configure users and computers to enroll or recover using one of the following methods described in [Table 10 on page 65](#):

Note: Typically, administrators enroll computers and Windows services remotely, requiring the enrollment to run silently (without dialog boxes asking for passwords and so forth) on the target computer. Only Microsoft CSPs allow silent enrollments so, Security Provider uses Microsoft CSPs for computer and Windows service enrollments.

Table 10: Enrollment and recovery

Method	Works for	Details
Manual	users, services and computers	<p>Users may enroll or recover to any available Cryptographic Service Provider (CSP) using the Enroll for Entrust Digital ID Wizard.</p> <p>You can enroll for and recover an Entrust digital ID for a computer or a Windows service to any available Microsoft Cryptographic Service Provider (CSP) using the Computer Digital ID MMC snap-in or Windows service Digital ID MMC snap-in. See “Adding and using the Entrust computer digital ID snap-in” on page 107 or “Adding and using the Entrust Windows services digital ID snap-in” on page 114 for details.</p>
Web	users	<p>Users may enroll or recover over the Web to any available CSP by launching the Enroll for Entrust Digital ID Wizard. This takes them to the Administration Services User Registration Service Web page where they can enroll or recover.</p> <p>The user is not required to enter activation codes—the activation codes are created in Security Manager Administration, passed to the Administration Services, and sent to the enrollment wizard.</p> <p>See the Entrust Authority Administration Services documentation for further information.</p>
Automatic	users and computers	<p>You may enroll for or recover Entrust digital IDs for users and computers using the Entrust Authority Administration Services Auto-enrollment Service.</p> <p>Note: The Auto-enrollment Service does not work with Windows services digital IDs.</p> <p>See “Using the Auto-enrollment Service (Administration Services)” on page 149 for further information.</p>

Silent enrollment or recovery

You might want to hide the wizard if you are enrolling or recovering machine digital IDs on operating systems that do not have a graphical user interface. To hide the enrollment or recovery wizard, run the following command from a shell running as SYSTEM:

```
<eeenlusr.exe|eerecusr.exe> -r <ref_num> -a <auth_code> -c <CA_DN> /ha
```

where:

- <eeenlusr.exe|eerecusr.exe> is one of `eeenlusr.exe` or `eerecusr.exe`, depending on whether you are enrolling or recovering a digital ID

<ref_name> is the reference number required to enroll or recover the digital ID

<auth_code> is the authorization code required to enroll or recover the digital ID

<CA_DN> is only required if there are multiple CAs configured with Security Provider for Windows. It is the distinguished name (DN) of the Certification Authority (CA) that will issue the digital ID.

/ha hides the wizard

Enrollment details with Security Manager

The enrollment feature contacts the CA with the enrollment or recovery request. In order to contact the CA, Security Provider for Windows requires the following information:

- distinguished name (DN) of CA
- host (server) name and port of the CA, or the IP address and port of CA
- [activation codes](#) ([reference number](#) and [authorization code](#)) during a manual enrollment—created in the Security Manager Administration by a Security Manager administrator when adding a user or computer, and securely communicated to the end user or computer

The details of the CA are stored in the Windows registry, and can be configured during the deployment process. For further information, see [“Deploying Security Provider for Windows” on page 281](#).

Key pair support with Security Manager

Security Provider for Windows supports 1, 2, 3, and 4-key-pair users created with Security Manager 8.x.

The number and type of key pairs that a user or computer will enroll for is specified in the user's or computer's [policy certificates](#). See [“Policy certificates for Security Manager” on page 92](#) for further information.

Enrollment and recovery details with Security Manager 8.x

Security Manager 8.x supports a key pair model to meet a wide range of security requirements for users or computers. The model that you choose for a particular situation depends on the authentication, confidentiality, and data security requirements of your organization.

These factors will help you to define the purpose of each key pair, which will lead to a decision on the number of key pairs you need. In some cases, an organization finds that it needs to use several of these models in different parts of the organization and with different functions and different types of employees. For further information, see the *Entrust Authority™ Security Manager Administration User Guide*.

The enrollment feature enrolls and recovers [V2-key-pair](#) users. For further information on [V2-key-pair](#) users, see the *Security Manager Administration User Guide*.

If a V2-key-pair user is enrolling or recovering, any or all following certificates and keys can be generated:

- encryption certificate and associated encryption key pair
- verification certificate and associated signing key pair
- EFS encryption certificate for Microsoft EFS and associated [EFS encryption key pair](#)

The EFS encryption key pair is used specifically to protect data using Microsoft EFS.

- CMP signing certificate and associated CMP signing key pair

The CMP signing key pair is used to connect to the CA when the digital ID does not need a verification certificate.

- nonrepudiation verification certificate and associated [nonrepudiation signing key pair](#)

The nonrepudiation signing key pair is used for users in high-assurance positions who need separate digital signature and nonrepudiation keys.

- dual-usage certificate and associated [key pair](#)
- smart card logon certificate and associated smart card logon key pair

In addition to the creation of keys and certificates by Security Provider and the CA, Security Provider also adds archived keys (also called a key history) to the appropriate security store if the **Back up private key** option is selected in the corresponding key's certificate definition policy. If the **Back up private key** option is disabled, archived keys are not added to the security store. The addition of archived keys occurs when users are recovered, but not when they enroll (because newly enrolled users do not have archived keys).

Some keys are created on the computer by the CSP or on the server by the CA. This is specified in the certificate definition settings of the user's or computer's policy certificate—see [“Policy certificates for Security Manager” on page 92](#) and [“Generating keys within the smart card CSP” on page 183](#) for further information.

Reasons for recovery

Entrust digital IDs may be recovered in these cases:

- when a user has forgotten the password
- the security store is lost or damaged
- the security store is compromised

How recovery is initiated

An Entrust digital ID recovery can be initiated by:

- end users

If an end user forgets the password, loses the security store, or thinks the security store is compromised, the user can request that their Entrust digital ID be recovered by calling their help desk. The administrator then puts the user in recovery mode.

- automatically

Entrust digital ID is automatically monitored and managed by the Security Provider for Windows Digital ID Monitor. The user is prompted with an Entrust Digital ID Recovery Request icon in their taskbar notification area when their verification certificate is expired or revoked. The user clicks the icon or balloon tip, and an Entrust Digital ID Recovery Request dialog box appears.

- an administrator

The administrator might determine that the user's digital ID needs to be recovered for whatever reason.

Once a recovery is initiated:

- The user right-clicks the Entrust security store icon in the taskbar and selects **Recover Entrust Digital ID**.

This launches the **Recover Entrust Digital ID** wizard. The user must either enter the recovery activation codes received from their Security Manager administrator if they are manually recovering, or they will automatically be redirected to the Administration Services Web page if they are configured to self-recover using the Web. They will not be required to enter activation codes using the second method — the activation codes are created dynamically by Administration Services and passed to the recovery wizard.

Note: Instead of notifying users with the security store icon in the taskbar, you can have an alert displayed in a popup dialog by setting the `SkipAutoEnrollRecoverNotification` registry key to 1.

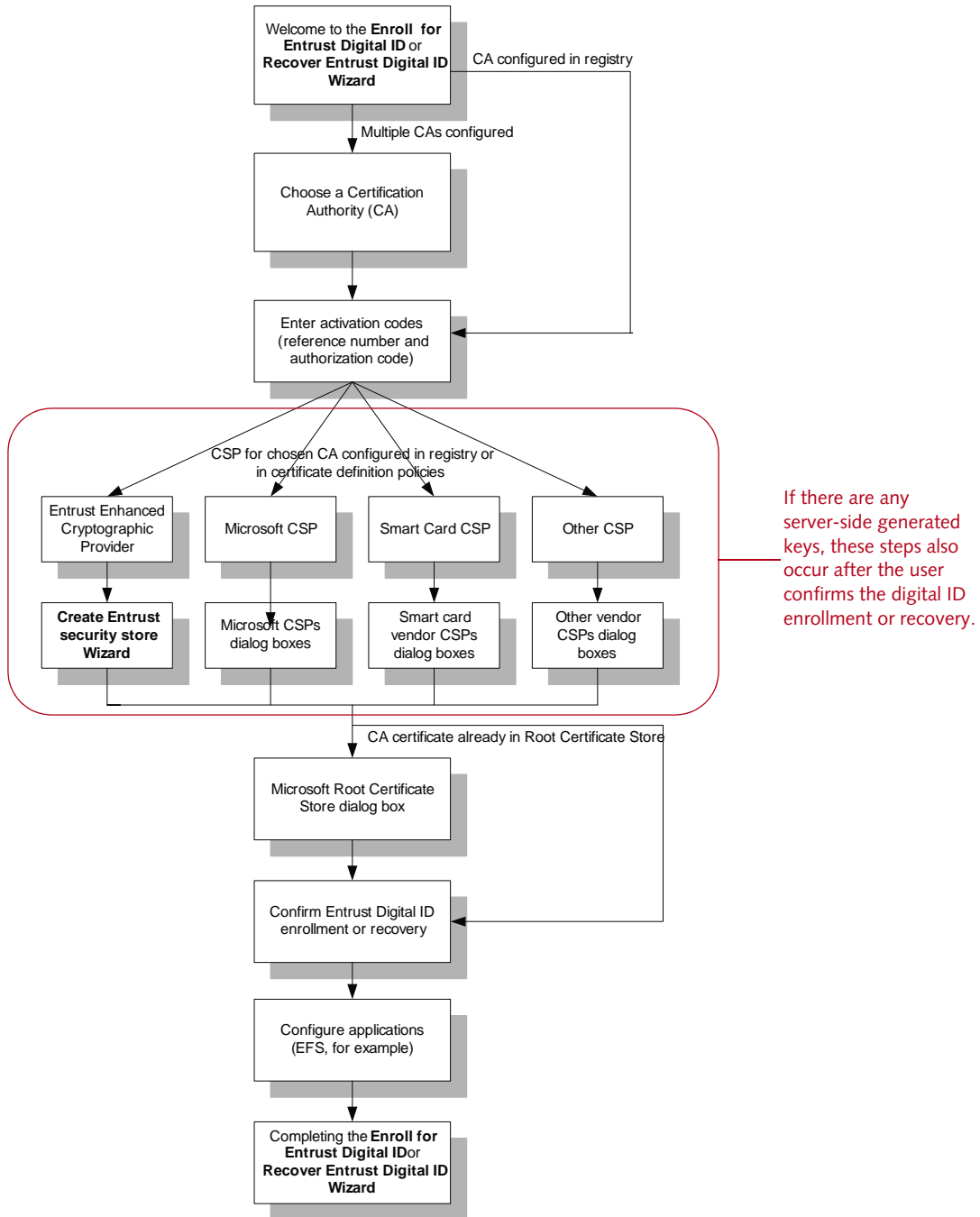
Recovery of a digital ID for a computer or Windows service behaves differently. Security Provider's Computer Digital ID Service detects a recovery for a computer or Windows service and runs the recovery silently. No UI appears.

Manual enrollment and recovery for users

This section describes the complete manual enrollment and recovery procedures for users. Since the **Enroll for Entrust Digital ID Wizard** and **Recover Entrust Digital ID Wizard** follow identical processes, you can assume that this is one process. This section also describes the pages the end user sees when the administrator configures the Windows registry prior to enrollment or recovery. [Figure 5 on page 70](#) provides an overview of the manual enrollment and recovery wizard process for users.

Note: This procedure does not provide all details about enrolling or recovering using Administration Services. See [“Using the Auto-enrollment Service \(Administration Services\)” on page 149](#) for further information.

Figure 5: Manual enrollment and recovery for users wizard processes



To manually enroll or recover users

1 An end user does one of the following:

- Select **Start > Programs > Entrust ESP > Enroll for Entrust Digital ID or Recover Entrust Digital ID**.
- or
- Right-click the taskbar status icon in the taskbar notification area. Select **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** in the pop-up menu.

Note: Instead of notifying users about enrollment with the status icon in the taskbar, you can have an alert displayed in a popup dialog by setting the `SkipAutoEnrollRecoverNotification` registry key to 1.

2 The end user clicks **Next** on the Welcome page.

3 The end user specifies a CA on the **Specify a Certification Authority (CA)** page.

Note: This page appears only if you configure several CAs in the Windows registry.

4 The end user enters a reference number and authorization code on the **Specify your activation codes** page. The activation codes are generated when you create the user's user entry in Security Manager. You must convey these codes to users securely.

Note: If users are enrolling using the Administration Services, the activation codes are sent from Administration Services to the **Enroll for Entrust Digital ID Wizard** or **Recover Entrust Digital ID Wizard**, and users are not prompted for them.

At this point, the CSPs display their corresponding wizards and dialog boxes. Some CSPs may display nothing.

- ### 5 If required, the end user enters information in the wizards and dialog boxes corresponding to any third-party CSPs you configured; for example, the smart card CSP. Users may be required to enter a password for the third-party CSP.
- ### 6 If you configured the Entrust Enhanced CSP, the **Create Entrust Security Store** dialog box appears. End users must fill out the following Entrust security store pages, as follows:

a **Entrust Security Store Location** page

The end user selects to work as a desktop user or roaming user. You, the administrator, can:

- preset and lock the folder location for the desktop Entrust security store
- preset and lock the name of the Entrust security store
- force either desktop or roaming security stores

For details on these and other Entrust security store-related configurations, see [“Entrust security store settings” on page 396](#) and [“Setting roaming permission” on page 254](#).

Note: Users can only enroll or recover an Entrust roaming security store successfully if their computers are configured to communicate with the Roaming Server. See [“Using the Roaming Server” on page 170](#) for further information.

b Entrust Security Store Name page

The end user selects a name for their Entrust security store. (You can preset or lock the Entrust security store name in this input field. See [“Entrust security store creation settings” on page 405](#).)

c Entrust Security Store Password page

The end user selects a password for their Entrust security store. (You can configure the password rules through Security Manager Administration, through the **Custom Installation** wizard, or through Group Policy.)

d Entrust Security Store Finish page

The end user clicks **Finish**.

Security Provider creates the Entrust security store.

- 7** If a user is enrolling to a CA for which the CA certificate is not already present in the Trusted Root certificate store, the **Root Certificate Store** dialog box may appear.

The Microsoft **Root Certificate Store** dialog box does not appear when one or more of the following are true:

- Microsoft Active Directory is in use and the CA certificate is distributed through Group Policy
- the **Anyone who uses this computer** option is enabled on the **User information** page of the Entrust Entelligence Security Provider for Windows setup file (`setup.exe`) and the CA certificate is added in the **Include Additional Certificates** page in the **Custom Installation** wizard

This dialog box asks if the user wants to add the CA certificate to the Trusted Root store. The user must select **Yes** in order for enrollment to successfully complete.

Attention: An end user who does not have local administrator rights on their computer may not be able to add the CA certificate to the Trusted Root store. If this is the case, the administrator must push the Root CA certificate to each end user's computer. CA certificates can be distributed to end users or computers by adding them through the **Include Additional Certificates** page of the **Custom Installation** wizard.

- 8 Some CryptoAPI applications keep internal information about the Entrust digital ID, such as a certificate hash. Security Provider updates this internal information for the following end-user applications during enrollment and recovery:
 - Microsoft Outlook
 - Security Provider for Outlook
 - Encrypting File System (EFS)
 - Cisco VPN Client
- 9 The **Enroll for Entrust Digital ID Wizard** or **Recover Entrust Digital ID Wizard** completes after any applications are configured, as described in the previous step. The end user can now encrypt, digitally sign, and authenticate transactions.

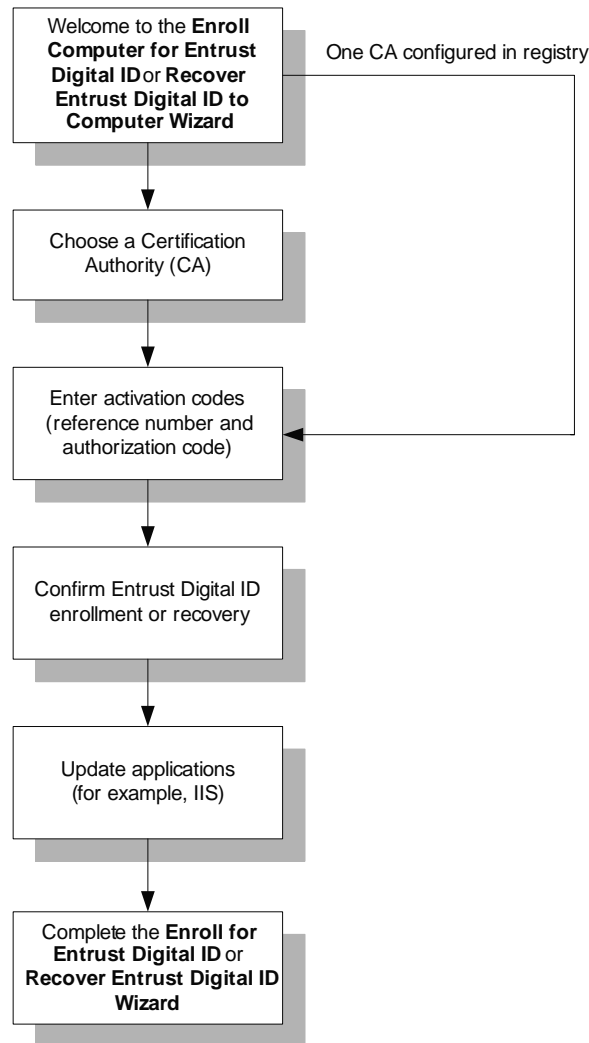
Manual enrollment and recovery for computer digital IDs

This section describes the complete enrollment and recovery procedures for computers. Since the **Enroll Computer for Entrust Digital ID Wizard** and **Recover Entrust Digital ID for Computer Wizard** follow identical processes, you can assume that this is one process.

Note: This procedure does not provide details about enrolling or recovering with the Auto-enrollment Service. See [“Using the Auto-enrollment Service \(Administration Services\)” on page 149](#) for further information.

[Figure 6 on page 74](#) provides an overview of the manual enrollment and recovery wizard process for computers.

Figure 6: Manual enrollment and recovery for computer wizard processes



To manually enroll or recover computer digital IDs

- 1 If you have not done so already, install the Entrust Computer Digital ID Snap-In. See ["To add the Computer Digital ID snap-in" on page 107](#) for details. The snap-in provides a GUI through which to manually enroll and recover Entrust digital IDs for computers.
- 2 Right-click **Entrust Computer Digital ID** in the tree on the left pane.
- 3 Choose either the **Enroll Computer for Entrust Digital ID** or **Recover Entrust Digital ID to Computer** menu option.

The **Welcome to the Enroll Computer for Entrust Digital ID Wizard** or **Recover Entrust Digital ID to Computer Wizard** appears and prompts you to begin the enrollment or recovery process.

- 4 You may be prompted by the **Specify a Certification Authority (CA)** page if an administrator has configured several CAs in the Windows registry. The administrator can configure CAs directly in the Windows registry or by using the **Custom Installation** wizard. If there are no CAs configured in the Windows registry, the enrollment or recovery wizard will not launch.

You can create multiple Certification Authorities and store each CA in the registry. Normally, each CA you create is visible to users in the **Enroll for Entrust Digital ID Wizard** and the **Recover Entrust Digital ID Wizard**.

There may be cases where you do not want every CA shown, such as when a CA is designed for behind-the-scene operations like automatic certificate downloads or CRL checking. Having such Certification Authorities visible in a wizard may confuse users.

To prevent a CA from displaying on the **Specify a Certification Authority** page of a wizard, leave the **Authority** setting empty (see [“General CA settings” on page 348](#) for related information). There must be at least one valid CA configured in the registry setting or the enrollment and recovery wizards will not launch.

- 5 After a CA is chosen or the wizard page is preconfigured with one CA name, you are prompted by the **Specify your activation codes** page. You are required to enter the reference number and authorization code provided by an administrator.

Enroll Computer for Entrust Digital ID Wizard

Specify the activation codes

The wizard needs to know your activation codes so that it can enroll for an Entrust digital ID that is right for you.

Enter your reference number and authorization code:

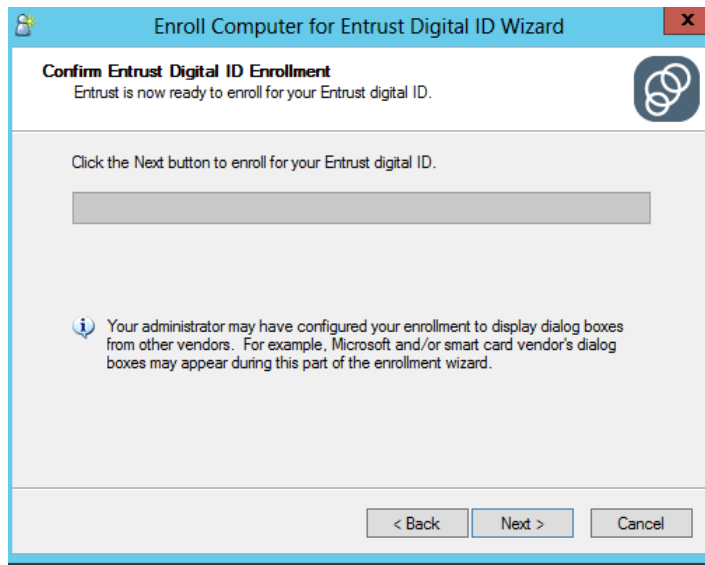
Reference number: 12345678

Authorization code: SXCE-J3PO-IYRE

Your administrator should have provided these values to you (for example, reference number: 91480170 and authorization code: CRTJ-8V0R-VFNS).

< Back Next > Cancel

6 Confirm the enrollment or recovery.



Some CryptoAPI applications keep internal information about the Entrust digital ID, such as a certificate hash. Security Provider updates this internal information for the Internet Information Server (IIS) during enrollment and recovery.

After the application is updated, once the activation codes are entered into the wizard, the next part of the enrollment or recovery process is determined by the Microsoft CSP that you or another administrator configured in the **Custom Installation** wizard, Windows registry, or Security Manager Administration. The CSP determines where the keys and certificates are stored.

The computer's keys and certificates can be enrolled using one of several Microsoft CSPs.

7 Click **Finish** to complete the wizard.

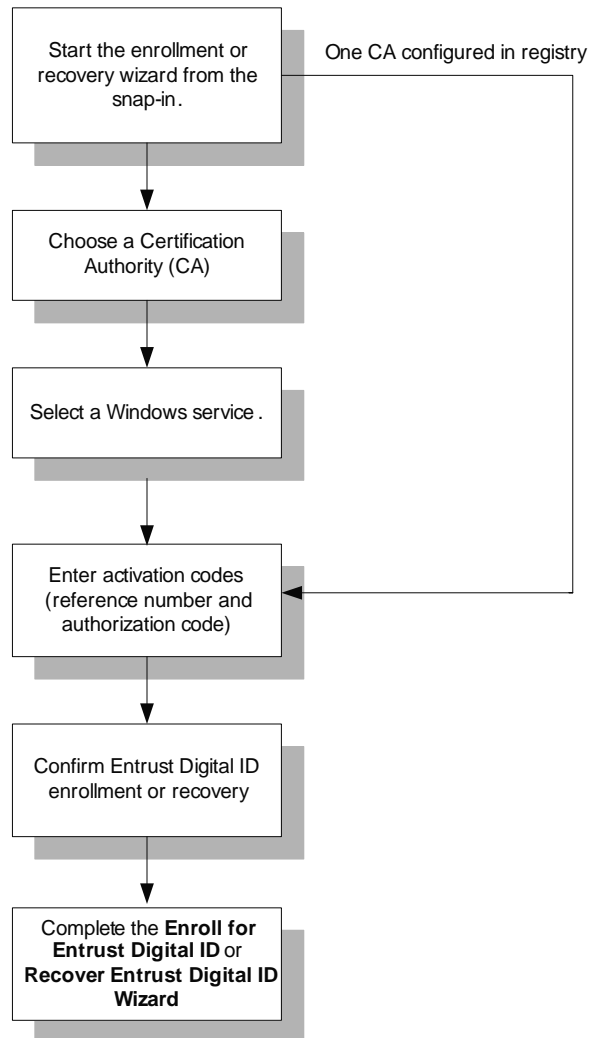
Manual enrollment and recovery for Windows Services

This section describes the complete enrollment and recovery procedures for Windows Services. The **Enroll Windows Services for Entrust Digital ID Wizard** and **Recover Entrust Digital ID for Windows Services Wizard** follow similar procedures.

Note: You cannot use the Auto-enrollment Service to manage Windows services digital IDs.

Figure 7 on page 77 provides an overview of the manual enrollment and recovery wizard process for Windows services.

Figure 7: Manual enrollment and recovery for Windows services wizard processes



To manually enroll or recover digital IDs for Windows services

- 1 If you have not done so already, install the Entrust Windows Service Digital ID Snap-In. See [“To add the Entrust Windows services Digital ID snap-in” on page 114](#) for details. The snap-in provides a GUI through which to manually enroll and recover Entrust digital IDs for Windows services.
- 2 Click **Entrust Windows Service Digital ID** in the tree on the left pane.
- 3 Click **More Actions > All Tasks > Enroll Windows Service for Digital ID** (or **Recover Windows Service for Digital ID**).

The **Welcome to the Enroll Windows services for Entrust Digital ID Wizard** or **Recover Entrust Digital ID to Windows services Wizard** appears and prompts you to begin the enrollment or recovery process.

- 4 If an administrator has configured several CAs in the Windows registry, you will be prompted to select the one to use by the **Specify a Certification Authority (CA)** page.

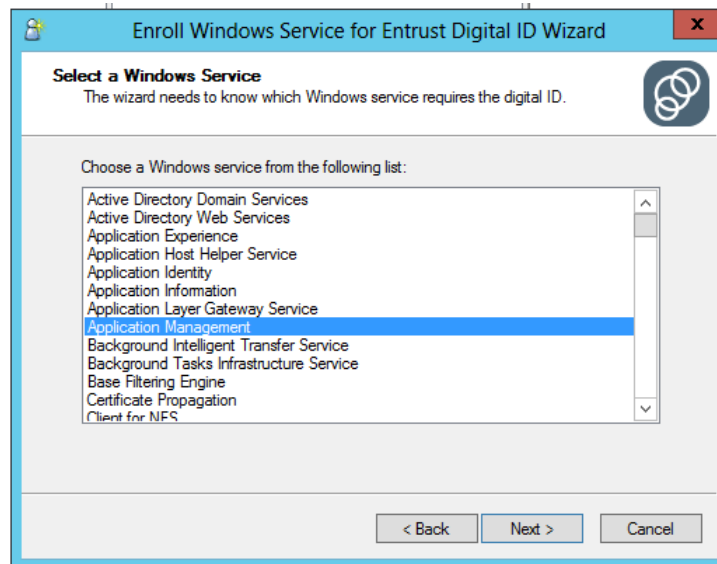
The administrator can configure CAs directly in the Windows registry or by using the **Custom Installation** wizard. If there are no CAs configured in the Windows registry, the enrollment or recovery wizard will not launch.

You can create multiple Certification Authorities and store each CA in the registry. Normally, each CA you create is visible to users in the **Enroll for Entrust Digital ID Wizard** and the **Recover Entrust Digital ID Wizard**.

There may be cases where you do not want every CA shown, such as when a CA is designed for behind-the-scenes operations like automatic certificate downloads or CRL checking. Having such Certification Authorities visible in a wizard may confuse users.

To prevent a CA from displaying on the **Specify a Certification Authority** page of a wizard, leave the **Authority** setting empty (see [“General CA settings” on page 348](#) for related information). There must be at least one valid CA configured in the registry setting or the enrollment and recovery wizards will not launch.

- 5 In the **Select a Windows Service** page, select a service from the list to use the certificate.



- 6 In the **Specify Activation Codes** page, enter the reference number and authorization code provided by the administrator.

The screenshot shows a window titled "Enroll Windows Service for Entrust Digital ID Wizard". The main heading is "Specify the activation codes". Below it, a message states: "The wizard needs to know your activation codes so that it can enroll for an Entrust digital ID that is right for you." There are two input fields: "Reference number:" with the value "67454544" and "Authorization code:" with the value "XXCC-T5DF-DFTY". An information icon and text note that the administrator should have provided these values, giving an example: "reference number: 91480170 and authorization code: CRTJ-8V0R-VFNS". At the bottom are buttons for "< Back", "Next >", and "Cancel".

- 7 Confirm the enrollment. The certificates are generated and placed in the correct stores by the CSP.

The screenshot shows a window titled "Enroll Windows Service for Entrust Digital ID Wizard". The main heading is "Confirm Entrust Digital ID Enrollment". Below it, a message states: "Entrust is now ready to enroll for your Entrust digital ID." There is a large grey rectangular button. An information icon and text note that the administrator may have configured the enrollment to display dialog boxes from other vendors, such as Microsoft or smart card vendors. At the bottom are buttons for "< Back", "Next >", and "Cancel".

- 8 Click **Finish** in the wizard to complete the enrollment.

Configuring the recovery of archived key pairs

When a digital ID is recovered, its archived key pairs (if it has any) must be placed somewhere. There are two ways to store recovered, archived key pairs on the client side, as described in Table 11.

Table 11: Methods for recovering archived key pairs

Archived key pairs can be stored...	Benefits and drawbacks
by the CSP that created the archived key pairs	<p>Benefit: Archived key pairs are placed in the same location they were in before the recovery took place.</p> <p>Drawback: You cannot move Entrust digital IDs from a smart card to a different store. This limitation occurs because archived key pairs created by the smart card CSP must be placed back on the smart card.</p> <p>Instructions: To enable this method, see “To archive key pairs stored by the original CSP” on page 80.</p>
by the current CSP (default). Specifically, this CSP is either <ul style="list-style-type: none">the one defined in the current Encryption Policy, orthe one that is currently configured to store archived key pairs, if no Encryption Policy is defined	<p>Benefit: You can move Entrust digital IDs from a smart card to a different store (by changing the CSP associated with the users through Security Manager).</p> <p>For example, users whose Entrust digital IDs are removed from a smart card in to an Entrust desktop security store have their archived key pairs placed in the location specified by the Entrust Enhanced CSP, as opposed to the smart card CSP.</p> <p>Drawback: None.</p> <p>Instructions: No instructions are provided. This is the default location.</p>

Note: EFS key pairs from the Microsoft Enhanced Cryptographic Provider V1.0 are always recovered to the Microsoft Enhanced Cryptographic Provider V1.0 and are not placed in the current CSP.

To archive key pairs stored by the original CSP

- 1 In Security Manager Administration, do the following:

Note: If the `force_cd_compliance` attribute is already in the `master.certspec` file and you just need to change the setting, skip this step and proceed directly to [Step 2](#).

- a** In the `master.certspec` file, under the `[polcert_cliset Attributes]` heading, add:

```
force_cd_compliance=1.2.840.113533.7.77.62,Boolean,<force_cd_compliance>
```

- b** In the `master.certspec` file, under the `[Variables]` heading, add:

```
force_cd_compliance=Boolean,Force Original CD Compliance:,This attribute instructs a client to honor the original cert-definition policies on all certificates in a digital identity's history.,Range,0,1
```

Note: The identifier `force_cd_compliance` can be replaced with any string. The OID, however, is registered with Security Manager Administration and must be entered exactly as shown.

- c** In the `entmgr.ini` file, under the `[Default Variable Values]` heading, add:

```
force_cd_compliance =0
```

- 2** In Security Manager Administration, expand the **User Policies** node.
- 3** Select the user policy that you are using.
- 4** On the **General Information** tab under **Policy Attributes**, enable **Force Original CD Compliance**.
- 5** Click **Apply**.
- 6** Ensure that the user policy is associated with the users whose archived key pairs you want stored with the original CSP.

Entrust digital ID management

Digital ID management refers to the process of:

- updating key pairs and certificates
- backing up keys
- maintaining key histories
- adding and removing key pairs

Digital ID management only works for Entrust digital IDs and requires the Security Manager CA.

For more on digital ID management, see the following sections:

- [“What is managed?” on page 82](#)
- [“When management occurs” on page 83](#)
- [“When management does not occur” on page 84](#)
- [“Are key histories maintained?” on page 85](#)
- [“How the user experiences key management” on page 85](#)
- [“Other sources of information” on page 87](#)

What is managed?

Security Provider manages:

- Entrust digital IDs stored in any supported store (such as an Entrust security store or smart card).
- information cached locally by CryptoAPI applications

Some CryptoAPI applications store (internally) information about the Entrust digital ID, such as a certificate hash. Security Provider keeps this cached information up-to-date for the following CryptoAPI applications:

- Microsoft Outlook 2010 and later
- Security Provider for Outlook, all versions
- Encrypting File System (EFS) available with Windows
- IIS 5.x and later
- Cisco® VPN Client 4.7 and later

This automatic refresh of cached information ensures that the CryptoAPI application uses the most recent certificates in the Entrust digital ID.

The refresh occurs at periodic intervals and during enrollment. (During enrollment, only Outlook, Security Provider for Outlook, and EFS are refreshed.)

When management occurs

Security Provider monitors certificates and keys for Entrust digital IDs, and updates them (if required) at a configurable time interval and whenever users or computers log in to Windows. After an update, Security Provider downloads the latest policy certificates from Security Manager.

Updates are performed when:

- the encryption public key or the signing private key lifetime is approaching expiry (the percentage of the verification certificate's lifetime at which the update occurs is configurable—see “Entrust digital ID for users options settings” starting on page 373 for details about the registry settings related to this feature)
- the encryption public key has expired (as long as there is still a valid signing key in the Entrust digital ID)
- the encryption public key is revoked (as long as there is still a valid signing key in the Entrust digital ID)
- an administrator updates the user's distinguished name (DN), or keys
- a root CA or subordinate CA key rollover occurs (these rollovers only occur if an administrator forces a key update)

When using Security Manager 8.x and later, updates are also performed for the following reasons:

- an Entrust digital ID is not synchronized (for example, if it is missing some backed-up certificates located on Security Manager, or if it is stored on multiple machines)

See [“Updating Entrust digital IDs” on page 273](#) for more information.

- the certificate update date, specified in the certificate definition policy, is reached
- a certificate type change is performed
- a certificate type is obsoleted
- a certificate definition is added or removed from the certificate type
- the user's or computer's entry in Security Manager is moved from one Security Manager 8.x to another Security Manager 8.x, and both CAs are known to Security Provider

(This moving of digital IDs is known as the automatic move user feature.) The move operation in Security Provider for Windows is automatic and behaves like a key update.

- an Entrust security store does not contain a certificate history


Entrust security stores created by some older Entrust products do not contain certificate histories. If this is the case, Security Provider downloads the

certificate history from Security Manager and places it in the Entrust security store (.epf file).

When management does not occur

Digital ID management does not occur if

- an Entrust security store (.epf file) is read-only
Users are alerted with a warning indicating that their read-only Entrust security store needs updating. For read-only security stores, Security Provider's Digital ID Monitor service still checks each certificate's expiration and rollover time, but no updates are performed until the user makes the .epf file writable.
- users' Entrust digital IDs have keys and certificates distributed in different security stores, and not all are available
This may be the case if users are roaming to new computers with only a portion of their Entrust digital IDs.
- Security Provider has not been configured
If Security Provider is installed without first being configured, then the Security Provider installation will not have your PKI and directory server settings. Without knowing which PKI or directory to connect to, digital ID management cannot occur.
- the user is offline

Attention: A user is said to be offline when Security Provider cannot connect to the network, Security Manager, or its directory. While offline, Security Provider's Digital ID Monitor checks each certificate's expiration and rollover time in the Entrust digital ID for a user. If an update is required, the user is prompted with an **Entrust Digital ID Update Request** icon  in their taskbar. The update request message informs the user that Security Provider could not contact Security Manager to complete the update.

Note: When the user is offline, Security Provider continues to retry managing the Entrust digital ID every 30 seconds if it receives a cannot connect error code. The retry rate is configurable, and useful for VPN users who may log in to their security stores before creating their VPN connection. In this scenario, the first couple of management attempts may fail, but once the VPN connection is established, Security Provider can successfully check for updates. For details on configuring the retry rate, see [“Entrust digital ID for users options settings” on page 373](#).

Are key histories maintained?

Key histories are maintained for users' and computers' encryption key pairs ([decryption private key](#) and encryption certificate) for V1 digital IDs. For V2 digital IDs, key histories are maintained for users' and computers' encryption key pairs as specified in the **Backup private key** option of the certificate definition settings [policy certificate](#). Verification keys cannot be backed up. See ["Certificate definition policy settings" on page 259](#) for further information.

How the user experiences key management

Security Provider's Digital ID Monitor, Computer Digital ID Service and Windows Services Digital ID Service check for key updates for users, computers, and Windows services respectively, at the following three events:

- when a user logs in to Windows (user digital IDs only)
- when the Computer Digital ID Service starts (computer digital IDs only)
- when the Windows Service Digital ID Service starts (Windows services digital IDs only)
- at a specified time interval (by default, every 12 hours)


The update is different for users and computers. See:

- ["Updating a digital ID for a user" on page 85](#)
- ["Updating a Digital ID for computer" on page 86](#)
-

Updating a digital ID for a user

Digital ID updates for users differ depending on whether users are logged in to their Entrust digital ID or not.

Note: The following describes the default update behavior. You can change this behavior with the following settings described in ["Entrust digital ID for users options settings" on page 373](#): `EffectOfLoginOnWaitingUpdate`, `CertUpdateInterval`, `IgnoreEntrustSecurityStoreUpdateUntilLogin`, `SkipUpdateAfterEntrustSecurityStoreLogin`, `UpdateDigitalIDSilently`, `MonitorStartingDelay`, `IgnoreUpdateAttempts`, and `SkipUpdateNotification`.

- If users are not logged in to their Entrust digital IDs, and the Digital ID Monitor detects that an update is required, by default, users are prompted with an **Entrust Digital ID Update Request** icon  in their taskbar notification area. At this point, users can double-click the icon in their

taskbar. This opens the **Entrust Digital ID Update Request** dialog box which presents users with three choices:

- update immediately

Click **Update**. Users' Entrust digital IDs begin updating. Users are informed when this process is complete.

- update later

Click **Remind Me Later**. Users are reminded at configurable time intervals.

- delete the digital ID

Click **Delete Digital ID**. This option is provided for users who no longer require a particular Entrust digital ID—for example, users who are no longer using the smart card that contains their Entrust digital IDs.

If users do not double-click the update icon in their taskbars, the update occurs automatically when they log in to their Entrust digital IDs.

- If users are logged in to their Entrust digital IDs, and the Digital ID Monitor detects that an update is required, the update occurs immediately without further action.

When you configure auto-enrollment or recovery for users to run silently, digital ID management is silent. Updates occur transparently and automatically without prompting the user.

Note: For details on the other effects of taking over management of an older Entrust security store, see [“Entrust digital ID and security store versions and contents” on page 499](#).

Updating a digital ID silently if Security Provider's Digital ID Monitor detects that an update is required

Security Provider can be set to update a digital ID silently (without displaying the update icon) any time that the Digital ID Monitor detects that an update is required. This feature is configured using the registry setting `UpdateDigitalIDSilently` (see page 382 for detailed information).

Note: The PKIX-CMP signing key must not be password protected for this feature to work properly. Be sure that Protect key storage for CSP is not selected in security manager's certificate definition policy settings.

Updating a Digital ID for computer

When the Computer Digital ID Service performs the digital ID management, the management is always silent. No user interface appears.

Updates for an Entrust computer digital ID occur in one of two ways:

- Automatic

The Computer Digital ID Service updates the digital ID silently, with no user intervention, at a specified time interval. See [“Entrust computer digital ID settings” on page 392](#) for details on setting the time interval.

- Manual

An administrator forces an update. The update then occurs silently, with no user input. See [“Viewing and managing computer digital IDs” on page 111](#) for details on how to force an update.

Updating a Digital ID for Windows service

When the Computer Digital ID Service performs the digital ID management, the management is always silent. No user interface appears.

Updates for an Entrust computer digital ID occur in one of two ways:

- Automatic

The Service updates the digital ID silently, with no user intervention, at a specified time interval. See [“Entrust Entelligence Windows Service Digital ID settings” on page 389](#) for details on setting the time interval.

- Manual

An administrator forces an update. The update then occurs silently, with no user input. See [“Viewing and managing Windows service digital IDs” on page 118](#) for details on how to force an update.

Other sources of information

For more information on key lifetimes and updates, see the *Security Manager Administration User Guide*.

Additional Entrust digital ID management for smart cards

Smart cards present an additional digital ID management challenge. As a user's certificates change over time, the history information can grow so large that the smart card fills up. You cannot just limit the number of old keys stored on a smart card or delete the oldest ones because the user may need to reference the old keys. For example, if a user wants to access a file encrypted using an older key, the user needs access to that old key.

Security Provider includes two features that work together to manage old smart card keys and key history:

- **Key Access Service (KAS)**

This digital ID management service provides access to a smart card user's old encryption keys stored by Security Manager when a CryptoAPI application requires an old key that is not on the smart card.

See ["How the Key Access Service works" on page 88](#).

- **Max key count** attribute

This certificate definition policy attribute sets the maximum number of keys that Security Provider will store on a smart card. Once the card reaches that number, Security Provider removes the oldest key or keys to make room for a new one.

To set this attribute, see ["Setting the Max key count attribute" on page 90](#).

Note: KAS manages and stores encryption keys and dual-purpose keys to provide access to documents encrypted by old keys. KAS is not concerned with signing key pairs. Consequently, the **Max key count** attribute applies to the number of encryption and dual-usage key pairs stored on a smart card. This attribute does not count the number of stored signing key pairs. See ["Calculating maximum keys" on page 91](#).

How the Key Access Service works

The Key Access Service (KAS) works automatically to retrieve old smart card keys from Security Manager when an application requests a key that is no longer stored on the smart card.

Attention: KAS requires Security Manager to retrieve old smart card keys.

KAS includes the following components and processes.

KAS application

The KAS application runs in the user's account and initiates during system startup. In turn, it starts up the other KAS components and establishes the connections among them. The KAS application also does the following:

- Retrieves backup user key pairs from Security Manager.
- Caches the user's key pairs and associated certificates to the internal cache, as required.
- Manages the internal cache.
- Provides private key information to the KAS Cryptographic Service Provider.
- Provides encryption certificates to the KAS Certificate Store Provider.

The KAS application detects when a user inserts a smart card. It reads the *Entrust Missing Key ID Sequence* extension in the KAS certificate to retrieve missing key IDs, and then generates a `key_prov_info.dat` internal cache file for each key ID. The KAS application checks for an inserted smart card twice a second.

KAS Certificate Store Provider

The KAS Certificate Store Provider works with the Microsoft Personal certificate store. When a CryptoAPI application cannot find the smart card certificate in the Personal certificate store, the Certificate Store Provider uses the KAS application to retrieve the certificate from Security Manager or the internal cache file.

KAS Cryptographic Service Provider

This CSP lets CryptoAPI applications access a user's old private keys that no longer exist on a smart card due to size limitations. For more information, see [“Entrust Key Access Service Cryptographic Service Provider” on page 131](#).

Internal cache

The internal cache is a file-based certificate store that holds older certificates. It works as an extension to the My Security store. The cache retains a user's old key pairs and associated certificates. For users with X509 certificates, the cache is located in a folder under:

`\Users\<user name>\AppData\Roaming\Entrust\ESP\KAS\<key id>`

where `<user name>` is the name of the logged-in user.

In all cases, `<key id>` is a hashed key ID created by the KAS application. The key ID folder contains three files: `key_prov_info.dat`, `key_pair.dat`, and `encryption_cert.sst`.

By setting the `KASCacheLifetime` registry key, you can control how long the cache files can exist before the KAS application must generate new ones. See

[“Miscellaneous settings” on page 484.](#)

Update and recovery processes

Update and recovery functionality is built-in to Security Provider.

The update mechanism informs the KAS application when a smart card digital ID is updated. For an update, the KAS application:

- deletes all cached files related to the smart card digital ID
- reads the Entrust Missing Key ID Sequence extension in the KAS certificate to retrieve missing key IDs
- generates a `key_prov_info.dat` internal cache file for each key ID

The recovery mechanism informs the KAS application when a smart card digital ID is recovered. For a recovery, the KAS application:

- reads the Entrust Missing Key ID Sequence extension in the KAS certificate to retrieve missing key IDs
- generates a `key_prov_info.dat` internal cache file for each key ID

Setting the Max key count attribute

To use the **Max key count** certificate definition policy attribute, you must first define it in Security Manager by adding the attribute to the `master.certspec` file.

To add the attribute to Security Manager

- 1 In Security Manager Administration, have a Security Officer export the `master.certspec` file and open it in an editor.
- 2 In the `master.certspec` file, under the `[polcert_certdefn Attributes]` heading, add the following on one line:

```
cd_key_max_count=1.2.840.113533.7.77.46.5.14,UTF8String,"<cd_key_max_count>"
```

- 3 In the `master.certspec` file, under the `[Variables]` heading, add this:

```
cd_key_max_count=TextString,Max key count:,Maximum number of keys to store in a user's CSP. A value of 0 disables the KAS application.,Range,0,1000
```

- 4 Save and import the modified `master.certspec`.
- 5 In the `entmgr.ini` file, under the `[Default Variable Values]` heading, add:

```
cd_key_max_count=<n>
```

where `<n>` is the maximum number of key containers available. See [“Calculating maximum keys” on page 91](#).) A value of 0 disables managing of the keys by KAS.

Once you modify the `master.certspec` file, you can set or change this attribute at any time using Security Manager Administration.

Note: For details on how to set an attribute in Security Manager Administration once it exists in the `master.certspec` file, see [“Configuring the certificate definition policy settings” on page 265](#).

Calculating maximum keys

When you set a value for the **Max key count** attribute in Security Manager Administration, keep in mind the following:

- Get an accurate count of the maximum number of key containers on the smart card from your smart card vendor's documentation.
- Keep in mind that KAS places its own certificate on the user's smart card. This takes up one key container on the smart card.
- When you need to replace an existing signing key with a new one, you need two containers: one for the new key and one for the old key before it is deleted.
- Given the above, the value you set for **Max key count** can be no greater than the maximum number of key containers available on your smart card minus three.

If you set the **Max key count** value higher than the maximum allowed by the above calculation, your users' smart cards may fill up. If this happens, there are two ways to fix the problem:

- To fix the problem for all users of that smart card:
 - Have users delete the certificates from their smart card and Personal certificate store.
 - In Security Manager Administration, reduce the value set for **Max key count**.
 - Have users perform a key recovery.
- To fix the problem on a user-by-user basis without changing the value for **Max key count**:
 - Have each user delete the certificates on their smart card and in their Personal certificate store, including their archived certificates.
(To see archived certificates in the Entrust Certificate Explorer, open your Personal certificate store, right-click the right pane, and select **View > Show Archived Certificates**.)
 - Have users perform a key recovery.
 - Let KAS monitor the key count. If the smart card fills up, Security Provider will remove at least two key pairs (the oldest ones) and add their key ID to the KAS certificate.

Communicating with the Certification Authority (CA)

When the required information is obtained by Security Provider for Windows, the [PKIX-CMP protocol](#) is used to securely communicate with the CA in order to complete the enrollment or recovery request.

You distribute Certification Authority (CA) certificates to end users or computers by adding them to the **Include Additional Certificates** page of the **Custom Installation** wizard.

The CA returns the following information to Security Provider for Windows:

- the user or computer's [policy certificates](#)
- the user or computer's certificates, as follows for 1-key-pair, 2-key-pair, and V2-key-pair users:
 - the user or computer's dual-key usage public key certificate (for a [1-key-pair](#) user)
 - the user or computer's encryption and verification certificates (for a [2-key-pair](#) user)
 - any combination of the user or computer's encryption certificate, verification certificate, stand-alone EFS encryption certificate, CMP signing certificate, EFS encryption certificate, nonrepudiation verification certificate, or a dual-usage certificate (for a [V2-key-pair](#) user)
- any user's or computer's key pairs generated by the CA
- the issuing CA's certificate
- the root CA's certificate (if a CA hierarchy is in use)
- the certificate path between the root CA and issuing CA certificates (if a CA hierarchy is in use)
- the key history (list of archived key pairs and certificates), in the case of a recovery request only

Policy certificates for Security Manager

A [V2-key-pair](#) user has two types of [policy certificates](#)—client settings policies (also known as role policies) and certificate definition policies.

Client settings policies, or role policies, are associated with user roles. The group of settings defined for a user role applies to every user or computer assigned the associated role.

In addition to being assigned a user role, each V2-key-pair user is also assigned a [certificate type](#). The certificate type determines the number and type of key pairs to be generated for the user or computer. Certificate types are associated with certificate

definitions, which have an associated certificate definition policy. The settings defined apply to every user or computer assigned the certificate type. For example, settings defined for the encryption certificate definition apply to every user or computer who is assigned the encryption certificate.

The enrollment feature caches the policy certificates to provide both the digital ID management and the Entrust security store features with access to the user or computer's policy information.

The **Key usage policy** option in the certificate definition policy specifies the purpose of the client-generated key pair as encryption, verification, or both. See [“Certificate definition policy settings” on page 259](#) and the “Key usage policy” section in the *Security Manager Administration User Guide* for more detailed information.

The enhanced key usage (EKU) certificate extension identifies the type of application the certificate will likely be used with, making it easier for the application to select a certificate to use if one is not already selected. See the chapter “Including AIA and EKU values in certificates” in the *Entrust Authority Security Manager Interoperating with Microsoft PKI-enabled applications* white paper published by Entrust for further information.

Note: This information is set by the Security Manager administrator, but will require information from you (or the Security Provider administrator).

V2-key-pair certificate types

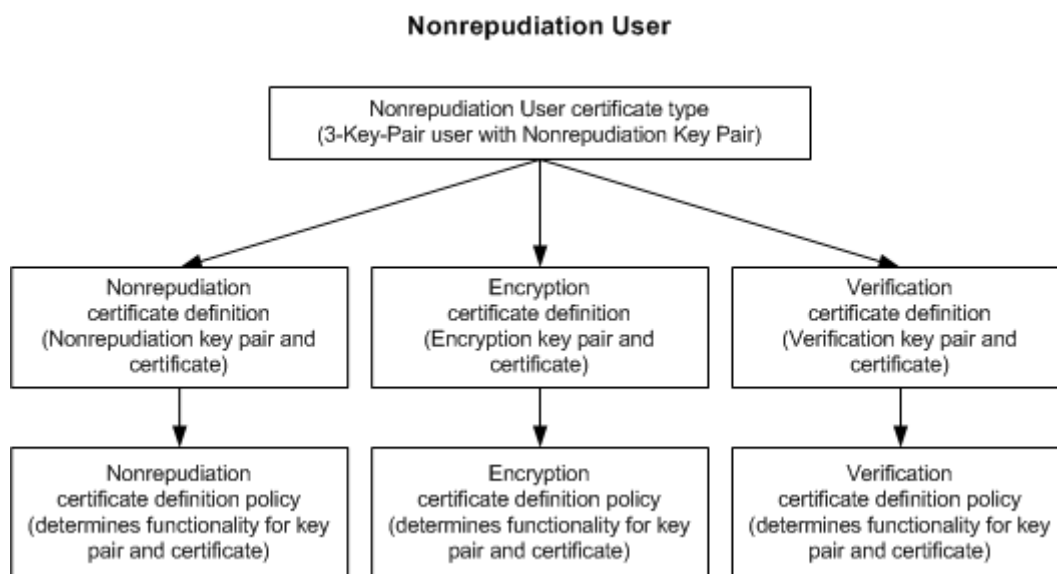
Entrust provides a number of default V2 certificate types, each with one to four associated certificate definitions. For example, the Nonrepudiation User certificate type has three associated certificate definitions:

- Nonrepudiation
- Encryption
- Verification

Each of these certificate definitions have associated certificate definition policy.

Figure 8 provides an example of how a certificate type has associated certificate definitions with associated certificate definition policies.

Figure 8: Example of the Nonrepudiation User certificate type



Relationship between certificate types, certificate definitions, and certificate definition policy

V2 certificate types map to the number of key pairs you want your user or computer to have in the Entrust digital ID. The Nonrepudiation User example in Figure 8 shows a 3-key-pair user.

A certificate definition always maps to a key pair. In the Nonrepudiation User example, there are three key pairs:

- Nonrepudiation key pair

- Encryption key pair
- Verification key pair

Each of these key pairs have associated certificates.

The certificate definition policy that is associated with a certificate definition determines the functionality for the user or computer's key and certificate:

- The nonrepudiation certificate definition policy determines the functionality for the nonrepudiation key pair and certificate.
- The encryption certificate definition policy determines the functionality for the encryption key pair and certificate.
- The verification certificate definition policy determines the functionality for the verification key pair and certificate.

See ["Certificate definition policy settings" on page 259](#) for further details about configuring certificate definition policies.

Configuring supported key pairs

Security Provider supports all default key pairs available in Security Manager.

The following table describes the supported key pairs and their certificate types.

Table 12: Security Manager supported V2 key pairs

Version	Certificate type	Certificate Definition	Certificate Definition Policy
V2	2-key-pair user	Encryption Verification	Encryption Policy Verification Policy
V2	1-key-pair user (1-key-pair user with a dual usage key pair)	Dual Usage	Dual Usage Policy
V2	EFS User (3-key-pair user with EFS key pair)	Encryption Verification EFS	Encryption Policy Verification Policy EFS Policy
V2	Standalone EFS User (2-key-pair user with EFS key pair)	Standalone EFS Encryption CMP Signing	MS EFS Policy MS CMP Signing Policy
V2	Nonrepudiation User (3-key-pair user with Nonrepudiation key pair)	Nonrepudiation Encryption Verification	Nonrepudiation Policy Encryption Policy Verification Policy

Table 12: Security Manager supported V2 key pairs

Version	Certificate type	Certificate Definition	Certificate Definition Policy
V2	Nonrepudiation/EFS User (4-key-pair user with Nonrepudiation key pair)	Encryption Verification Nonrepudiation EFS	Encryption Policy Verification Policy Nonrepudiation Policy EFS Policy
V2	Smart Card Logon for Microsoft Security Framework users (Windows Smart Card Logon Certificates for a Microsoft Security Framework environment)	Dual Usage	Dual Usage No Key Backup Policy

1-key-pair user

The 1-key-pair model should be used when a user or computer is using Secure Multipurpose Internet Mail Extension (S/MIME) applications that do not interoperate with the Entrust 2-key-pair model. The key pair consists of two dual-usage keys:

- a public key, used for both encryption and verification
- a private key, used for both decryption and signing

In the V1 1-key-pair model the encryption and digital signature functions are combined. The V2 1-key-pair model combines the encryption function with either the digital signature function or the nonrepudiation function.

There are several circumstances in which Entrust recommends that you do not create 1-key-pair users:

- When both digital signature and nonrepudiation are essential, since the dual-usage private key will be backed up in order to enable key recovery.
- When the user is an administrative user. While users of any role can be 1-key-pair users, nonrepudiation is essential for administrative users.

2-key-pair user

The V1 and V2 2-key-pair models are designed for the most common encryption and digital signature requirements. They take a fairly standard approach to security requirements by providing the encryption and digital signature capabilities separated into two key pairs.

EFS User

The EFS User is a 3-key-pair certificate type. It is for users or computers that need to use the Microsoft EFS functionality and also need email encryption and signing capabilities.

Entrust recommends that the EFS User enrolls for an Entrust security store (.epf file) for the following reasons:

- EFS key pair can roam with the user
If users roam with their Entrust security store (by either setting themselves up as a roaming user and then changing computer, or by copying their .epf file to another computer), the EFS key pairs are added to that computer when the user logs in to their Entrust security store.
On user login, Security Provider copies the EFS key into CSP appropriate for the key length (Microsoft Base Cryptographic Service Provider is limited to a maximum key size of RSA-1024) and automatically changes the CSP name in the certificate properties to that CSP.
- no accidental deletion of the EFS key pair
If the user accidentally deletes their EFS certificate from the certificate store, Security Provider refreshes this EFS certificate the next time the user logs in to their Entrust security store.

Note: The EFS key cannot be stored on a smart card.

Standalone EFS User

The Standalone EFS User is a 2-key-pair certificate type designed for those using EFS exclusively. This user does not need to do any regular signing or encrypting operations. This model has two key pairs, one for EFS encryption, and one for CMP (Certificate Management Protocol) Signing.

The key pairs are stored directly in the Cryptographic Service Provider appropriate to the key length, which eliminates the need for the Entrust security store. The EFS and CMP Signing keys are not password protected. The CMP Signing key pair is necessary to sign key update messages sent to the CA, and this key update can only occur with a valid message signing certificate. The CMP Signing key prevents third-party CryptoAPI-enabled applications from using it as a signing key. The EFS key cannot be stored on a smart card.

Attention: The Microsoft Base Cryptographic Provider v1.0 only supports 1024-bit keys.

Nonrepudiation user

The nonrepudiation user is a 3-key-pair certificate type. It is for users in high-assurance positions who require separate digital signature and nonrepudiation keys. A user must authorize a secure signing operation, through the use of a password prompt, every time they want to access this key pair.

Note: Entrust Enhanced Cryptographic Provider forces secure signing authorization for the nonrepudiation key. It is up to third-party CSP vendors to support these configuration rules for the nonrepudiation key.

Nonrepudiation and EFS User

The nonrepudiation and EFS User is a 4-key-pair certificate type. It is for users in high-assurance positions who require separate digital signature and nonrepudiation keys, and users who need to use the Microsoft EFS functionality with email encryption and signing capabilities. The EFS key cannot be stored on a smart card. .

Attention: Entrust computer digital ID and Windows services digital IDs do not support the use of 4-key pairs.

Smart card logon user

The smart card logon user is a 1-key-pair certificate type. It is for smart card users who typically use their smart cards to log in to applications on their workstation or log in to a Windows workstation. The smart card logon user combines the encryption function with the digital signature function. This dual usage key usage satisfies Microsoft's requirements. The dual usage key is never backed up, which prevents the smart card from filling up with key history. Typically, the key is not used to encrypt data so the key history is not necessary.

Selecting supported Security Manager key pairs

When an administrator creates a new user in Security Manager Administration, they can select one of the default number of key pair [certificate types](#) to assign to the end user:

- [2-key-pair user](#)
- Standalone EFS User (2-key-pair user with EFS key pair)
- EFS User ([3-key-pair user](#) with EFS key pair)
- Nonrepudiation/EFS User ([4-key-pair user](#) with nonrepudiation and EFS key pairs)

- Nonrepudiation user (3-key-pair user with nonrepudiation key pair)
- 1-key pair ([1-key-pair user](#) with a dual-usage key pair)
- smart card logon user (1-key-pair user with a dual-usage no key backup key pair)

Each of the above certificate types is associated with certificate definitions, which are associated with a certificate definition policy. See the table [“Security Manager supported V2 key pairs” on page 95](#) for information on the relationship between certificate types, certificate definitions, and certificate definition policies.

In Security Manager Administration, you assign certificate types to a user in the **New User** dialog box. See [“To register new entries with Security Manager Administration” on page 268](#) for further information on assigning a certificate type to an end user.

Automatic additional certificate download

Security Provider for Windows includes the **Automatic Additional Certificate Download** feature to make CA certificate distribution transparent and automatic.

With this feature, Security Provider for Windows automatically retrieves intermediate certificates, CA link certificates, and cross-certificates from the directory configured with your Security Manager product. All these certificates are placed in the Intermediate CA certificate store.

Note: CA root certificates are not retrieved.

The certificates are then cached in the Intermediate CA certificate store.

How Security Manager's certificates are downloaded

Security Provider for Windows connects to the directory of each of your configured Security Manager CAs. The CA entry is located in the directory and the cross-certificates and link certificates are imported into the user's (or computer's) Intermediate CA store.

Where CA certificates are stored

The type of Entrust digital ID, user or computer, determines where to store the cross-certificates and link certificates:

- Entrust user digital ID
The cross-certificates and link certificates are stored in the current user (HKEY_CURRENT_USER) physical registry intermediate store.
- Entrust computer digital ID and Windows services digital ID
The cross-certificates and link certificates are stored in the local machine (HKEY_LOCAL_MACHINE) physical registry intermediate store.

When CA certificates are downloaded

The automatic additional certificate download is invoked:

- immediately following enrollment
- when the CA has rolled over
- at configurable intervals, as defined by the `RetrieveExtraCertsInterval` setting

For details, see ["Certificate path discovery, validation, download, and extensions settings"](#) on page 470

Entrust Desktop Solutions migration

Entrust Desktop Solutions (EDS) is another, older, Entrust product that enables managed, Entrust digital IDs. When Entrust Desktop Solutions users start using newer Security Provider, users' Entrust digital IDs are migrated automatically from EDS to Security Provider. This migration involves Security Provider taking over management of the ID, and putting the user's cryptographic information in the correct locations and formats.

Note: This migration only occurs for users with Entrust security stores (.epf files).

Topics in this section:

- [“What is migrated?” on page 101](#)
- [“Disabling automatic migration” on page 103](#)
- [“Migrating smart cards from EDS to Security Provider” on page 103](#)
- [“Using smart cards on EDS after migration” on page 104](#)

What is migrated?

Aside from the digital ID itself, the following additional items are migrated:

- [“Address book \(PAB\)” on page 101](#)
- [“Recipient lists \(ERLs\)” on page 102](#)

Address book (PAB)

Entrust Desktop Solutions users may possess a personal address book (.pab file) that contains a collection of certificates for people that the user explicitly trusts. In a Microsoft CryptoAPI environment, a user instead stores these certificates in the Trusted People certificate store. Security Provider for Windows migrates the certificates from a PAB when the user logs in to their Entrust security store. At every Entrust security store login, if a modified PAB is found, the new certificates in the PAB are migrated to the appropriate Microsoft certificate store.

Users can manually import a PAB (see [“About manual address book migration” on page 102](#)).

For both automatic and manual PAB import, Security Provider puts the imported certificates into the user's Trusted People certificate store by default. Administrators can set the `ExportPABToOtherPeopleStore` registry key to have Security Provider for Windows always migrate certificates to the Other People store instead of the Trusted People store. (See [“Entrust Certificate Explorer settings” on page 463](#).)

Whatever store you select, Security Provider removes duplicate certificates in the other store.

When the certificate exported from the PAB is an intermediate certificate, the certificate is imported into the Intermediate Certification Authority (CA) store.

When the certificate exported from the PAB is a root certificate and this root certificate does not exist in the root store, Security Provider for Windows displays a dialog box explaining that Microsoft will display a message to allow the root certificate to be imported into the Trusted Root certificate store.

Attention: If an error occurs during the migration of an Entrust address book to the certificate store, a warning-level log is written to the `logfile.xml` file. An error-level log is never used by this feature, since the Entrust security store login always completes regardless of whether the migration was successful.

About manual address book migration

Users can manually import the contents of a personal address book (.pab) file using the Certificate Explorer. This allows users to manually import addresses from Entrust Desktop Solutions. An administrator must enable the feature using the `EnableEntrustPABImport` registry setting. (See [“Entrust Certificate Explorer settings” on page 463.](#))

When enabled, the menu option **Import Entrust Address Book** appears under **File > Import** in the Certificate Explorer. This option opens a wizard. The wizard also appears when the user double-clicks a .pab file.

Recipient lists (ERLs)

Entrust Desktop Solutions users may have Entrust recipient lists stored in an .erl file. These recipient lists are used to encrypt information for a given set of users on a recurring basis. The recipient lists fulfill the same function as Personal Encryption Groups do in Security Provider. For more information on Personal Encryption Groups, see [“File Security application” on page 202.](#)

When a user logs in using the **Entrust Security Store Login** dialog box, Security Provider migrates the user's .erl file to Personal Encryption Groups. After the migration, when the user tries to encrypt a file, the recipient lists appear as Personal Encryption Groups in the file encryption wizard. At every Entrust security store login, if a modified .erl file is found, the .erl file is migrated to a Personal Encryption Group.

When the user's Entrust security store is located at the Entrust Authority Roaming Server, Security Provider for Windows will request the ERL at the same time as the Entrust security store from the Roaming Server.

Attention: If an error occurs during the migration of the .erl file, a warning-level log is written to the logfile.xml file. An error-level log is never used by this feature, since the Entrust security store login always completes regardless of whether this migration was successful.

About the manual recipient list migration

Users can manually import an Entrust recipient list (ERL), a shared recipient list (SRL), or a Personal Encryption Group (PEG) using the Certificate Explorer. This allows users to manually migrate groups from Entrust Desktop Solutions. An administrator must enable these features using the ShowPersonalEncryptionGroups registry setting. (See “[Entrust Certificate Explorer settings](#)” on page 463.)

When enabled, the menu option **Import Encryption Groups** appears under **File > Import** in the Certificate Explorer. This option opens a wizard. The wizard also appears when the user double-clicks an .eepeg file.

If an imported group was a shared group originally, it does not retain its shared status once imported.

About the manual export of a PEG

Once the ability to import a recipient list or a Personal Encryption Group is made available in the Certificate Explorer, the user can also export any Personal Encryption Group to an .eepeg file. This allows users to pass encryption groups to other Security Provider users.

When enabled, the menu option **Export Personal Encryption Group** appears under **File > Import** in the Certificate Explorer. This option opens a wizard.

Disabling automatic migration

You can disable the automatic migration of users' Entrust digital IDs (.epf files) to Security Provider using the DisableAutomaticEntrustSecurityStoreUpgrade registry setting. For more information on this setting, including its effect on the user's key history, see page 377.

Unless you have a unique and specific need to prevent the migration, Entrust recommends that this setting be left at its default (enable the migration). For details, see page 377.

Migrating smart cards from EDS to Security Provider

Smart card digital IDs created with Entrust Desktop Solutions (EDS) are not automatically migrated. To perform a smart card migration, users must run the smart card migration utility, available for download from <https://secure.entrust.com/trustedcare>. (You need a username and password to

access the site. This information was provided in a customer letter.) The migration process is as follows.

To migrate a smart card from EDS to Security Provider

- 1** A user (Bob) installs Security Provider on his computer.
- 2** On this computer, Bob inserts his smart card, which contains his EDS digital ID.
- 3** Bob runs the smart card migration utility, which makes the digital ID compatible with Security Provider.

Specifically, the migration utility:

- downloads Bob's private key history from the CA
- places his keys and certificates in the appropriate Microsoft security stores, where Security Provider expects them

All this occurs without requiring Bob to recover his digital ID. (Note that a recovery does occur; however, it is performed silently, by the migration utility, without Bob needing to enter activation codes.)

After completing [Step 3](#), Security Provider can successfully manage the user's smart card digital ID.

Note: By default this plug-in is configured for SafeNet smart cards. See the utility's documentation for more information.

Using smart cards on EDS after migration

Security Provider includes a feature that lets smart card users continue to use EDS after migrating to Security Provider. For details, see ["Using smart cards with Security Provider and EDS" on page 185](#).

Importing and exporting the Entrust key file

Through the Certificate Explorer, users can import or export an Entrust key file. This file allows you to move certificates between Security Provider and Entrust Desktop Solutions.

A .key file contains an encryption certificate, a signing certificate, and a CA certificate. The Certificate Explorer imports the CA certificate into the Intermediate Certification Authorities store or the Trusted Root Certification Authorities store, depending on whether the certificate is self-signed.

Security Provider validates all aspects of the certificates before importing or exporting them.

Importing certificates from an Entrust key file

Users can manually import a recipient's encryption certificate into the Trusted People store using the Certificate Explorer. This lets users encrypt files or messages for that recipient. An administrator must enable the feature using the `EnableEntrustKeyImport` registry setting. (See ["Entrust Certificate Explorer settings" on page 463.](#))

When enabled, the menu option **Import Certificates from Entrust Key File** appears under **File > Import** in the Certificate Explorer. This option opens a wizard. The wizard also appears when the user double-clicks a .key file.

Certificate Explorer does not import the recipient's signing certificate from a .key file.

Exporting a certificate to an Entrust key file

Users can manually export a recipient's encryption certificate to a .key file. This allows users to pass encryption certificates to other Security Provider users. An administrator must enable the feature using the `EnableEntrustKeyExport` registry setting. (See ["Entrust Certificate Explorer settings" on page 463.](#))

When enabled, the menu option **Export Certificates to Entrust Key File** appears under **File > Export** in the Certificate Explorer. This option opens a wizard.

Users can export just one encryption certificate at a time.

Configuring an enrollment station

You can configure a computer to be used as an enrollment station. You can use the `EnrollmentStation` setting to prevent certificates from being copied into the user's local Personal certificate store.

When using an enrollment station, a user can enroll using the Entrust Enhanced Cryptographic Provider or a smart card vendor's CSP.

See ["Miscellaneous settings" on page 484](#) for further information on configuring this feature.

Entrust Enhanced Cryptographic Provider

When a user enrolls to the Entrust Enhanced Cryptographic Provider, their keys and certificates are copied into their Entrust security store.

If a user is a desktop user, they must copy their Entrust security store `.epf` file onto a disk or perform some other secure means of getting this `.epf` to their own machine.

If the user enrolls as a roaming user, their certificates and keys are located in the directory. When the user returns to their own computer and connects to the Roaming Server, they can log in as a roaming user with their keys and certificates found in the directory. Once the user logs in to their Entrust security store as a desktop or roaming user, their certificates are copied to the local certificate store.

Smart card vendor Cryptographic Service Provider (CSP)

When a user enrolls to a smart card vendor's CSP, the certificates are copied onto the smart card. Once the user returns to their own computer and inserts the smart card into the reader, the certificates are copied to the local certificate store.

Note: Depending on the smart card in use, propagation of certificates from the smart card to the local certificate store may behave differently. Some smart card vendors only propagate one certificate to the local certificate store, while others propagate all certificates. For more information about certificate propagation, contact your smart card vendor.

Attention: If a user tries to use an enrollment station to enroll using a Microsoft CSP, the enrollment fails. (This is because Microsoft CSPs place their certificates in the local certificate store only.) An error message appears and the activation codes that the user attempted to use are no longer valid.

Adding and using the Entrust computer digital ID snap-in

The Entrust computer digital ID snap-in integrates with the Microsoft Management Console (MMC). It provides a GUI through which to view and manage Entrust computer digital IDs on local or remote computers.

See the following sections for details on the Computer Digital ID snap-in:

- [“Computer Digital ID snap-in functionality” on page 107](#)
- [“Adding the Entrust Digital ID” on page 107](#)
- [“Viewing and managing computer digital IDs” on page 111](#)
- [“Viewing event logs for computer digital IDs” on page 112](#)

Computer Digital ID snap-in functionality

Through the snap-in, you can perform the following tasks:

Task	Instructions
View all the certificates on a local or remote computer.	“To view, update or recover computer digital IDs” on page 111
Manually start an enrollment or recovery of an Entrust computer digital ID on a local or remote machine.	
Manually start a check for updates for an Entrust computer digital ID on a local or remote computer.	
View all the events for the Entrust computer digital ID. You can view the event log to determine if enrollment, recovery, or updates are successful.	“To view the event logs for computer digital IDs” on page 113

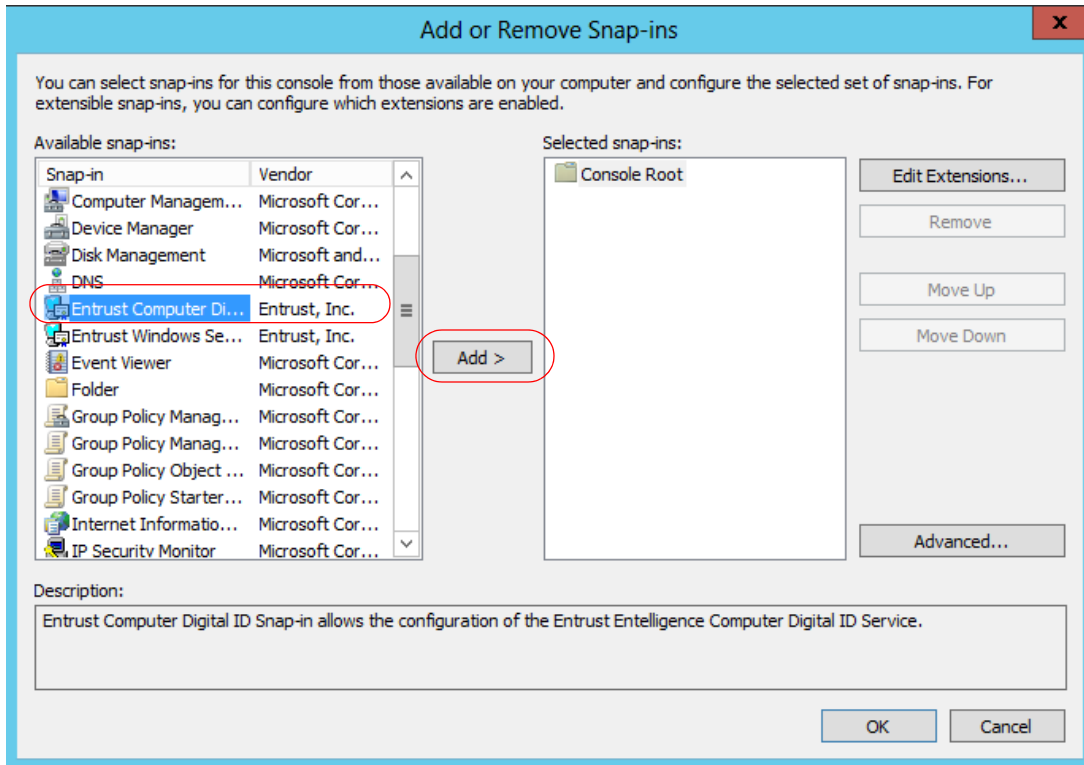
Adding the Entrust Digital ID

The snap-in is installed as an optional module when you install Security Provider using the custom installation wizard. You must add the Computer Digital ID snap-in before you can use it to view certificates and perform management tasks.

To add the Computer Digital ID snap-in

- 1 Open a command prompt (or in older Windows systems, from the **Start** menu, select **Run**).

- 2 Type MMC.
The Microsoft Management Console appears.
- 3 In the **Console** dialog box, select **File > Add or Remove Snap-in**. The **Add or Remove Snap-in** dialog box appears.



- 4 Scroll down and select the **Entrust Computer Digital ID Snap-in**.
- 5 Click **Add**.
The **Select Computer** page appears.

- 6 Select the computer you want the Entrust Computer Digital ID snap-in to manage, by choosing one of the following:

Select Computer

Select the computer you want this Snap-in to manage.

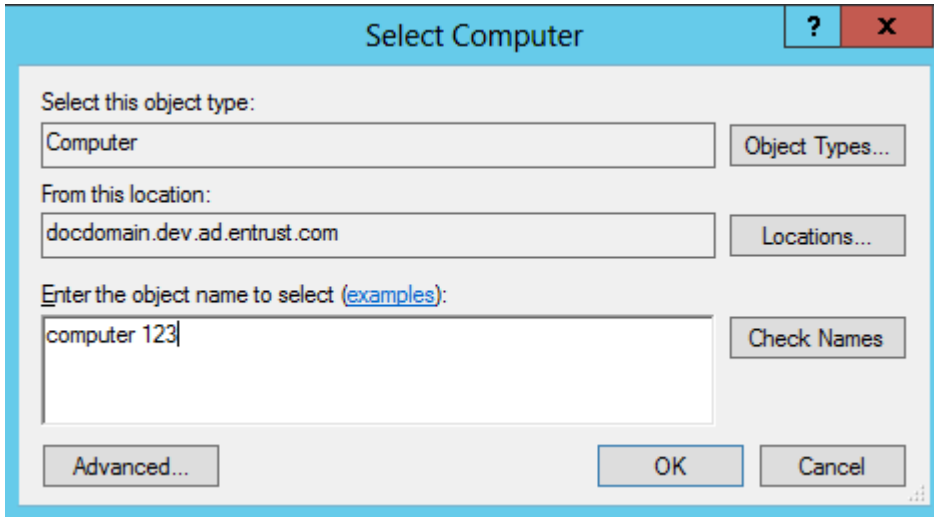
This snap-in will always manage:

☒ Local computer: (the computer this console is running on)

☐ Another computer:

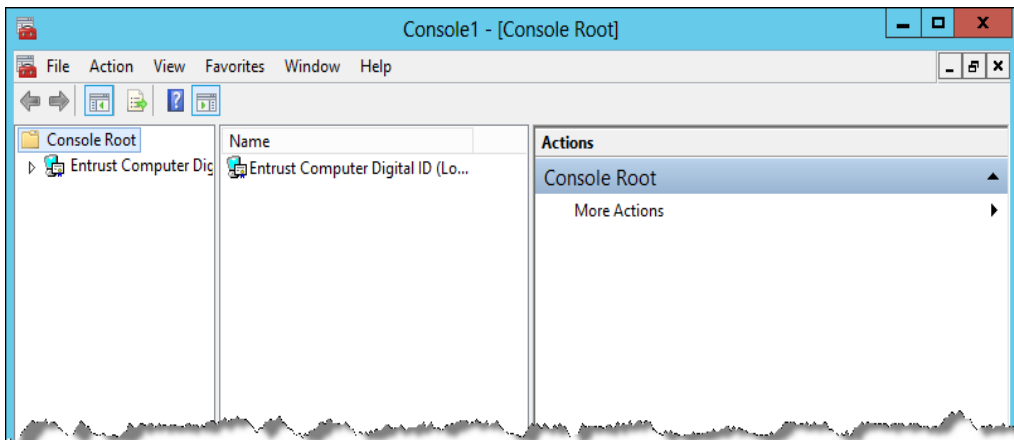
- If you are working from the computer where the digital ID being managed by the snap-in will be stored, select **Local computer** and click **Finish**.

- If you are working remotely, select **Another computer** and browse to the desired location (domain and computer):



Use the **Check Names** tool to be sure that you have entered a the computer name correctly. Click **OK** and then **Finish** to save your configuration. The **Advanced** option allows you to list the computers presently visible in the domain. See the Microsoft Management Console online help, from the ? (help) menu, for more information, if required.

- 7 Click **OK** on the **Add or Remove Snap-in** dialog box. The snap-in appears.



The following two steps are optional.

- 8 When the console tree on the left-hand pane displays the **Entrust Computer Digital ID** option under the **Console Root** folder, select **File > Save**.
- 9 Choose a file name for your MSC file and click **Save**.

You have successfully added the Entrust Computer Digital ID snap-in.

Viewing and managing computer digital IDs

Add the Entrust Windows service Digital ID snap-in, as described in [“To add the Computer Digital ID snap-in” on page 107](#) and enroll a certificate, as described in [Table 10 on page 65](#) before starting this procedure. Follow the steps below to view, update, or recover a Windows service digital ID.

To view, update or recover computer digital IDs

- 1 Do one of the following:
 - Add the Entrust Computer Digital ID snap-in, as described in [“To add the Computer Digital ID snap-in” on page 107](#).
 - Open the Microsoft Management Console and open the Entrust Computer Digital ID snap-in .msc file.
- 2 In the tree view on the left, do one or all of the following:
 - Expand each node to reveal the appropriate certificates (Figure 9).
 - Click **More Actions** and select the appropriate management option (Figure 10).

For details on enrolling and recovering Entrust digital IDs for computers, see [“Manual enrollment and recovery for computer digital IDs” on page 73](#).

Figure 9: Certificates in the Computer Digital ID Snap-In

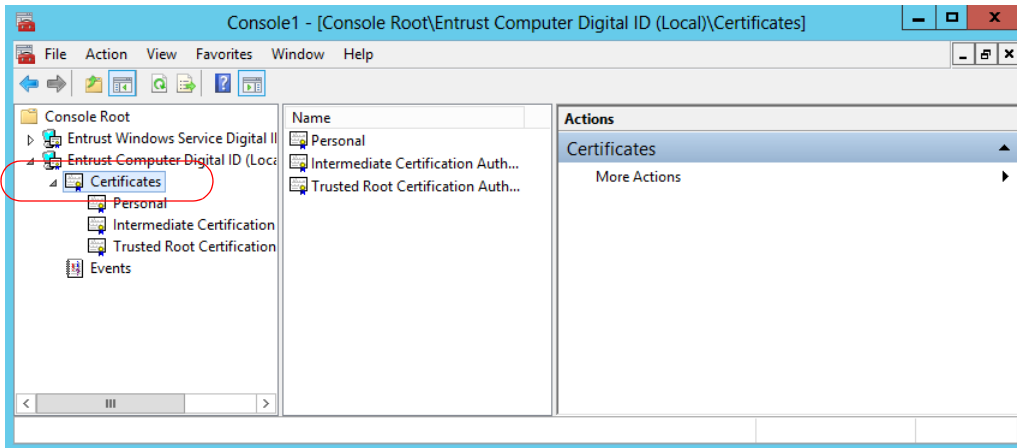
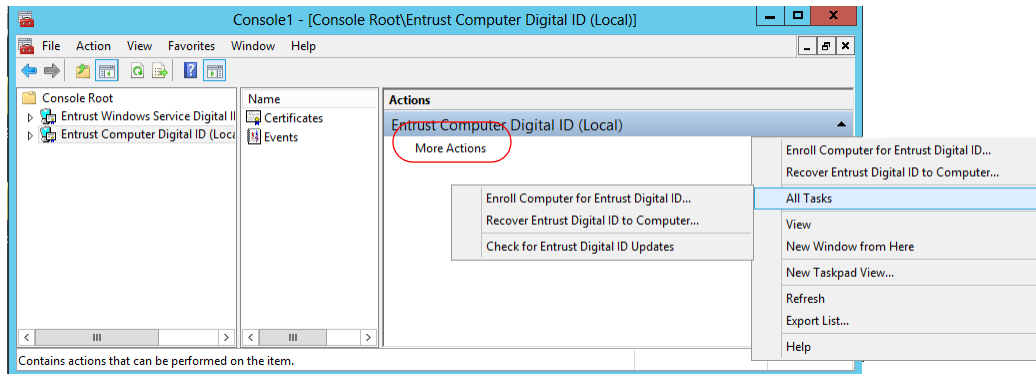


Figure 10: Management options in the Computer Digital ID Snap-In



Viewing event logs for computer digital IDs

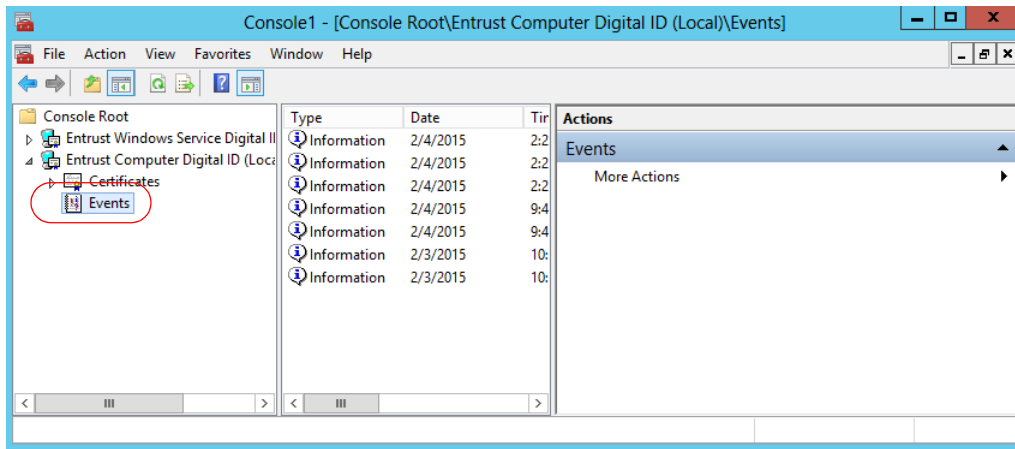
Add the Entrust Windows service Digital ID snap-in, as described in [“To add the Computer Digital ID snap-in” on page 107](#) and enroll a certificate, as described in [Table 10 on page 65](#) before starting this procedure. Follow the steps below to view, update, or recover a Windows service digital ID.

Because Security Provider performs management tasks on computer digital IDs silently, the only way to know whether the task was successful is to view the event logs.

To view the event logs for computer digital IDs

- 1 Do one of the following:
 - Run the Entrust Computer Digital ID snap-in, as described in [“To add the Computer Digital ID snap-in” on page 107](#).
 - Open the Microsoft Management Console and open the Entrust Computer Digital ID snap-in .msc file.
- 2 In the tree view on the left, click **Events** to display the event logs for the Computer Digital ID Service (Figure 11).

Figure 11: Events in the MMC console



Adding and using the Entrust Windows services digital ID snap-in

The Entrust Windows Services Digital ID snap-in integrates with the Microsoft Management Console (MMC). It provides a GUI through which to view and manage Entrust Windows services digital IDs on local or remote computers.

See the following sections for details on the Windows services Digital ID snap-in:

- [“Windows service Digital ID snap-in functionality” on page 114](#)
- [“Adding the Digital ID snap-in” on page 114](#)
- [“Viewing and managing Windows service digital IDs” on page 118](#)
- [“Viewing event logs for Windows service digital IDs” on page 120](#)

Windows service Digital ID snap-in functionality

Through the snap-in, you can perform the following tasks:

Task	Instructions
View all the certificates on a local or remote computer.	“To view, update or recover Windows service digital IDs” on page 118
Manually start an enrollment or recovery of an Entrust Windows services digital ID on a local or remote machine.	
Manually start a check for updates for an Entrust Windows services digital ID on a local or remote computer.	
View all the events for the Entrust Windows services digital ID. You can view the event log to determine if enrollment, recovery, or updates are successful.	“To view the event logs for Windows service digital IDs” on page 120

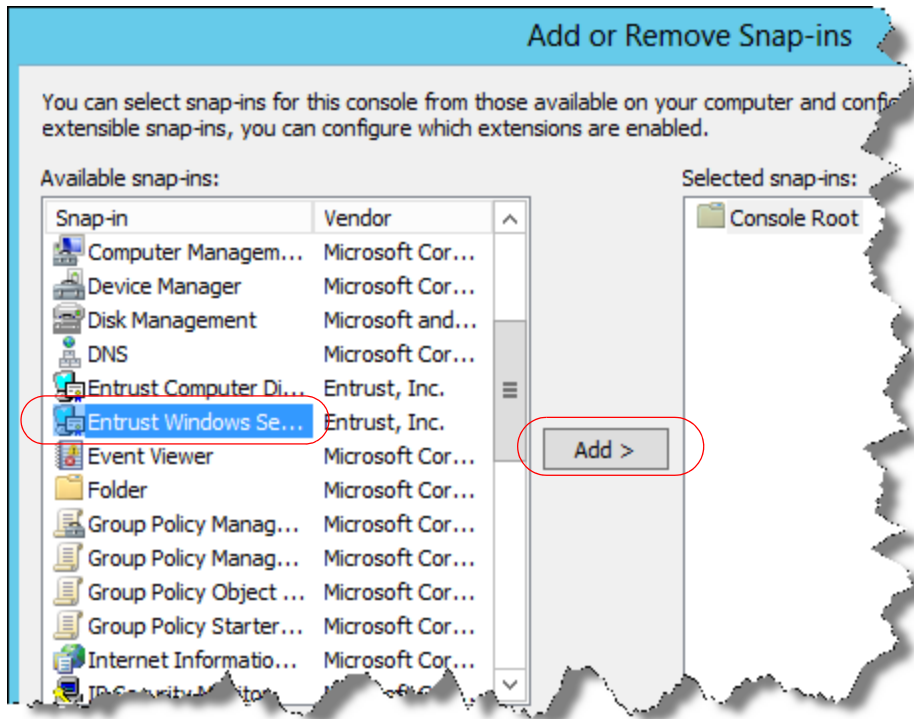
Adding the Digital ID snap-in

The snap-in is installed as an optional module when you install Security Provider using the custom installation wizard. You must add the Entrust Windows services Digital ID snap-in before you can use it to view certificates and perform management tasks.

To add the Entrust Windows services Digital ID snap-in

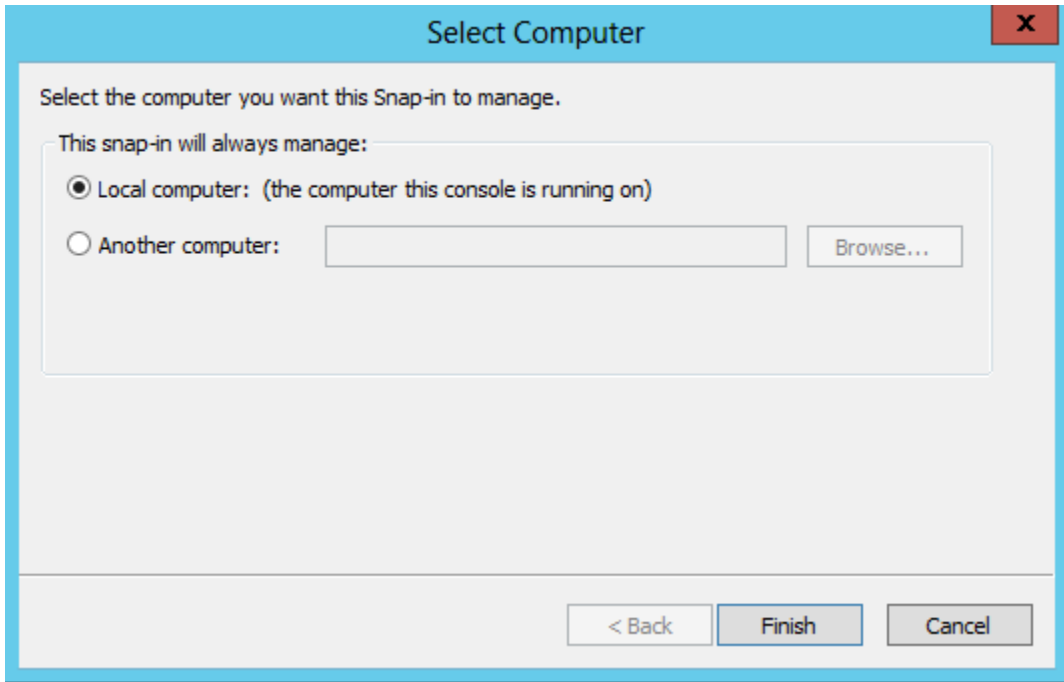
- 1 Open a command prompt (or in older Windows systems, from the **Start** menu, select **Run**.).

- 2 Type MMC.
The Microsoft Management Console appears.
- 3 In the **Console** dialog box, select **File > Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog box appears.



- 4 Select **Entrust Windows Service Digital ID** and click **Add**.

The **Select Computer** page appears.



Select Computer

Select the computer you want this Snap-in to manage.

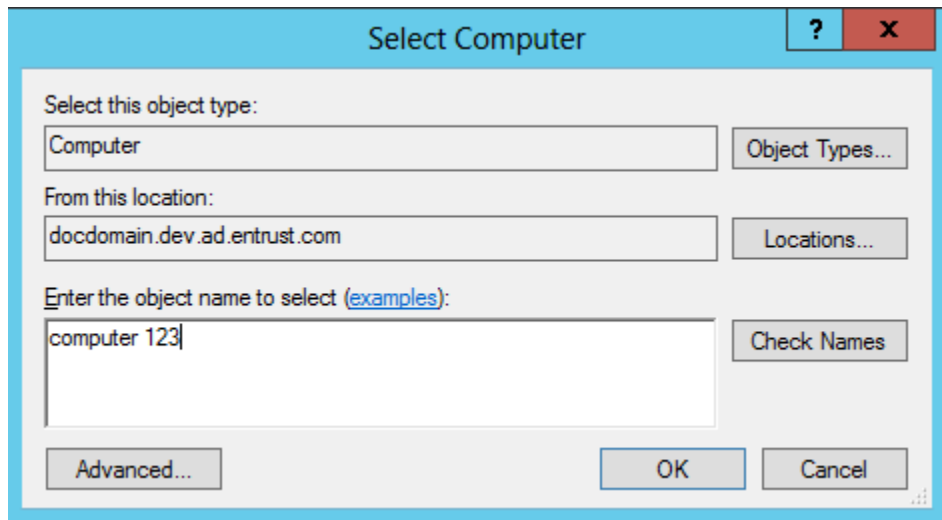
This snap-in will always manage:

☒ Local computer: (the computer this console is running on)

☐ Another computer:

- 5 Select the computer where the digital ID being managed will be stored:
 - If you are working from the computer where the digital ID being managed by the snap-in will be stored, select **Local computer** and click **Finish**.

- If you are working remotely, select **Another computer** and browse to the desired location (domain and computer):

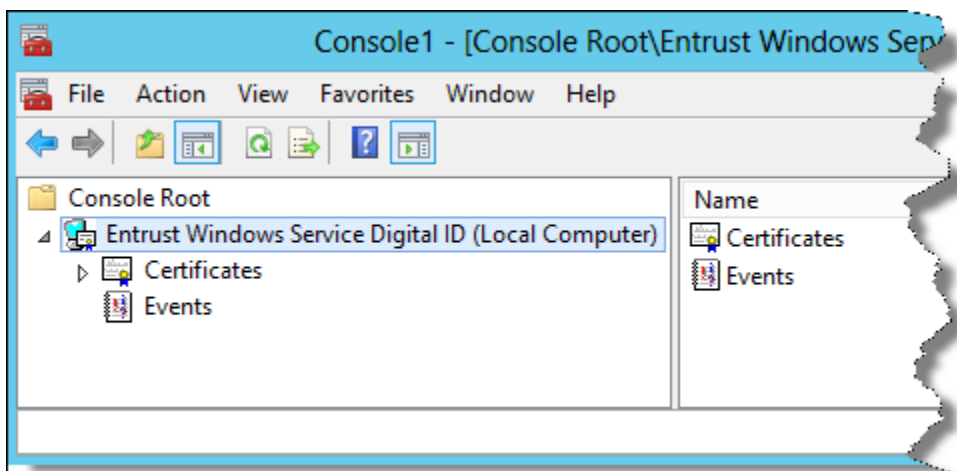


The 'Select Computer' dialog box has a title bar with a question mark and a close button. It contains three main sections: 'Select this object type:' with a dropdown set to 'Computer' and an 'Object Types...' button; 'From this location:' with a text field containing 'docdomain.dev.ad.entrust.com' and a 'Locations...' button; and 'Enter the object name to select (examples):' with a text field containing 'computer 123' and a 'Check Names' button. At the bottom are 'Advanced...', 'OK', and 'Cancel' buttons.

Use the **Check Names** tool to be sure that you have entered the computer name correctly. Click **OK** and then **Finish** to save your configuration. The **Advanced** option allows you to list the computers presently visible in the domain. See the Microsoft Management Console online help, from the ? (help) menu, for more information, if required.

- 6 Click **OK** on the **Add or Remove Snap-in** dialog box.

The Entrust Windows Service Digital ID snap-in appears in the console.



7 Optionally, you can choose to save your MSC file under a different name. To do so:

- a** Under the **Console Root** folder, select **File > Save as**.
- b** Choose a file name for your MSC file and click **Save**.

You have successfully added the Entrust Windows services digital ID snap-in.

Viewing and managing Windows service digital IDs

Add the Entrust Windows service Digital ID snap-in, as described in [“To add the Entrust Windows services Digital ID snap-in” on page 114](#) and enroll a certificate, as described in the procedure [“Manual enrollment and recovery for Windows Services” on page 76](#) before starting this procedure. Follow the steps below to view, update, enroll, or recover a Windows service digital ID.

To view, update or recover Windows service digital IDs

- 1** Open the Microsoft Management Console and open the Entrust Windows service Digital ID snap-in .msc file.
- 2** In the tree view on the left, do one or all of the following:
 - Expand each node to reveal the appropriate certificates (Figure 12).
 - Click **More actions** under **Entrust Windows Service Digital ID** and select the appropriate management option (Figure 10).

For details on enrolling and recovering Entrust digital IDs for Windows services, see [“Manual enrollment and recovery for Windows Services” on page 76](#).

Figure 12: Certificates in the Windows service Digital ID Snap-In

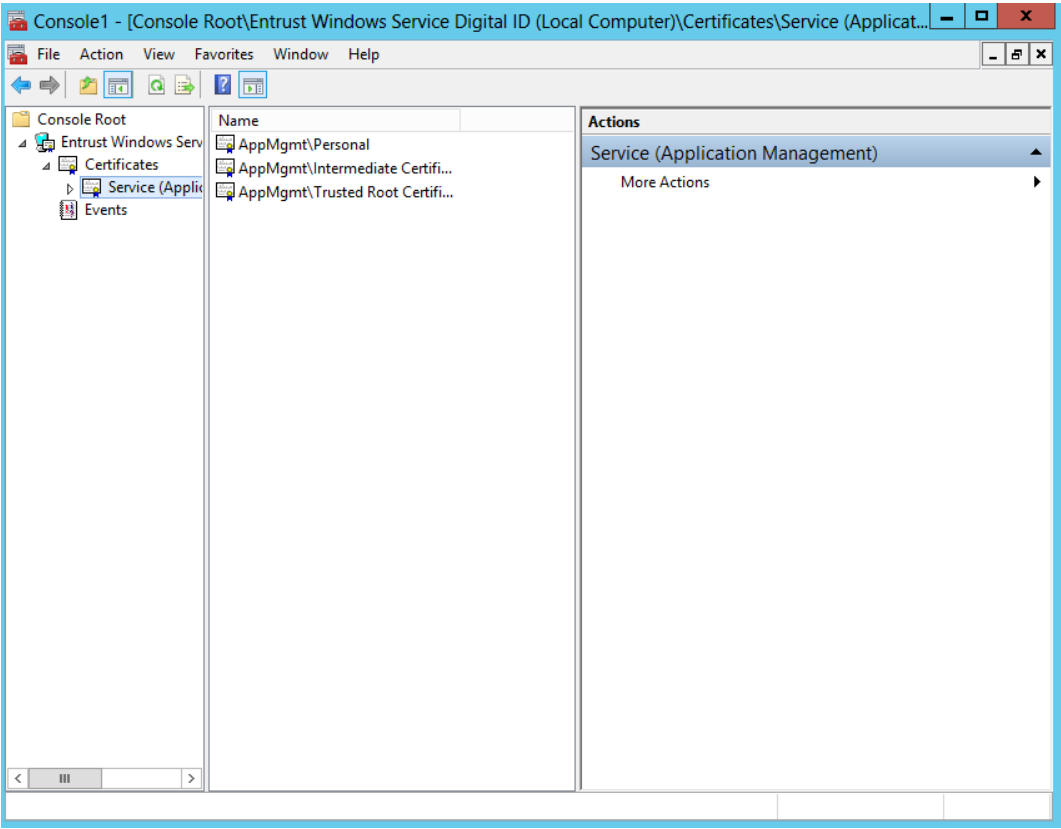
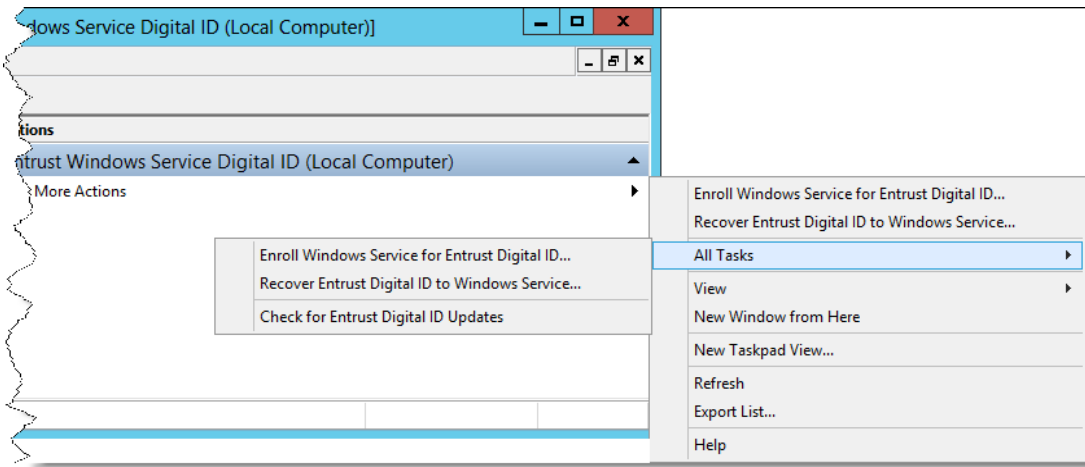


Figure 13: Management option in the Windows service Digital ID Snap-In



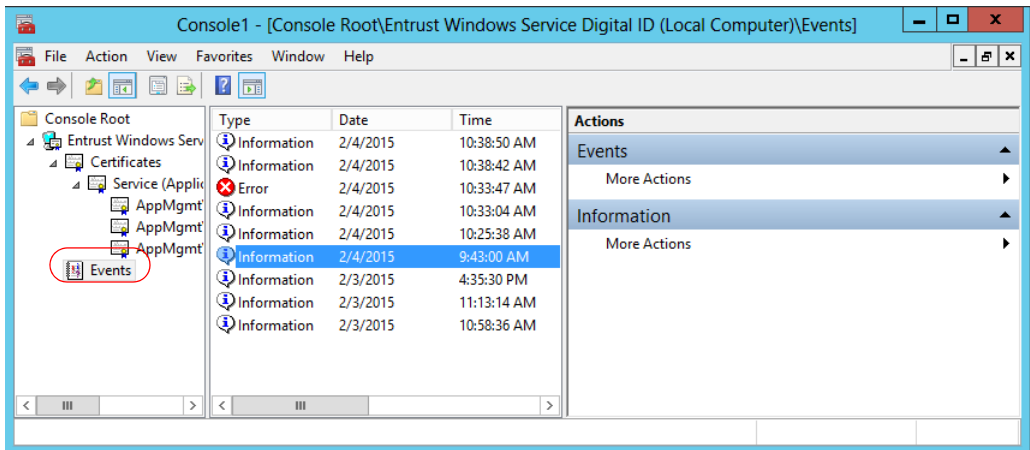
Viewing event logs for Windows service digital IDs

Add the Entrust Windows service Digital ID snap-in, as described in [“To add the Entrust Windows services Digital ID snap-in” on page 114](#) and enroll a certificate, as described in the procedure [“Manual enrollment and recovery for Windows Services” on page 76](#) before starting this procedure. Follow the steps below to view, update, or recover a Windows service digital ID.

To view the event logs for Windows service digital IDs

- 1 Open the Microsoft Management Console and open the Entrust Windows Service Digital ID snap-in .msc file.
- 2 In the tree view on the left, click **Events** to display the event logs for the Digital ID Service (Figure 14).

Figure 14: Events in the MMC console



CryptoAPI enhancements

Security Provider can enhance native CryptoAPI capabilities. These enhancements do not require an Entrust CA, and in some cases, do not even require a digital ID.

For developer-level information on the CryptoAPI capabilities of Security Manager, consult the Security Provider for Windows white paper library available on the Entrust TrustedCare Web site at <https://www.entrust.com/trustedcare/>. You must have a user name and password to access the site.

The following CryptoAPI enhancements are available:

- “Importing keys into an Entrust security store” on page 124
- “Entrust Cryptographic Service Providers” on page 129
- “CRL Revocation Provider” on page 136
- “OCSP Revocation Provider” on page 139
- “Certificate path discovery, validation, and extension checking” on page 141

Importing keys into an Entrust security store

Security Provider allows third-party CryptoAPI applications to import keys and certificates into a desktop Entrust security store (.epf file). These third-party keys and certificates are not managed by Entrust nor are they compatible with Entrust applications other than Security Provider.

The following existing functionality (available through Microsoft CryptoAPI-enabled applications) can import keys to Entrust security stores (although any CryptoAPI application can include functionality to perform the import):

- Microsoft auto-enrollment
- Microsoft Web enrollment
- MMC Certificate Snap-in enrollment

See the following sections for details on the import:

- [“About the import process” on page 124](#)
- [“Enabling the import” on page 126](#)

About the import process

The following steps describe how a third-party application and Security Provider work together to import keys and certificates into an Entrust security store.

1 A third-party CryptoAPI application either:

- imports pregenerated keys and certificates to the Entrust Enhanced Cryptographic Service Provider, or
- asks the Entrust Enhanced Cryptographic Service Provider to generate them

These keys and certificates can be signed by a non-Entrust CA such as the Microsoft CA.

The import can be accomplished in two ways:

- The third-party application can display a dialog box asking the user to choose a CSP. The user then selects the Entrust Enhanced Cryptographic Service Provider and the third-party application imports the keys and certificates to it.
- The third-party application can import the keys and certificates programmatically to the Entrust Enhanced Cryptographic Service Provider, without displaying dialog boxes to users.

2 After the key import, the Entrust Enhanced Cryptographic Service Provider detects that the keys are from a third-party application and displays the following dialog box to the user.



- 3 Assuming the user selects **Create a new Entrust security store**, Security Provider displays a wizard, which prompts users to select a name and password for their Entrust security store.
- 4 When users finish stepping through the wizard, the Entrust Enhanced Cryptographic Service Provider:
 - a places the private keys into key containers
 - b adds the key containers and public key certificates to an Entrust security store that is formatted specifically for keys and certificates from a non-Entrust product
- 5 The third-party CryptoAPI application adds the public key certificates to the Microsoft certificate store. These certificates point to the corresponding private key container name.
- 6 If the third-party application needs to store new keys in an Entrust security store, users are again presented with the **Import a New Key** dialog box. This time, they can select **Add to an existing Entrust security store** to add their keys and certificates to an existing generic-formatted Entrust security store.
- 7 After the import, whenever the Entrust security store is accessed, Security Provider displays the login dialog box where users must specify their password. The Entrust security store can be accessed:
 - by the user
The user can right-click the Security Provider taskbar status icon and select **Log In**.
 - by a CryptoAPI application such as Security Provider, when it needs to perform a cryptographic operation

Enabling the import

The following instructions describe how to enable and customize the import of keys and certificates into an Entrust security store. You can use either the **Custom Installation** wizard or Microsoft Group Policy to enable the import.

- [“Preconfiguration step” on page 126](#)
- [“To enable and customize the import using the wizard” on page 126](#)
- [“To enable and customize the import using Group Policy” on page 127](#)

Preconfiguration step

Ensure that your third-party application imports pregenerated keys and certificates to the Entrust Enhanced Cryptographic Service Provider (CSP).

You can enable this import programmatically, without displaying dialog boxes to users. Alternatively, you can display a dialog box asking users to choose the Entrust Enhanced CSP.

To enable and customize the import using the wizard

- 1 Run through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#). Fill out the pages related to Entrust security stores, as described below.

On this page in the wizard...	Do this...
Select Application Features	Enable the Entrust Security Store option, and optionally, its subfeatures. Disable the Entrust digital ID option, unless you want to also provide managed, Entrust digital IDs to your users. Disabling Entrust digital IDs hides the Enroll and Recover options in the taskbar because this functionality requires an Entrust CA.
Entrust Security Store Login Options	Fill out the check boxes and fields as described in “Entrust security store login settings” on page 396 . Note: Entrust Roaming Security store options are ignored. Only Desktop security stores (.epf files) can contain keys and certificates whose creation is initiated by a non-Entrust application.
Entrust Security Store Login Options > Customize Links	On the Login , Unlock , and ReAuthenticate tabs, select either Generic Certification Authority , or Custom . If you select Custom , specify your custom links. For details, see “Entrust security store login settings” on page 396 .
Entrust Security Store Creation Options	Fill out the fields and check boxes as described in “Entrust security store creation settings” on page 405 .

On this page in the wizard...	Do this...
Entrust Security Store Creation Options > Advanced	Set your policy by filling out the fields on the Advanced page. These settings are described at the end of “Entrust security store creation settings” on page 405 .
Entrust Security Store Startup and Shutdown Options	Fill out the check boxes as described in “Entrust security store startup and shutdown settings” on page 416 .

- 2** Proceed to the end of the wizard and click **Finish** to save your settings.
The .mst file is updated with your new Entrust security store settings.
- 3** Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).
You have selected and customized Entrust security stores. Your third-party application can now import keys into the Entrust security store.

To enable and customize the import using Group Policy

- 1** Run through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#) until you reach the **Select Application Features** page and do the following:
 - a** Enable the **Entrust Security Store** option, and optionally, its subfeatures.
 - b** Disable the **Entrust digital ID** option, unless you want to also provide managed, Entrust digital IDs to your users. Disabling Entrust digital IDs hides the **Enroll** and **Recover** options in the taskbar. (Enrollment is available but only when a third-party application initiates it.)

Note: The settings above are not configurable through Group Policy.

- 2** Proceed to the end of the wizard and click **Finish** to save your settings.
The .mst file is updated with your new Entrust security store settings.
You can now specify the rest of the Entrust security store-related settings through Group Policy, as described in [Step 3](#) in this procedure.
- 3** Specify additional Entrust security store settings listed in the following sections:
 - [“Entrust security store login settings” on page 396](#).
 - [“Entrust security store creation settings” on page 405](#)
 - [“Entrust security store startup and shutdown settings” on page 416](#)

Note: Do not set Entrust roaming security store settings. Only desktop security stores (.epf files) can contain keys and certificates whose creation is initiated by a non-Entrust application.

- 4** Push out your settings to your users through Group Policy to have the new registry values written to each user's registry.
- 5** If you changed settings through the **Custom Installation** wizard, package, test, and distribute the installation to your users. For details, see ["Deploying Security Provider for Windows" on page 281](#).

You have selected and customized Entrust security stores. Your third-party application can now import keys into the Entrust security store.

Entrust Cryptographic Service Providers

Security Provider includes several Cryptographic Service Providers (CSPs) that it uses to perform cryptographic operations. Other CryptoAPI applications can use these CSPs as well.

These CSPs are included when users install Security Provider:

- [“Entrust Enhanced Cryptographic Service Provider” on page 129](#)
- [“Entrust Symmetric Cryptographic Service Provider” on page 130](#)
- [“Entrust Key Access Service Cryptographic Service Provider” on page 131](#)
- [“Entrust Elliptic Curve Cryptographic Service Provider” on page 132](#)
- [“Entrust Smart Card Cryptographic Provider” on page 133](#)

Cryptographic Service Providers (CSPs) are organized by type. A CSP type is loosely defined by the asymmetric algorithm that the CSP supports. For example, type RSA Full Signature and Key Exchange (called just RSA Full from this point on) requires that all CSPs of that type support RSA public-private key pairs. (The Entrust Elliptic Curve CSP has no relation to RSA Full because it does not store RSA keys.)

It is quite common for multiple types to support the same asymmetric algorithms, though a CSP can belong to only one type. Each type is assigned a default CSP.

Applications built on CryptoAPI can ask for a specific CSP when they begin performing cryptographic operations, or they can use the default CSP on the system for the particular algorithm that they want to use. The default CSP is typically used for public operations, encryption, or signature verification.

Note: The following topics describe the CSPs that Security Provider uses to perform cryptographic operations, including supported algorithms. To set the algorithms Security Provider uses for various features, you must use the Custom Installation Wizard or configure the Windows registry. See [“Security Provider registry settings” on page 327](#) for details.

Entrust Enhanced Cryptographic Service Provider

The Entrust Enhanced CSP contains a FIPS 140-2 compliant security kernel. This CSP is responsible for storage and use of keys and certificates in the Entrust security store (*.epf). When a CryptoAPI application attempts to use these keys and certificates, the Entrust Enhanced CSP conducts the requested cryptographic operation.

Note: Some registry settings affect FIPS 140-2 compliance for Security Provider; see CSPDoNotEnforceRSAPublicKeyExponentLength and CSPEnforceRSAKeyPairLength starting on [page 484](#).

The Entrust Enhanced CSP is of the type RSA Full.

The Entrust Enhanced CSP supports cryptographic advancements, such as:

- Probabilistic Signature Scheme (PSS), a cryptographic padding option for RSA signatures
- Optimal Asymmetric Encryption Padding (OAEP), a cryptographic padding option for RSA keys used to protect a symmetric key or raw data
- AES Galois/Counter Mode (AES-GCM), a cipher mode option used when an AES symmetric key needs to encrypt a data stream

You can have your CryptoAPI application use the Entrust Enhanced CSP to:

- perform cryptographic operations that use the algorithms listed in Table 13
- store keys and certificates in an Entrust security store (.epf file)

For details, see [“Importing keys into an Entrust security store” on page 124](#)

Table 13: Entrust Enhanced Cryptographic Service Provider algorithms

Algorithm type	Supported algorithms
Asymmetric	RSA 1024, 2048, 4096, and 6144-bit
Symmetric	Symmetric DES, Triple-DES CAST 40, 64, 80, and 128-bit IDEA 128-bit AES 128, 192, and 256-bit RC2 40, 56, 64, 128-bit
Hashing	MD2, MD5 SHA-1, SHA 224, SHA 256, SHA 384, SHA 512

Attention: MD5 is not recommended as the underlying signing digest algorithm. For more information see technote [TN 7707](#).

Entrust Symmetric Cryptographic Service Provider

The Entrust Symmetric CSP allows CryptoAPI applications to perform cryptographic operations requiring CAST, IDEA, or AES symmetric keys, in cases where another CSP does not support these algorithms.

The Entrust Symmetric CSP is not type RSA Full, rather it is type Symmetric Algorithms (CAST, IDEA, AES). This is because the Entrust Symmetric CSP does not implement any asymmetric algorithms.

The Entrust Symmetric CSP is designed to be used when encrypting data with the default CSP or when decrypting data with the private key's CSP, in cases where the specified CSP does not support the desired algorithms. Security Provider (or any other CryptoAPI application) uses the Entrust Symmetric CSP to perform the symmetric cryptographic operations and the specified CSP for the asymmetric operations. For example, during a decryption operation, the encrypted symmetric key is decrypted using the specified CSP and then imported to the Entrust Symmetric CSP. The Entrust Symmetric CSP is then used to decrypt the encrypted data.

The Entrust Symmetric CSP can encrypt and decrypt raw data using one of the following algorithms.

Table 14: Entrust Symmetric Cryptographic Service Provider algorithms

Algorithm type	Supported algorithms
Symmetric	Symmetric CAST 40, 64, 80, and 128-bit IDEA 128-bit AES 128, 192, and 256-bit

Note: The Entrust Symmetric CSP is not a standard RSA CSP and is not FIPS 140-2 compliant.

Entrust Key Access Service Cryptographic Service Provider

The Entrust Key Access Service CSP contains a FIPS 140-2 compliant security kernel. This CSP lets CryptoAPI applications access a user's old private keys that no longer exist in a smart card CSP due to smart card size limitations. The keys are protected and managed by the Key Access Service component.

Note: Some registry settings affect FIPS 140-2 compliance for Security Provider; see CSPDoNotEnforceRSAPublicKeyExponentLength and CSPEnforceRSAKeyPairLength starting on [page 484](#).

The Entrust Key Access Service CSP is of type RSA Full.
For more information on the Key Access Service, see [“Additional Entrust digital ID management for smart cards” on page 88](#).

[Table 15 on page 132](#) outlines the key lengths that are supported by the 1024 bit Key Access Service keys. The Key Access Service key length is 1024 bits and cannot be changed.

Table 15: User key algorithms that Entrust Key Access Service Cryptographic Service Provider can secure

Algorithm type	Supported algorithms
Asymmetric	RSA 1024, 2048, 4096, and 6144-bit
Symmetric	Symmetric DES, Triple-DES CAST 40, 64, 80, and 128-bit IDEA 128-bit AES 128, 192, and 256-bit RC2 40, 56, 64, 128-bit
Hashing	MD2, MD5 SHA-1, SHA 256, SHA 384, SHA 512

Note: The Entrust Key Access CSP does not support SHA 224.

Attention: MD5 is not recommended as the underlying signing digest algorithm. For more information see technote [TN 7707](#).

Entrust Elliptic Curve Cryptographic Service Provider

The Entrust Elliptic Curve CSP contains a FIPS 140-2 compliant security kernel. This CSP is used when protecting data with elliptic curve keys.

The Elliptic Curve CSP supports two types of Elliptic Curve Cryptographic (ECC) algorithms:

- ECDSA (Elliptic Curve Digital Signature Algorithm)
- ECDH (Elliptic Curve Diffie-Hellman)

[Table 16 on page 133](#) outlines the supported algorithms.

Table 16: Algorithms that Entrust Elliptic Curve Cryptographic Service Provider can secure

Algorithm type	Supported algorithms
Asymmetric	ECDSA supports elliptic curves p256, p384, and p521 ECDH supports elliptic curves p256, p384, and p521
Symmetric	DES 64-bit 3DES 168-bit CAST3 40 and 64-bit CAST5 40, 64, 80, and 128-bit IDEA 128-bit AES 128, 192, and 256-bit RC2 40, 56, 64, 128-bit
Hashing	MD2, MD5 SHA-1, SHA 256, SHA 384, SHA 512

The Elliptic Curve CSP also supports the CALG_SSL3_SHAMD5 CryptoAPI hashing algorithm.

Entrust Smart Card Cryptographic Provider

The Entrust Smart Card CSP contains a FIPS 140-2 compliant security kernel. This CSP is used when protecting data that comes from or is written to a smart card. This CSP is compatible with Microsoft CAPI. The user's private keys are accessed and protected using the Entrust Smart Card Key Storage Provider.

The Entrust Smart Card CSP supports the following algorithms:

Table 17: Algorithms that the Entrust Smart Card CSP can secure

Algorithm type	Supported algorithms
Asymmetric	RSA 1024, 2048-bit

Table 17: Algorithms that the Entrust Smart Card CSP can secure

Algorithm type	Supported algorithms
Symmetric	DES 64-bit 3DES 168-bit CAST3 40 and 64-bit CAST5 40, 64, 80, and 128-bit IDEA 128-bit AES 128, 192, and 256-bit RC2 40, 56, 64, 128-bit
Hashing	MD2, MD5 SHA-1, SHA-224, SHA 256, SHA 512

Key Storage Providers

Security Provider includes key storage providers (KSPs) that work with some cryptographic providers to allow Microsoft Cryptography API: Next Generation (CNG) and CryptoAPI applications to access users' keys.

Entrust Smart Card Key Storage Provider

The Entrust Smart Card Key Storage Provider (KSP) works with the Entrust Smart Card CSP to provide support for the Cryptography API: Next Generation (CNG).

Security Provider uses the KSP to let CryptoAPI and CNG applications access the functionality provided by the user's private keys stored on a smart card. The KSP lets CNG applications use existing user's keys but does not generate or import the user's keys.

Entrust Enhanced Key Storage Provider

The Entrust Enhanced Key Storage Provider (KSP) works with the Entrust Enhanced CSP, Entrust Elliptic Curve CSP to provide support for the Cryptography API: Next Generation (CNG).

Security Provider uses the KSP to let CryptoAPI and CNG applications access a user's private keys stored in an Entrust security store (.epf). The KSP lets CNG applications use existing user's keys but does not generate or import the user's keys. The Entrust Enhanced CSP and the Entrust Elliptic Curve CSP provide those services.

For Windows operating systems starting with Windows Vista (including the Windows Server 2008 family and above), CNG goes beyond CryptoAPI to provide APIs that make use of advanced cryptographic algorithms, such as ECDSA.

CNG implements the United States government's (NSA) Suite B cryptographic algorithms. These algorithms meet the security of information up to a classification level of Top Secret. CNG is validated to FIPS 140-2.

CRL Revocation Provider

A [certificate revocation list \(CRL\)](#) contains a list of serial numbers of certificates that were revoked and should not be trusted because they are no longer considered valid by the CA that issued them.

Security Provider for Windows enhances Microsoft CryptoAPI's built-in certificate revocation checking capabilities by transparently checking the appropriate CRL when verifying a signature or encrypting information for a recipient. This check confirms that the certificate in question was not revoked. When the CRL Revocation Provider feature is installed, it is run before Microsoft CryptoAPI's certificate revocation functionality.

See the following sections for details on the CRL Revocation Provider:

- [“Supported CRL revocation functionality” on page 136](#)
- [“How CRLs are checked” on page 137](#)

Supported CRL revocation functionality

The following certificate revocation functionality is included:

- The CRL Revocation Provider supports CRL verification specified through the [CRL distribution point \(CDP\)](#) using the directory name format.
- The CRL Revocation Provider supports combined and partitioned CRL verification specified through the CDP using the URL format (supports LDAP, HTTP, FTP, and File protocols).
- The CRL Revocation Provider looks up the AIA extension in a certificate when the certificate and CRL are signed by different CA keys. If the CA information is available, the CRL Revocation Provider retrieves the CA certificates and imports them to the certificate store.
- The CRL Revocation Provider looks up the CRL in a default directory that you choose when PKI data is not available in the registry.
- The CRL Revocation Provider supports the `onlySomeReasons` and `indirectCRL` fields in the Issuing Distribution Point (IDP) as well as the `cRLIssuer` field in the CDP.
- Administrators can assign CRL or OCSP revocation based on the CA in the DN of the certificate. Root certificates and intermediate or cross certificates may be assigned different revocation methods (see [page 420](#) for more information).

For further information on CRLs and how they are managed using Security Manager, see “Certificate revocation lists (CRLs)” in the “About Security Manager” chapter of the *Security Manager Administration User Guide*.

How CRLs are checked

Security Provider retrieves a CRL and then checks whether users' certificates are included in it. If they are included, it means the certificates are revoked, and Security Provider displays a message recommending that the users to whom the certificates belong recover their Entrust digital IDs. Users can still use their digital IDs, but their digital signatures are no longer trusted and certificate updates are no longer performed.

The following steps describe how Security Provider's CRL Revocation Provider retrieves a CRL and checks certificates against it.

- 1 Security Provider fetches a CRL. Security Provider includes an option to always use the directory to perform a CRL check, instead of checking a cached CRL that is located in the local CRL store. See ["CRL Revocation Provider settings" on page 419](#).

When the CRL distribution point (CDP) in the certificate uses a directory name format, Security Provider finds the directory containing the CRL by reading the `Directory` values configured in the user's registry. See ["Directory settings" on page 331](#) for further information on configuring this value.

If you have several Entrust CAs (a cross-certified environment) and want the CRL checker to verify CRLs from each CA, ensure that you configure each CA in the **Entrust PKI Configuration** page of the **Custom Installation** wizard. When you do not configure each CA, your end users cannot verify CRLs that come from another CA. This also applies to all cross-certified environments.

- 2 The CRL Revocation Provider validates the CRL by ensuring that the retrieved CRL is accurate with respect to its scope. The scope of the CRL is determined by the IDP extension in the CRL.
- 3 The CRL Revocation Provider verifies that the signature of the CRL is valid. The CRLs are digitally signed by the CA. The CA's public key is used to verify the CA's signature on the retrieved CRL.
- 4 The CRL Revocation Provider verifies the time validity of the CRL. The lifetime of the CRL is checked to ensure it is still valid.
- 5 The CRL Revocation Provider checks the status of the certificate by looking for the certificate's serial number in the CRL.
 - If the certificate's serial number is found, the certificate is considered revoked.
 - If the certificate's serial number is not found, the certificate is considered valid.
- 6 If the certificate is still considered valid, the CRL Revocation Provider checks the critical extensions in the CRL.
 - If a CRL contains an unrecognized critical extension but the certificate's serial number being validated does not appear in the list of revoked certificates, the

status of the certificate is basically unknown. The CRL Revocation Provider considers the CRL as being invalid and it cannot be used.

When the critical extension in the CRL is considered valid and the serial number does not appear in the CRL as a revoked certificate, the certificate is considered valid.

OCSP Revocation Provider

The Online Certificate Status Protocol (OCSP) enables applications to determine the revocation status of certificates in a more timely manner than CRLs. Security Provider for Windows OCSP Revocation Provider is an OCSP requester that integrates with Microsoft CryptoAPI to provide CryptoAPI-enabled applications with online revocation checking capabilities. When both the OCSP Revocation Provider and CRL Revocation Provider are installed, Security Provider invokes the OCSP Revocation Provider first.

- [“OCSP revocation functionality” on page 139](#)
- [“How OCSP Revocation Provider checks certificates” on page 139](#)

OCSP revocation functionality

The following OCSP Revocation Provider functionality is included:

- support for a variety of available OCSP responders that conform to the OCSP standard, such as, CoreStreet RTC Responder
- provide configurable OCSP responder locations
- accept basic OCSP responses provided by any compliant OCSP responder
- configuring to include a nonce in the OCSP request
- use of HTTP or HTTPS over SSL to exchange OCSP transactions
- support caching of OCSP responses
- verify OCSP responses
- validate the value of the extensions in the OCSP response
- provide logging to write detailed transaction information and binary dumps of OCSP requests and responses to files
- Administrators can assign CRL or OCSP revocation based on the CA in the DN of the certificate. Root certificates and intermediate or cross certificates may be assigned different revocation methods (see [page 426](#) for more information).

How OCSP Revocation Provider checks certificates

When a Microsoft CryptoAPI-enabled application asks CryptoAPI to validate the current status of a certificate and check that it is trusted, CryptoAPI passes the request for validation to the OCSP Revocation Provider.

The following describes how the OCSP Revocation Provider validates a certificate:

- 1** OCSP Revocation Provider constructs a request for the status of a certificate.
- 2** OCSP Revocation Provider determines the OCSP responder to which it will send the request. The responder is discovered through one of the following:

- a URL that you configured
See [“OCSP Revocation Provider settings” on page 425](#).
- a URL that is specified in the Authority Info Access (AIA) extension of the certificate in question
If multiple responder URLs are specified, the OCSP Revocation Provider tries each URL in the order specified in the AIA until a successful response is returned.

- 3** The OCSP Revocation Provider sends the request to the chosen OCSP responder, using HTTP or HTTPS over SSL, and waits for a response. (If you add an application proxy server to your system architecture, you can have the OCSP Revocation Provider communicate through this proxy.) If no response is received, the OCSP Revocation Provider sends the request to the next OCSP responder that it is configured to query.
- 4** If the OCSP Revocation Provider receives a response, the response is validated.
- 5** If the response is valid, the status of the certificate is returned to CryptoAPI.
- 6** Optionally, the OCSP Revocation Provider caches the OCSP response. The caching minimizes bandwidth usage in high-volume OCSP deployments. The OCSP certificate cache store is in one of the following files:

```
<Local Application Data>\Entrust\OCSPCacheStore.sst
```

Note: Double-click the file to view it in the Microsoft Management Console.

- 7** The OCSP Revocation Provider sets the following certificate properties in the certificates that are saved to the OCSP certificate cache store:
 - a timestamp
 - an encoded OCSP response
 - an encoded [nonce](#) that is generated when sending an OCSP request to the OCSP responder server
- 8** Once the OCSP response is cached, the OCSP Revocation Provider only sends a new OCSP request when one of the following occurs:
 - the timestamp certificate property does not exist
 - the timestamp certificate property exists, and the difference between the current time and the timestamp is greater than or equal to the `OCSPCacheStoreUpdateInterval` setting

For details on this setting, and other OCSP settings, see [“OCSP Revocation Provider settings” on page 425](#).

Certificate path discovery, validation, and extension checking

In simple terms, certificate path discovery and validation is the process of discovering a path from the user's certificate to a trusted CA. Sometimes to find the trusted CA, a path (also called a chain) must be built through a number of intermediate CAs. When the path is built and validated, the user's certificate can be trusted. Part of the validation process is checking whether critical extensions are known.

CryptoAPI includes built-in certificate path discovery and validation functionality that Security Provider leverages when it needs to validate certificates.

In addition, Security Provider offers three features—Certificate Path Discovery, Certificate Path Validation, and Certificate Path Critical Extension Policy Provider—that improve CryptoAPI's certificate path building and validation capabilities. These features—excluding the Certificate Path Critical Extension Policy Provider—are activated automatically for any CryptoAPI applications that use CryptoAPI's certificate path discovery and validation features.

Certificate path discovery and validation are explained in detail in the following sections:

- [“Path discovery and validation overview” on page 141](#)
- [“About the Certificate Path Discovery feature” on page 142](#)
- [“About the Certificate Path Validation feature” on page 143](#)
- [“About the Certificate Path Critical Extension Policy Provider” on page 143](#)
- [“Customizing certificate path discovery” on page 144](#)
- [“Customizing certificate path validation” on page 145](#)
- [“Customizing the Certificate Path Critical Extension Policy Provider” on page 146](#)

Path discovery and validation overview

When a certificate needs to be validated, the following steps are performed:

- 1** A CryptoAPI application (Security Provider, for instance) calls CryptoAPI to build the certificate path between the user's (or computer's) certificate and a trusted root certificate. To help with this task, the Certificate Path Discovery feature may be invoked. See [“About the Certificate Path Discovery feature” on page 142](#) for details.
- 2** The application calls CryptoAPI to perform the base-chain-policy-verification checks as well as the basic-constraints-chain-policy checks. To help with this task, the Certificate Path Validation feature is invoked. For details, see [“About the Certificate Path Validation feature” on page 143](#).

- 3 The application calls CryptoAPI to perform critical extension chain policy checks. In order to perform these checks, the Certificate Path Critical Extension Policy Provider can be invoked. Unlike the Certificate Path Discovery and Verification features, your application must be coded to call the Certificate Path Critical Extension Policy Provider. For details, see [“About the Certificate Path Critical Extension Policy Provider” on page 143](#).

Note: If any of the steps in the path validation procedure fails, the path validation is aborted.

About the Certificate Path Discovery feature

Security Provider offers the Certificate Path Discovery feature. It allows Security Provider (or any CryptoAPI-based application) to discover and download intermediate CA certificates (also called subordinate CA certificates), CA cross-certificates, and link certificates located in any directory. CryptoAPI can then use these certificates to build certificate paths to a trusted root CA.

Without the Certificate Path Discovery feature, CryptoAPI must rely solely on the AIA extension in certificates (which is often not in certificates) as the basis from which to discover intermediate CA certificates.

When the Certificate Path Discovery feature is activated, the following occurs:

- A CryptoAPI application (Security Provider, for instance) needs to check a signature on a certificate. CryptoAPI searches the Intermediate CA certificate store for CA certificates that can build a path to a trusted root CA certificate.
- If the application is unable to find a CA certificate that can successfully build a path, it searches the Entrust CA Certificate Search store located within the Intermediate Certification Authorities store. This invokes a small program called Entrust CA Certificate Search.
- The Entrust CA Certificate Search program looks in the directory that you configured as the default directory. This directory can be any LDAP directory of your choosing, including Active Directory—it does not need to be associated with Security Manager.
- The Entrust CA Certificate Search program downloads any intermediate CA certificates, cross-certificates, and link certificates that it finds to this location:

```
<Local Application Data>\Entrust\ESP\eespcacertcache.sst
```

You can view the certificates in `eespcacertcache.sst` by double-clicking the file.

- From this point forward, the Entrust CA Certificate Search program uses the cached certificates first and only searches the directory again if the cached certificates do not successfully verify a certificate.

About the Certificate Path Validation feature

The Certificate Path Validation feature ensures that X.509 and RFC 3280 validation checks are performed on certificate paths.

Certificate Path Validation replaces Microsoft's base-chain-policy-verification checks. This replacement means that Security Provider—and any CryptoAPI applications that use Microsoft's base-chain policy verification checks—automatically performs the following validation checks detailed in RFC 3280bis-02 section 6.1:

- signature verification
- validity periods
- name chaining
- basic constraints
- key usage
- certificate policies
- require explicit policy
- policy mappings
- inhibit policy mapping
- inhibit any policy
- name constraints
- weak or insecure hash algorithms

About the Certificate Path Critical Extension Policy Provider

As mentioned in the [“Path discovery and validation overview” on page 141](#), the final step in validating a certificate path is to validate the critical extension policy. A certificate path satisfies this policy if all critical extensions are known. If an unknown critical extension is found on any certificate in the path, the path is invalid.

The Certificate Path Critical Extension Policy Provider is not part of Microsoft's base-chain policy verification checks nor is it part of Security Provider's Certificate Path Validation feature.

The Certificate Path Critical Extension Policy Provider is added to the user's system during the Security Provider for Windows installation. It is installed by default with Security Provider and there is no option to disable it. When installed, it is registered with CryptoAPI. This registration allows Security Provider for Windows to access the Certificate Path Critical Extension Policy Provider through the existing CryptoAPI path validation calls.

CryptoAPI applications, other than Security Provider, do not use the Certificate Path Critical Extension Policy Provider unless specifically called to do so.

See page 473 for information about using the registry setting to configure these.

Customizing certificate path discovery

Although the Certificate Path Discovery feature is activated automatically when users install Security Provider, some customizations may be necessary to ensure that the feature works properly in your environment.

The following instructions describe how to customize the Certificate Path Discovery feature using either the **Custom Installation** wizard or Microsoft Group Policy.

- [“To enable certificate path discovery using the wizard” on page 144](#)
- [“To enable certificate path discovery using Group Policy” on page 144](#)

To enable certificate path discovery using the wizard

- 1** Work through the pages of the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#), until you reach the **Select Application Features** page.
- 2** Ensure that the Certificate Path Discovery feature is selected.
- 3** Click **Next**.
The **Specify Directory Information** page appears.
- 4** Click **Add** and add a directory that you want the Certificate Path Discovery feature to search. This directory can be any LDAP directory. It does not need to be associated with Security Manager.
- 5** On the **Specify Directory Information** main page, ensure that the directory you want Certificate Path Discovery to search appears in bold. To make the directory bold, select the directory in the list and click **Default**.
Certificate Path Discovery only checks for certificates in the default directory.
- 6** Optionally, proceed through the wizard until you reach the **Specify Additional Registry Values** page, and specify the `CASearchResultLifetime` registry setting described in [“Certificate path discovery, validation, download, and extensions settings” on page 470](#).
- 7** Proceed to the end of the wizard and click **Finish** to save your settings.
The `.mst` file is updated with your new Certificate Path Discovery settings.
- 8** Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

When users install Security Provider, the Certificate Path Discovery feature will now be activated.

To enable certificate path discovery using Group Policy

- 1** Specify a directory that you want the Certificate Path Discovery feature to search by configuring the registry values and keys described in [“Directory settings” on page 331](#). Follow these guidelines when specifying the directory:

- The directory must be the default directory.
 - The directory can be any LDAP directory. It does not need to be associated with Security Manager.
- 2 Optionally, specify the `CASearchResultLifetime` registry setting described in [“Certificate path discovery, validation, download, and extensions settings” on page 470](#).
 - 3 Push out your settings to your users through Group Policy. The registry values are written to your users’ registries.

When users install Security Provider, the Certificate Path Discovery feature will now be activated.

Customizing certificate path validation

Although Certificate Path Validation is activated automatically when users install Security Provider, some customizations may be necessary to ensure that the feature behaves the way you want it to.

The following instructions describe how to customize Certificate Path Validation using either the **Custom Installation** wizard or Microsoft Group Policy.

- [“To customize the certificate path validation using the wizard” on page 145](#)
- [“To customize certificate path validation using Group Policy” on page 146](#)

To customize the certificate path validation using the wizard

- 1 Work through the pages of the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#), until you reach the **Select Application Features** page.
- 2 Ensure that Certificate Path Validation is selected.
- 3 Proceed through the wizard until you reach the **Specify Additional Registry Values** page. Optionally, specify the Certificate Path Validation registry values described in [“Certificate path discovery, validation, download, and extensions settings” on page 470](#).
- 4 Proceed to the end of the wizard and click **Finish** to save your settings.
The `.mst` file is updated with your new Certificate Path Discovery settings.
- 5 Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

You have activated Certificate Path Validation feature. Security Provider now uses Certificate Path Validation, as well as any CryptoAPI applications that currently use Microsoft’s base-chain-policy-verification checks.

To customize certificate path validation using Group Policy

- 1 Optionally, specify the Certificate Path Validation registry values described in [“Certificate path discovery, validation, download, and extensions settings” on page 470](#). If you do not specify these settings, the Certificate Path Validation feature is activated with the defaults.
- 2 Push out your settings to your users through Group Policy. The registry values are written to your users’ registries.

You have activated the Certificate Path Validation feature. Security Provider now uses Certificate Path Validation, as well as any CryptoAPI applications that currently use Microsoft’s base-chain-policy-verification checks.

Customizing the Certificate Path Critical Extension Policy Provider

By default, there are no known critical extensions defined in the Certificate Path Critical Extension Policy Provider.

If your environment consists of issued certificates that have critical extensions in them, these extensions must be listed in the Windows registry for each user of Security Provider for Windows. The list of extensions you define informs the Certificate Path Critical Extension Policy Provider that those extensions are known.

To specify critical extensions using the wizard

- 1 Work through the pages of the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#), until you reach the **Specify Additional Registry Values** page. Specify the Certificate Path Critical Extension Policy Provider registry value as described on page 473.
- 2 Proceed to the end of the wizard and click **Finish** to save your settings.
The .mst file is updated with your new Certificate Path Discovery settings.
- 3 Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

You have now specified known critical extensions.

To specify critical extensions using Group Policy

- 1 Specify the Certificate Path Critical Extension Policy Provider registry value described in [“Certificate path discovery, validation, download, and extensions settings” on page 470](#).
- 2 Push out your setting to your users through Group Policy. The registry value is written to your users’ registries.

You have now specified known critical extensions.

Integrating with other products

This chapter contains information on how Security Provider for Windows integrates with other Entrust and third-party products.

This chapter contains the following topics:

- [“Creating digital IDs in Administration Services” on page 148](#)
- [“Using the Auto-enrollment Service \(Administration Services\)” on page 149](#)
- [“Using the Roaming Server” on page 170](#)
- [“Using Entrust TruePass” on page 176](#)
- [“Using an application proxy server” on page 177](#)
- [“Using Security Manager Proxy” on page 178](#)
- [“Using smart cards” on page 180](#)
- [“Using a Card Management System” on page 188](#)
- [“Using PIV smart cards with Entrust IdentityGuard” on page 191](#)
- [“Using Security Provider for Windows with non-Entrust PIV smart card management software” on page 197](#)
- [“Using Microsoft Application Virtualization \(App-V\)” on page 199](#)

Creating digital IDs in Administration Services

You can use Entrust Authority Administration Services to provide digital signatures for users of Security Provider and for Web certificates. An Administration Services administrator creates a new account in the User Management Service (UMS) interface. Security Manager generates a reference number and authorization code (collectively called activation codes) for each account and passes these to Administration Services. The administrator then distributes the codes in a secure fashion to each user. You can also use the UMS to recover and manage digital IDs.

Note: The most detailed and current information about using Administration Services is in the Administration services documentation suite.

Using the Auto-enrollment Service (Administration Services)

The Auto-enrollment Service is part of Administration Services. It performs the functions previously performed by the Auto-enrollment Server. Use it to automatically deliver an Entrust digital ID to a Security Provider for Windows client. All types of Entrust digital IDs that are supported by Security Provider for Windows can be auto-enrolled. Depending on the behavior of the Cryptographic Service Provider (CSP), the auto-enrollment can be completely silent or can display the **Enroll for Entrust Digital ID** wizard.

Note: The Auto-enrollment Server has been superseded by the Auto-enrollment Service (AES), a service in Administration Services 8.2 and later. Users who are familiar with the Auto-enrollment Service should find similar functionality in the Auto-enrollment Service.

Security Provider for Windows, in conjunction with the Auto-enrollment Service, can provide an Entrust digital ID for a user or Entrust computer digital ID to the following Windows-based machines:

- Microsoft Windows laptops and desktops
- Microsoft Windows IIS Web servers
- Microsoft Windows domain controllers
- Microsoft Windows authentication clients and servers (RRAS, IAS, VPN, Radius servers)

Attention: The Security Provider for Windows client must be online for auto-enrollment and recovery to occur.

The Auto-enrollment Service supports Security Manager 8.x and above.

Enabling auto-enrollment

To make use of the auto-enrollment and recovery capability, add a configuration setting to the Windows registry. You must activate the different types of Entrust digital IDs that you enroll, user or computer, using separate registry values in the event that different CAs perform these enrollments:

- `AutoEnrollUserURL` is the complete URL of the Auto-enrollment Service for auto-enrolling and recovering users.
- `AutoEnrollMachineURL` is the complete URL of the Auto-enrollment Service for auto-enrolling and recovering computers.

For details on these settings, see [“Auto-enrollment settings” on page 361](#).

You can configure both registry values using the **Auto-Enrollment** tab located in the **PKI Configuration** page of the **Custom Installation** wizard. The registry values support a list of URLs in case connections to multiple servers is desired. If the first server does not work, then the second is tried, and so on. Once a connection is established with one server, connections to other servers are not attempted. (See also [“Configuring hardened desktop environments” on page 322](#) for information on setting a registry key to enable log files.)

Note: You can set auto-enrollment and recovery for each <DN_of_CA> configured in the registry. If multiple CAs have auto-enrollment activated, the auto-enrollments occur one after the other.

Auto-enrollment for an Entrust digital ID for a user

Security Provider for Windows supports requesting an auto-enrollment for an Entrust digital ID for a user. The CSP used for the user enrollment determines whether or not the enrollment performs silently:

- silent enrollment
Choose a CSP that does not require input from the user. For example, Microsoft CSPs can be configured to behave silently. For further information on silent auto-enrollment, see the topic [“Silent auto-enrollment and recovery” on page 156](#).
- manual enrollment
When you use the auto-enrollment feature to create an Entrust digital ID for a user stored in an Entrust security store (.epf) or on a smart card, the **Enroll for Entrust Digital ID** wizard appears.

How the user auto-enrollment is initiated

Auto-enrollment is one of three tasks for which the Digital ID Monitor is responsible. The other two operations are checking for required key updates of user's Entrust digital IDs, and performing automatic certificate downloads.

For each CA that has auto-enrollment activated, the Digital ID Monitor searches the user's local Personal certificate store for certificates issued by that CA and managed by Security Provider for Windows. If a certificate is present that is not managed by Security Provider for Windows, it is ignored. If no certificates are found, an auto-enrollment is initiated.

Security Provider for Windows initiates an auto-enrollment whenever there are no certificates issued by the CA. However, the Auto-enrollment Service does not always grant an auto-enrollment. The Auto-enrollment Service decides if an auto-enrollment

is appropriate. Furthermore, the Auto-enrollment Service determines if an enrollment or a recovery is the appropriate action and communicates that information to Security Provider for Windows.

When Security Provider for Windows requests a user auto-enrollment because no certificates exist in the user's local Personal certificate store, the Auto-enrollment Service grants the request and instructs Security Provider for Windows to perform an auto-enrollment in the following cases:

- the user does not exist yet in Security Manager
- the user is in the Added state in Security Manager

The Auto-enrollment Service rejects the auto-enrollment request in the following cases:

- the user is in the Active state in Security Manager
- the user is in the Key Export state in Security Manager
- the user is in the Disabled state in Security Manager

Even if the Auto-enrollment Service grants the request, this does not mean that enrollment occurs immediately. Depending on the rules in place at the Auto-enrollment Service, the request may be queued for administrative approval before Security Provider for Windows is allowed to proceed with the enrollment. See [“Enrollment and recovery queues for administrator approval” on page 155](#) for further information.

In order to communicate securely with the Auto-enrollment Service, Security Provider for Windows must first authenticate the user to the SSL Server. The Internet Information Services (IIS) will be configured to require secure communication (through SSL), and the authentication method required will be set to Windows Integrated Logon. See the *Entrust Authority Administration Services Configuration Guide* for further information. Windows Integrated Logon to the SSL server will be possible, provided the user's Windows login name and domain name are acceptable or trusted by IIS. Once IIS authenticates the user, secure communication is achieved with the Auto-enrollment Service.

Auto-enrollment for an Entrust computer digital ID

Security Provider for Windows supports requesting auto-enrollment for an Entrust computer digital ID. The CSP used for the Entrust computer digital ID must perform silently and there should be no notifications, no enrollment wizard, and no password prompts. For example, configure Microsoft CSPs to behave silently. See the topic [“Silent auto-enrollment and recovery” on page 156](#) for further information.

How the computer auto-enrollment is initiated

Auto-enrollment is one of three tasks for which the Computer Digital ID Service is responsible. The other two operations are checking for required key updates of a computer's Entrust digital ID and performing Automatic Certificate Downloads.

For each CA that has auto-enrollment activated, the Computer Digital ID Service searches the computer's local Personal certificate store for certificates issued by that CA and managed by Security Provider for Windows. If a certificate is present that is not managed by Security Provider for Windows, it is ignored. If no certificates are found, auto-enrollment is initiated. Security Provider for Windows initiates an auto-enrollment whenever there are no certificates issued by the CA. However, the Auto-enrollment Service does not always grant an auto-enrollment. The Auto-enrollment Service decides if auto-enrollment is appropriate. Furthermore, the Auto-enrollment Service determines if enrollment or recovery is the appropriate action and communicates that information with the Security Provider for Windows client.

When Security Provider for Windows requests a computer auto-enrollment because no certificates exist in the computer's local Personal certificate store, the Auto-enrollment Service grants the request and instructs Security Provider for Windows to perform auto-enrollment in the following cases:

- the computer does not exist yet in Security Manager
- the computer is in the Added state in Security Manager
- the computer is in the Active state in Security Manager

The Auto-enrollment Service rejects the request in the following cases:

- the computer is in the Key Export state in Security Manager
- the computer is in the Disabled state in Security Manager

Even if the Auto-enrollment Service grants the request, this does not mean that the enrollment occurs immediately. Depending on the rules in place at the Auto-enrollment Service, the request may be queued for Administrative approval before Security Provider for Windows is allowed to proceed with the enrollment. See ["Enrollment and recovery queues for administrator approval" on page 155](#) for further information.

In order to communicate securely with the Auto-enrollment Service, Security Provider for Windows must first authenticate the computer to the SSL server. Configure Internet Information Services (IIS) to require security communication (using SSL), and the authentication method required will be set to Windows Integrated Logon. See the *Entrust Authority Administration Services Configuration Guide* for further information. Windows Integrated Logon to the SSL server will be possible provided the computer's Windows name and domain name are acceptable or trusted by IIS. Once IIS authenticates the computer, secure communication will be achieved with the Auto-enrollment Service.

Auto-recovery

Security Provider for Windows supports requesting an auto-recovery. The CSP that is used for the auto-recovery determines whether or not it runs silently:

- silent recovery

Choose a CSP that does not require input from the user. For example, configure Microsoft CSPs to behave silently. For further information on silent auto-enrollment, see the topic [“Silent auto-enrollment and recovery” on page 156](#).

Note: Auto-recovery for a computer digital ID is always silent.

- manual recovery
 - When you use the auto-enrollment feature to recover an Entrust digital ID for a user, the **Recover Entrust Digital ID** wizard appears for user input.
 - When you use the auto-recovery feature to recover an Entrust digital ID for a user stored in an Entrust security store (.epf) or on a smart card, the **Recover Entrust Digital ID** wizard appears.

How the auto-recovery is initiated

The digital ID management component is responsible for detecting and initiating all required user auto-recoveries. When digital ID management detects that an Entrust digital ID is in one of the following invalid states, Security Provider for Windows attempts an auto-recovery:

- the signing certificate is expired
- the signing certificate is revoked
- all certificates are revoked
- the user requires an update, but the user is in the Key Recovery state at the CA
- the user requires an update, but updates are not allowed for this user at the CA

If auto-recovery is activated for the CA, Security Provider for Windows sends the auto-recovery request to the Auto-enrollment Service. When the auto-recovery is granted by the Auto-enrollment Service, Security Provider for Windows is instructed to perform an auto-recovery.

Depending on the rules in place at the Auto-enrollment Service, the digital ID management component may queue the request for administrator approval before allowing Security Provider for Windows to proceed with the recovery. See [“Enrollment and recovery queues for administrator approval” on page 155](#) for further information.

When certificates exist in the user's local Personal certificate store and digital ID management detects one of the invalid states, an update of the user's Entrust digital ID is performed. When digital ID management performs silently, due to the configured CSP, the update occurs silently. When digital ID management does not occur silently, the user's Entrust digital ID begins updating. A dialog box informs the user when this process completes.

Auto-recovery of users in the Active state in Security Manager

The Auto-enrollment Service rejects auto-recoveries of users in the Active state in Security Manager. This is necessary to prevent roaming users from recovering at each machine they log in to. If this restriction was not in place, auto-recoveries could occur at several different machines, rather than allowing the user to log in to their existing Entrust digital ID (for example, a roaming Entrust security store or a smart card).

Sometimes a user legitimately requires a recovery while in the Active state in Security Manager. This could be due to a forgotten password, a lost security store, or perhaps corrupt or deleted certificates in the local Personal certificate store. When this is the case, the user must inform their administrator of the problem. The administrator sets the user for key recovery in Security Manager.

Customizing the certificate type and role

Auto-enrollment Service can use Security Provider for Windows settings to choose a specific role or certificate type for the user or computer Entrust digital ID. By default, the Auto-enrollment Service determines the role or certificate type. The following Security Provider for Windows registry settings configure users and computers with different roles and certificate types than the default set at the Auto-enrollment Service:

- `AutoEnrollUserDigitalIDType` sets the certificate type and role for an Entrust digital ID for a user.
- `AutoEnrollMachineDigitalIDType` sets the certificate type and role for an Entrust computer digital ID.

Which string that you configure in the `AutoEnrollUserDigitalIDType` or the `AutoEnrollMachineDigitalIDType` registry setting depends on the certificate type information located in the Auto-enrollment Service's `ae-defaults.xml` file. See the *Entrust Authority Administration Services Configuration Guide* for further information.

When the Auto-enrollment Service decides what role and certificate type to use for the enrollment, it communicates this to Security Manager. Security Manager then creates the appropriate identity at the CA.

Responses to auto-enrollment and recovery requests

When the auto-enrollment and recovery request is sent from a Security Provider for Windows client to the Auto-enrollment Service, the Auto-enrollment Service sends one of the following responses to the Security Provider for Windows client:

- The approval response includes an authorization code and reference number that Security Provider for Windows can use to communicate with the CA, and enroll and recover the user or computer. The response also indicates the validity period of these activation codes and whether an enrollment or a recovery should be performed.
- The queued response indicates that the request is queued for administrative approval. See the topic [“Enrollment and recovery queues for administrator approval” on page 155](#).
- The rejection response includes an error code and reason string indicating why the auto-enrollment and recovery cannot occur. See the topic [“Rejected auto-enrollment and recovery response” on page 158](#).

Once Security Provider for Windows has the Approval response, communication with the Auto-enrollment Service is complete. The enrollment and recovery is then performed through direct communication with Security Manager.

Enrollment and recovery queues for administrator approval

Whenever the Auto-enrollment Service queues a request, the following occurs:

- Auto-enrollment Service sends a queued response to Security Provider for Windows.
- Security Provider for Windows logs this information, but does not save it to memory.
- Security Provider for Windows continues to send identical auto-enrollment and recovery requests, until the administrator has approved the request.
- The administrator releases the request from the queue, and the Auto-enrollment Service sends an approval response to the Security Provider for Windows client.

See the *Entrust Authority Administration Services Configuration Guide* for further information.

Queued responses

The end user never sees queued responses. It is only after Security Provider for Windows receives the approval response that the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard appears for user enrollments and recoveries that are not configured as silent.

If an auto-recovery is attempted, due to an invalid state, and Security Provider for Windows receives a queued response instead of an approval response, the user is notified of this in a dialog box.

Silent auto-enrollment and recovery

Silent auto-enrollment of an Entrust computer digital ID means that no password prompts, no wizards, no dialog boxes, and no error messages appear.

Silent auto-enrollment for an Entrust digital ID for a user is the same as for a computer, except that error messages can appear even in silent mode.

Once Security Provider for Windows has the approval response from the Auto-enrollment Service, Security Provider for Windows sends preliminary messages to the CA, including the reference number and authorization code, requesting the policy certificates for the user. The CA returns the desired policy certificates and Security Provider for Windows reads the certificate definition policy certificates. The certificate definition policy certificate has information about:

- the CSP to use for the auto-enrollment and recovery
This is the **CSP to manage keys** certificate definition policy setting.
- whether or not the Entrust digital ID for a user auto-enrollment or recovery will be silent

This is the **Protected key storage for CSP** certificate definition policy setting.

With this information, Security Provider for Windows knows whether to display the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard. The auto-enrollment or recovery for an Entrust digital ID for a user runs silently only when you configure the following two settings:

- the **CSP to manage keys** setting; for example, Microsoft CSPs
- the **Protected key storage for CSP** setting is disabled in all certificate definition policies, in each certificate type
Smart card CSPs and the Entrust Enhanced CSP ignore the **Protected key storage for CSP** setting. See the topic [“Protect key storage for CSP” on page 264](#).

Note: Because smart card CSPs ignore the **Protected key storage for CSP** setting, silent auto-enrollment and recovery is not possible for smart card users. Smart card users are always prompted to perform a key enrollment, recovery, or update.

The auto-enrollment or recovery for an Entrust computer digital ID always runs silently.

Attention: If the **CSP to manage keys** setting is not set to a CSP that supports silent behavior, the auto-enrollment or recovery fails.

When auto-enrolling or recovering an Entrust computer digital ID, the **Protected key storage for CSP** setting is always ignored. See the topic [“Protect key storage for CSP” on page 264](#).

When an Entrust digital ID for a user or computer is silently auto-enrolled successfully, digital ID management for that Entrust digital ID always runs silently. Because the process is silent, you may want to view the `logmain.htm` file to determine if problems occurred during any of these operations.

Nonsilent user auto-enrollment and recovery

When Security Provider for Windows receives the auto-enrollment or recovery approval from the Auto-enrollment Service and it is not a silent installation, Security Provider for Windows displays a tray notification icon and balloon tip that notifies the user that they can begin enrollment or recovery.

When the user clicks the icon or balloon tip, an **Enroll for Entrust Digital ID Request** or **Entrust Digital ID Recovery Request** dialog box appears. When the user clicks **Enroll** on the **Enroll for Entrust Digital ID Request** dialog box or the user clicks **Recover** on the **Entrust Digital ID Recovery Request** dialog box, the respective **Enroll for Entrust Digital ID** or **Recover for Entrust Digital ID** wizard is launched.

The user will never see the following pages in the wizard:

- **Enter activation codes** page
The activation codes (reference number and authorization code) are in the approval response.
- **Specify a Certification Authority (CA)** page
Security Provider for Windows also knows which CA is being enrolled to.

Approved Entrust computer digital ID auto-enrollment and recovery requests

When Security Provider for Windows receives the auto-enrollment or recovery approval from the Auto-enrollment Service, Security Provider for Windows silently performs the enrollment or recovery of the Entrust computer digital ID. Since this is a silent installation, you may want to view the `logmain.htm` file to determine if any problems occurred during the auto-enrollment or recovery.

Rejected auto-enrollment and recovery response

There may be several reasons why an auto-enrollment or recovery is rejected, including:

- the CA is not running
- the user or computer is not allowed to enroll or recover because they are revoked, and there is no queue selected
- the user is not allowed to recover because they are in the Active state
- the user or computer's signing certificate is revoked, and there is no queue selected
- the user is not allowed to recover because key updates are not allowed for this user at the CA, and there is no queue selected

Every time the Digital ID Monitor or the Computer Digital ID Service runs, Security Provider for Windows sends another auto-enrollment request until it gets an approval response. When a response message from the Auto-enrollment Service contains a fatal error, Security Provider for Windows writes this information to the Security Provider for Windows log (`logmain.htm`) file.

When queuing is available, all auto-recovery requests are placed in the queue and the administrator decides if an auto-recovery should be granted or denied. When queuing is not available for an administrator, the following automatic auto-recoveries are granted or denied:

Granted:

- when the signing certificate is expired
- when the user is in the Key Recovery state at the CA

Denied:

- when the signing certificate is revoked
- when all certificates are revoked
- when updates are not allowed at the CA for this user

When an auto-recovery is denied, the Auto-enrollment Service returns an error to the Security Provider for Windows client. In nonsilent mode, an error message appears explaining that an auto-recovery attempt failed. In this case, the user must inform their administrator that a recovery is required. The administrator must set the user for Key Recovery at the CA. Once the user is switched from the Active state to the Key Recovery state, an auto-recovery is automatically granted by the Auto-enrollment Service.

Resending auto-enrollment requests

When an auto-enrollment request is sent to the Auto-enrollment Service, the request to create users is then sent to Security Manager. If many users or computers are

attempting auto-enrollment simultaneously, the connection attempt from the Auto-enrollment Service to Security Manager may fail.

When the connection attempt fails, the Auto-enrollment Service returns an AES0170 error code in the response message to Security Provider for Windows. When Security Provider for Windows reads the AES0170 error code in the response message, it tries to resend the auto-enrollment request using the following settings:

- `AutoEnrollNumberOfRetries` sets the number of times you want to retry sending the request. The default is 10 times.
- `AutoEnrollRetryInterval` sets the number of seconds that should elapse between each retry. The default is every 30 seconds.

See [“Auto-enrollment settings” on page 361](#) for details on these settings.

Note: Security Provider only retries when the Auto-enrollment Service sends the AES0170 error code in its response. If an auto-enrollment is not successful for a reason other than AES0170, or if all retries are unsuccessful, auto-enrollment will be attempted again:

- at the next interval set by `CertUpdateInterval`, or the next time the Computer Digital ID Monitor starts (for user enrollment)
 - at the next interval set by `ComputerCertUpdateInterval`, or the next time the Computer Digital ID Service starts (for computer enrollment)
-

Why Security Provider for Windows might reject SSL certificates from Microsoft IIS

To send or receive messages, Security Provider for Windows uses the WinHTTP functions built into Microsoft Windows to establish the connection with the Auto-enrollment Service. Checks on the SSL certificate are made inside the WinHTTP functions, so Security Provider for Windows does not control this behavior.

There are several different reasons why Security Provider for Windows might reject SSL Web server certificates. If any of the following errors are found to exist on the certificate, authentication to Microsoft IIS does not occur and therefore, auto-enrollment is not attempted:

- revocation check failed
For some reason, the revocation check could not be completed. Possible reasons:
 - the directory is down and the CRL could not be fetched
 - the PKI configuration data is not defined in the registry for the CA that issued the SSL certificate, and therefore the Security Provider for Windows CRL checker does not know the server name of the directory
- invalid certificate

- revoked certificate
- unknown CA

The root certificate (and any required intermediate CA certificates or self-signed certificate) are missing from the local certificate store. WinHTTP must be able to build a path from the SSL certificate to a trusted root.

- invalid common name

The common name (`cn`) portion of the subject name (or `subjectAltName`) in the SSL certificate does not match the Web server that Security Provider for Windows is attempting communication with. For example, if the URL entered in the PKI configuration data in the registry is

`https://xyz.abc.com/AdminServicesApp/AutoEnroll`, then the `cn` portion of the subject name (or `subjectAltName`) must be `xyz.abc.com`.

- invalid date

The current time is not within the validity period of the certificate (for example, the certificate expired).

- wrong usage

For example, the SSL certificate has an extended key usage (EKU), but the Server Authentication OID is not included in the EKU list.

- security channel error

Using an SSL certificate with the Auto-enrollment Service

When enrolling a user digital ID, WinHTTP must be able to build a path from the SSL certificate to the Current User Trusted Root store. Similarly, when enrolling a computer digital ID, WinHTTP must be able to build a path from the SSL certificate to the Local Machine Trusted Root store.

If either digital ID uses a self-signed certificate, first add that certificate to the applicable certificate store: the User Trusted Root store or the Local Machine Trusted Root store.

Enabling SSL on Active Directory

Note: This procedure is not required if you are using Administration Services version 8.3 or higher.

In order to enable SSL on Active Directory, if Security Provider for Windows is used to manually create a domain controller certificate, the domain controller certificate:

- must not have a Netscape Certificate Extension Definition

The Java JRE that is used by the Auto-enrollment Service rejects the certificate when the Netscape Certificate Extension Definition is detected.

See the *Entrust Authority Security Manager Administration User Guide* for further information about the Netscape Certificate Type and Netscape Certificate Extension Definition.

- have the `EnableCRLCache` setting set to 1

This (1) is the default value. If this setting is 0, SSL connections to Active Directory fail.

For details on this setting, see [“CRL Revocation Provider settings” on page 419](#).

Creating and updating an SSL Web server certificate

You can use a computer digital ID to create Web server certificates for the Entrust Authority Auto-enrollment Service and Web servers. See the *Entrust Authority Administration Services Configuration Guide*.

Creating an SSL Web server certificate

To create an SSL certificate using Security Provider for Windows, complete the steps in all of the following procedures:

- [“To create a new certificate type for your SSL server certificate” on page 161](#)
- [“To create a certificate definition policy for your SSL certificate” on page 162](#)
- [“To associate the certificate definition to the SSL server certificate type” on page 163](#)
- [“To use Entrust Security Manager Administration to create a new Web Server user if Entrust security Manager uses LDAP” on page 163](#) or [“To use Entrust Security Manager Administration to create a new Web Server user if Entrust Security Manager uses Active Directory” on page 164](#)

You may need to export your Entrust digital ID, if you enroll the digital ID on a machine other than the one where Microsoft IIS is installed. Complete the procedure in the [“To export your Entrust computer digital ID to Microsoft IIS” on page 165](#) topic. If you enroll directly onto the Microsoft IIS machine, you do not need to export the Digital ID.

To create a new certificate type for your SSL server certificate

- 1 In the `master.certspec` file, locate the [Certificate Types] section header.
- 2 On a new line in the [Certificate Types] section, add a description for the new certificate type.

```
[Certificate Types]
```

```
;
```

```
-----  
; certificate type defining 1 dual usage key pair  
-----
```

```
ent_ssl_server=enterprise,SSL Server Digital ID,SSL Server Digital  
ID with Dual Usage Key Pair
```

You can add a new line anywhere in the [Certificate Types] section, although you typically add descriptions for new certificate types after the default ones.

- 3 On a new line in the [Extension Definitions] section, add the description for the certificate definition. Typically, you add descriptions for new certificate definitions after the default definitions.

```
[Extension Definitions]
```

```
[ent_ssl_server Certificate Definitions]
```

```
;
```

```
-----  
; SSL Server Digital ID Certificate Type  
-
```

```
;- This certificate type defines one key pair for SSL Server
```

```
;- DualUsage: has keyEncipherment and digitalSignature key usage
```

```
;
```

```
-----  
1=DualUsage
```

```
[ent_ssl_server DualUsage Extensions]
```

```
keyusage=2.5.29.15,n,m,BitString,101
```

```
extkeyusage=2.5.29.37,n,o,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.1  
1.3.6.1.5.5.7.3.2
```

- 4 Once you complete all changes to the master.certspec file, you must import these changes back into Security Manager Administration.

To create a certificate definition policy for your SSL certificate

- 1 Log in to Security Manager Administration as a Security Officer, or any administrator with permissions to manage SSL certificates.
- 2 Double-click **Security Policy** in the tree view, and then double-click **User Policies**. The available policy certificates appear below the **User Policies** heading.
- 3 Right-click the **Dual Usage Policy** and select **Copy**. A copy of the selected policy certificate appears under **User Policies**.
- 4 Rename this copy to **Computer DualUsage Exportable Policy**.

- 5 Double-click the **Computer DualUsage Exportable Policy** certificate. The policy attributes page appears on the right.
- 6 Change the following policy attributes:
 - for **CSP to manage keys**, use Microsoft Enhanced Cryptographic Provider v1.0
 - select **Private key export from CSP**
 - deselect **Protected key storage for CSP**
- 7 Click **Apply**.

Once you create a computer policy certificate, you must associate it with the certificate definition in your **one key pair for SSL Server** certificate type.

To associate the certificate definition to the SSL server certificate type

- 1 While logged in to Security Manager Administration, double-click **Security Policy** in the tree view.
- 2 Double-click **Certificate Categories**, and then double-click **Enterprise** to expand the list of certificate categories.
- 3 Double-click **Types** to expand the list of certificate types.
- 4 Double-click the **SSL Server Digital ID** certificate type.
- 5 Double-click the **Dual Usage** certificate definition displayed below the **SSL Server Digital ID** certificate type. The **Policy Mapping** property page appears in the right pane of the window.
- 6 Under the section **Certificate Definition Policy** on the **Policy Mapping** page, select the **Computer DualUsage Exportable Policy** from the drop-down list.
- 7 Click **Apply**.

You have successfully created a new certificate type for use with SSL server certificates.

When you manually create an account for an SSL server certificate using Security Manager Administration, ensure that you select **Enterprise** as the certificate category and the **one key pair for SSL Server** certificate type that you just created.

To use Entrust Security Manager Administration to create a new Web Server user if Entrust security Manager uses LDAP

- 1 While logged in to Security Manager Administration, right-click the **User** icon in the left-hand column.
- 2 Select **New User** from the menu.
- 3 The **New User** dialog box appears. In the **Naming** tab, select **Web Server** as the **Type** of user.

- 4 For the name, the fully qualified host name must be used. For example,
`cn=autoenrolladdev.AUTOENROLLAD_DEV.entrust.com,`
`o=DesktopSM7, c=ca`
In this case, `autoenrolladdev` is the name of the computer that has Microsoft IIS installed and `AUTOENROLLAD_DEV.entrust.com` is the domain.
- 5 Select the **Certificate Info** tab.
- 6 Select **Enterprise** as the **Category** from the drop-down list.
- 7 Select the **SSL Server Digital ID** certificate **Type** from the drop-down list.
- 8 The computer identity can now be created by clicking **OK**. You are requested to authorize this activity.
- 9 The computer identity creation is confirmed with an **Operation Completed Successfully** dialog box. The dialog box displays the activation codes (reference number and authorization code) that you must distribute to the user in a secure manner. The activation codes are used during the enrollment process.

You have now added a computer identity to Security Manager Administration.

To use Entrust Security Manager Administration to create a new Web Server user if Entrust Security Manager uses Active Directory

- 1 Make sure your users already exist in Active Directory.
- 2 While logged in to Security Manager Administration, right-click the **User** icon in the left-hand column.
- 3 Select **Find > By Directory Attributes**. The **Find Users by Directory attributes** dialog box appears.
- 4 Locate the computer's entry in Active Directory.
- 5 Right-click the chosen entry and click **Properties**. The **User Properties** dialog box appears for the chosen user.
- 6 Select the **General** tab in the **User Properties** dialog box. The **User DN** is populated with information from Active Directory.
- 7 Type the fully qualified host name in the **subjectAltName** field for the computer. For example:
`dNSName=autoenrolladdev.AUTOENROLLAD.DEV.entrust.com`
- 8 Select the **Certificate Info** tab.
- 9 Select **Enterprise** as the **Category** from the drop-down list.
- 10 Select the **SSL Server Digital ID** certificate **Type** from the drop-down list.
- 11 The computer identity can now be created by clicking **OK**. You will be requested to authorize this activity.

- 12** The computer identity creation is confirmed with an **Operation Completed Successfully** dialog box. The dialog box displays the activation codes (reference number and authorization code) that you must distribute to the user in a secure manner. The activation codes are used during the enrollment process.

You have now added a computer identity from Active Directory to Security Manager Administration.

Exporting your Entrust computer digital ID to Microsoft IIS

When you enroll your Entrust digital ID onto a different machine other than the one with Microsoft IIS installed, complete the steps in this procedure.

To export your Entrust computer digital ID to Microsoft IIS

- 1** Start the Microsoft Management Console.
On a Windows 2008 Server:
 - a** From the **Start** menu, select **Run**. The **Run** dialog box appears.
 - b** Type `MMC` in the **Open** text box.
 - c** Click **OK**.On a Windows 2012 server:
 - a** Select Windows PowerShell:
 - b** Type `mmc` in the PowerShell window.
 - c** Press **Enter**.The Microsoft Management Console appears.
- 2** Open your Entrust Computer Digital ID file with the `.msc` extension (Windows 2008 Server) or select **File > Add/Remove Snap-in...** (Windows 2012 Server)
- 3** When the console tree on the left-hand pane displays the **MS Certificates Snap-In** option under the **Console Root** folder, expand the **MS Certificates Snap-In** option.
- 4** Expand the **Certificates** option and click **Personal** certificates. The computer's personal certificate store displays all available certificates.
- 5** Right-click the chosen computer certificate, select **All Tasks > Export**. This launches Microsoft's **Certificate Export** wizard.
- 6** In the **Certificate Export** wizard, specify that you want to export the private key with the certificate.
- 7** Choose the **Personal Information Exchange - PKCS #12(.PFX)** export file format, and specify that you want to include all certificates in the certification path, if possible.
- 8** Complete the **Certificate Export** wizard.

This should create the .pfx file containing the certificates and keys from the Entrust computer digital ID.

- 9** Copy the .pfx file to the computer that has Microsoft IIS installed.
- 10** Using Microsoft Management Console, open the **Certificates** snap-in for the local computer (do not select current user).
- 11** When the console tree on the left-hand pane displays the **Certificates (Local Computer)** option under the **Console Root** folder, expand the list of certificates.
- 12** Click **Personal** certificates.

The computer's personal certificate store displays all available certificates.
- 13** Right-click the chosen computer certificate, select **All Tasks > Import**.

This launches Microsoft's **Certificate Import** wizard.
- 14** In the **Certificate Import** wizard, specify that you do not want strong protection of the keys.
- 15** Complete the **Certificate Import** wizard, which should import the certificate in your local machine personal store.

When you export your Entrust computer digital ID to Microsoft IIS procedure, continue to the ["To assign the SSL Server certificate in Microsoft IIS \(version 8 used in procedure\)" on page 166](#) procedure.

To assign the SSL Server certificate in Microsoft IIS (version 8 used in procedure)

- 1** Launch Microsoft **Internet Information Services** (IIS).
- 2** Expand the **Internet Information Services** tree in the **Connections** pane.
- 3** Expand **Sites**.
- 4** Select **Default Web Site**.
- 5** Under **Actions** click **Bindings**.

The **Site Bindings** dialog appears.
- 6** Click **Add**.

The **Add site binding** dialog appears.
- 7** In the **Type** dropdown list select **https**.
- 8** Under **SSL certificate**, select the certificate that you imported.
- 9** Click **OK**.

Your **https** link will appear in the list.
- 10** Click **Close**.

You have successfully assigned your SSL Web Server certificate in Microsoft IIS.

Updating the SSL Web server certificate

Security Provider for Windows includes an IIS update component. When a certificate is configured in IIS, the IIS update component checks to see if the existing certificate in IIS matches the certificate being updated. If there is a match, Security Provider configures IIS to use the newly updated certificate instead. If no certificate is configured in IIS, Security Provider does not configure a certificate in IIS.

The IIS update component is only used when Microsoft IIS is installed on the same machine as Security Provider for Windows. All Web sites in IIS, whether they are running or not, are checked by the IIS update component.

SSL Web server certificates in IIS are updated when any of the following occur:

- natural rollover
- forced key update
- update due to expired certificate
- update due to revoked certificate
- update due to approaching **Cert update date** (configured in the certificate definition policy)
- DN change

SSL Web server certificates in IIS are not updated when any of the following occur:

- certificate type change
- certificate type obsoleted
- automatic move user
- during a recovery of an Entrust digital ID

Note: Security Provider requires the IIS (Internet Information Services) Metabase Compatibility component to detect the IIS configuration and allow IIS to use the certificate. This component is not installed by default when you install IIS version 7. See ["If certificate updates are not working properly with IIS 7.x or 8.x" on page 167](#) for information about the Metabase Compatibility component.

If certificate updates are not working properly with IIS 7.x or 8.x

In IIS version 7.x or 8.x the Metabase Compatibility component is not installed by default. This component is used by Security Provider to detect IIS configuration and configure IIS to use the certificate. If this component is missing from the IIS installation, Security Provider logs the following messages (log level 4):

```
Information 11/03/2009 11:48:58 IIS Notify Plug-in eemdisrv.exe 1028
1144 105 Checking if IIS is installed on this computer. This is done by
initializing the MSAdminBase (COMM) object.
```

Information 11/03/2009 11:48:58 IIS Notify Plug-in eemdisrv.exe 1028
1144 125 IIS is not installed on this computer. No need to check if the
certificate in IIS should be updated.

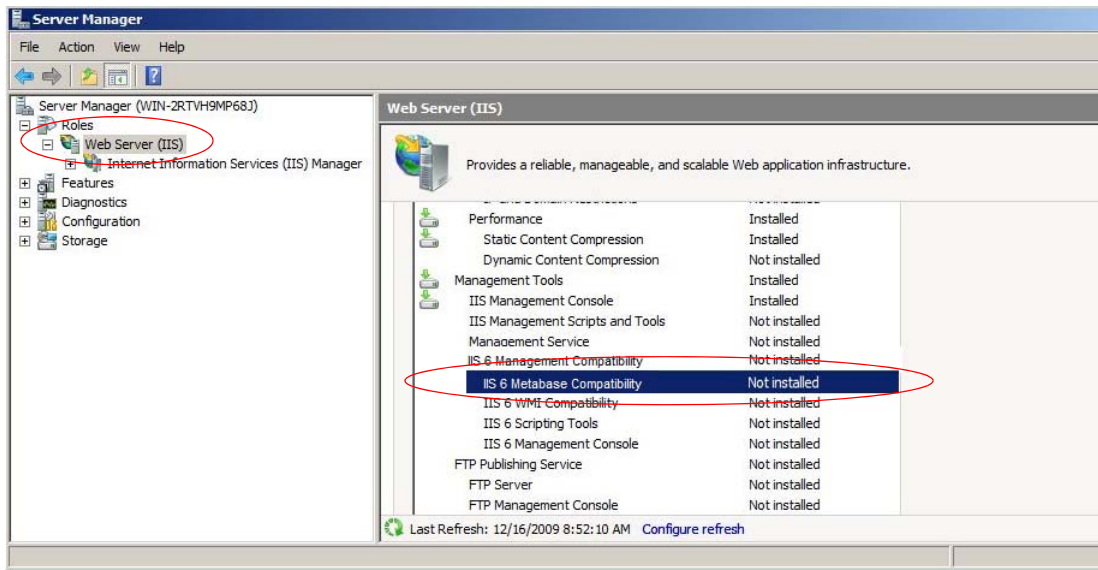
To solve this problem, add the Metabase Compatibility component to the IIS
installation.

To add the Metabase Compatibility component to IIS

- 1 Start the Server Manager. Select **Start menu > Administrative Tools > Server Manager**.



- 2 In the left pane, under **Roles** select **Web Server (IIS)**. From the list in the right pane under **IIS 6 Management compatibility**, select **IIS 6 Metabase compatibility**.



- 3 Click **Add Role Services**.
- 4 In the **Select Role Services** page, click **Next**.
- 5 In the **Confirm Installation Selections** page, click **Install**.

Using the Roaming Server

Security Provider for Windows supports the use of the Entrust Authority™ Roaming Server in its architecture. Users enrolled using the Entrust Enhanced Cryptographic Service Provider may be configured to work as roaming users to encrypt, digitally sign, and authenticate electronic transactions from any computer connected to Roaming Server. Roaming Server lets users store their Entrust digital ID in an Entrust security store located in a centralized directory. The digital ID is then accessed remotely.

According to a user's requirements and where they are working, a user can work as a desktop user and then switch to work as a roaming user. For instance, a user can log in and work as a desktop user from their computer at work. When the user wants to work as a roaming user from either their computer at work or another computer, the user switches to become a roaming user.

The Entrust roaming security store is saved to the Roaming Server immediately after an update occurs or when there is a change to the Entrust roaming security store's options.

Topics in this section:

- [“Enabling roaming users” on page 170](#)
- [“Switching between a roaming and desktop user” on page 171](#)
- [“Configuring roaming certificate settings” on page 172](#)
- [“Allowing users with mixed digital IDs to roam” on page 172](#)
- [“Working offline as a roaming user” on page 174](#)
- [“Roaming Server problems” on page 175](#)

Enabling roaming users

The following instructions describe how to enable roaming users in a Security Provider environment.

To enable roaming

- 1 Install the Roaming Server and add it to Security Manager. If you choose to install multiple Roaming Servers, ensure that the Roaming Servers read and write to and from the same directory.

See the *Entrust Authority Roaming Server User Guide* for instructions.

- 2 In Security Manager Administration, create entries for your roaming users, ensuring that their user policy
 - has the **Permit roaming** policy attribute selected (see [“Configuring user policy” on page 252](#) for further information).

- has the **Algorithm for digital signature** set to 4096-bit RSA or lower (see [“Configuring user policy” on page 252](#) for further information)

For more information on creating roaming user entries, see the *Entrust Authority Roaming Server User Guide*.

- 3 Through Security Provider's **Custom Installation** wizard or through Microsoft Group Policy, create or modify a custom installation package for your end users that enables connectivity between Security Provider and your organization's Roaming Servers. For details on the Roaming Server settings, see:

- [“Roaming Server settings” on page 354](#)
- [“Entrust security store login settings” on page 396](#) (this section describes one roaming-related setting)
- [“Entrust security store startup and shutdown settings” on page 416](#) (this section describes one roaming-related setting)

For details on creating a custom installation package, see [“Customizing the installation” on page 285](#).

- 4 Package, test, and distribute the installation package to end users. See [“Packaging the installation” on page 297](#), [“Testing the installation” on page 303](#), and [“Distributing the installation package” on page 304](#).

Switching between a roaming and desktop user

Depending on how the administrator has configured the end users' policy, users may have the ability to switch between working as a roaming or a desktop user. If roaming is activated on their computer and users have the taskbar status icon installed, they can choose between the **Work as a desktop user** and **Work as a roaming user** check boxes in the **Entrust Security Store Options** dialog box.

When a user works as a desktop user, their Entrust security store is an .epf file on their computer in a location specified during the enrollment process. When a user works as a roaming user, their Entrust security store is copied to the directory.

If the user's policy is changed to desktop only or roaming only, the Administrator can use a registry setting to change the profile automatically, the next time the user logs in (see `EnableAutomaticEntrustSecurityStoreTypeSwitch` in the section [“Entrust security store login settings” on page 396](#)).

Information for end users is provided in the Security Provider for Windows online help documentation, available by right-clicking the taskbar status icon. If the icon feature is disabled, users can locate the `eesp.chm` file a sub folder under where they installed Security Provider for Windows (the default is `\Program Files\Entrust\ESP\1033\` for 32 bit or `\Program Files (x86)\Entrust\ESP\1033\` for 64 bit).

Configuring roaming certificate settings

You can have Security Provider for Windows delete users' certificates from the local certificate stores at logout and startup.

To delete users' certificates on logout or startup

- 1 Through Security Provider's **Custom Installation** wizard or through Microsoft Group Policy, create or modify a custom installation package for your end users that deletes certificates on logout or startup. For details, see:
 - [“Entrust security store login settings” on page 396](#) (this section describes the `DeleteCertsAtLogout` setting)
 - [“Entrust security store startup and shutdown settings” on page 416](#) (this section describes the `DeleteRoamCertsAtStartup` setting)For details on creating a custom installation package, see to [“Customizing the installation” on page 285](#).
- 2 Package, test, and distribute the installation package to end users. See [“Packaging the installation” on page 297](#), [“Testing the installation” on page 303](#), and [“Distributing the installation package” on page 304](#).

Allowing users with mixed digital IDs to roam

You can enable users with mixed digital IDs to roam with their Entrust security stores. You may want to do this if you want users to store their signing key pair in a third-party security store—typically a smart card—but keep their encryption key pair and history in an Entrust roaming security store.

How roaming works with mixed digital IDs

In order for users with mixed digital IDs to roam, their Entrust roaming security store must contain a signing key pair. This key pair is used during authentication to the Roaming Server. Even if the mixed digital ID already contains a signing key pair in a third-party security store, you still need to add a second signing key pair in the Entrust roaming security store. This key pair ensures that users can log in. Since this second signing key pair should not be used for anything other than authentication to the Roaming Server, it may contain a special extended key usage (EKU) that limits it to this usage.

Enabling users with mixed digital IDs to roam

The following procedure describes how to add a second signing key pair that is limited to Roaming Server authentication. There are many methods you can use to enable this capability, depending on how you set up your certificate policies in Security Manager. The following instructions cover only one method. You should review the

instructions and extrapolate a method that works in your Security Manager environment.

To add a Roaming Server authentication key pair

- 1** Have a Security Officer use Security Manager Administration to create certificate definition policies for each of the three key pairs (the normal two key pairs plus second signing key pair), as follows:
 - a** In the tree view on the left, expand **Security Policy > User Policies**.
 - b** Add the Roaming Authentication Policy certificate definition policy, and then do the following:
 - In the main window, under **Policy attributes**, scroll to the **CSP to manage keys** setting.
 - Ensure that this setting is left blank and click **Apply**.This configuration ensures roaming authentication key pair is stored with the Entrust Enhanced Cryptographic Service Provider, in an Entrust roaming security store.
- 2** Still in Security Manager Administration, export the `master.certspec` file.
- 3** Open the `master.certspec` file in any text editor.
- 4** Add the following lines for the certificate type to which you want to add the Roaming Server authentication key pair. In this example, the certificate type is `ent_roam_mixeddigitalID`. (This certificate type is not available by default.):

```
[ent_roam_mixeddigitalID Certificate Definitions]
;-----
;- Roaming Mixed Digital ID Certificate Type -
;- -
;- This certificate type defines three key pairs -
;- Encryption: has keyEncipherment key usage bit set -
;- Verification: has digitalSignature key usage bit set
;- RoamingAuth: has digitalSignature key usage bit + RoamSvrAuth EKU set -
;-----
1=Encryption
2=Verification
3=RoamingAuth
[ent_roam_mixeddigitalID Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001
[ent_roam_mixeddigitalID Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1
```

```
[ent_roam_mixeddigitalID RoamingAuth Extensions]
```

```
keyusage=2.5.29.15,n,m,BitString,1
```

```
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,2.16.840.1.114027.40.7
```

- 5 Save the `master.certspec` and import it back into Security Manager.
- 6 Associate the appropriate certificate definition policy with each certificate within the certificate type, as follows:
 - a In Security Manager Administration, expand **Security Policy > Certificate Categories > Enterprise > Certificate Types > <your certificate type>**
 - b Select the new key pair and select the Roaming Authentication Policy from the **Certificate Definition Policy** drop-down menu. This is the key pair stored in the Entrust roaming security store. It authenticates the user to the Roaming Server.
- 7 For new users, ensure they have the correct certificate type when you create them in Security Manager.
- 8 If you have existing users with Entrust digital IDs, use the **Notify Client** option in Security Manager Administration to notify Security Provider of the change. This notification is required because Security Provider does not automatically detect when new key pairs are added to a certificate type.

Users with mixed digital IDs can now roam with their Entrust security stores while having their signing key pair in a third-party security store.

Working offline as a roaming user

Security Provider for Windows users can work offline with their Entrust roaming security store. That is, they can be roaming users, even when the Entrust Authority Roaming Server is not available. To make this possible, the user must log in online at least once with their Entrust roaming security store or switch from using a Entrust desktop security store.

The ability to work offline with an Entrust roaming security store is controlled by Entrust policy. You can also choose to disable offline roaming by overriding Entrust policy through the use of the `DisableOfflineRoaming` setting in the Windows registry.

The offline roaming feature works by caching a copy of the Entrust roaming security store locally on the computer so that it is available when the Roaming Server is not. The default location of the cached copy is:

```
<Local Application Data>\Entrust Offline Security Store\
```

You can choose a different location by configuring the `OfflineRoamingFolder` setting.

The cached copy of the Entrust roaming security store is only valid for 14 days by default. After that time, the user cannot log in unless they have access to the

Roaming Server. To change the validity period of the cached copy, configure the `OfflineRoamingLifetime` setting.

When a user logs in to the cached copy of the Entrust roaming security store, a warning dialog box appears. It notifies the user that

- they are working offline
- that password changes are disabled
- digital ID management cannot occur
- changes to the Entrust security store options are lost when they access the online version of their Entrust roaming security store

You can disable this warning by configuring the `SkipOfflineRoamingNag` setting.

For details on all Roaming Server settings, see [“Roaming Server settings” on page 354](#) for further information.

Roaming Server problems

This section describes possible problems when using the Roaming Server with Security Provider for Windows.

Support for Entrust Enhanced CSP users only

The roaming functionality is only available for end users enrolling using the Entrust Enhanced Cryptographic Service Provider (CSP). Security Provider for Windows does not support roaming users enrolling using a third-party CSP.

Signing certificate is mandatory

A user must have a signing or dual-usage certificate in an Entrust security store to use the Roaming Server.

Choosing an algorithm for digital signature

Roaming Server does not support 6144 bit or longer key lengths for RSA. Configure the **Algorithm for digital signature** setting in Security Manager Administration, to 2048 or 4096 RSA algorithms.

Using Entrust TruePass

Entrust TruePass and Security Provider for Windows can coexist on the same machine.

Entrust TruePass 8.x understands the current Entrust security store; so, interoperability with Security Provider for Windows is seamless and there are no compatibility issues.

Using an application proxy server

Security Provider for Windows supports the use of an HTTP application proxy server for Web access. You can use the application proxy server independently or as an intermediary between it and any of the following:

- Security Manager proxy server
- Online Certificate Status Protocol (OCSP) responder
- HTTP-hosted CRLs

How the application proxy server connection works

Security Provider for Windows automatically sends HTTP messages through the application proxy server to the Security Manager proxy server, when you select the proxy server setting in Internet Explorer.

To configure the application proxy server settings in Internet Explorer

- 1** In Internet Explorer, select **Tools > Internet Options > Connections**.
- 2** Click **LAN Settings**.
The **Local Area Network (LAN) Settings** dialog box appears.
- 3** Select **Use a Proxy Server for your LAN**.
- 4** Do one of the following:
 - Enter your application proxy server address and port in the **Address** and **Port** text boxes and click **OK**.
 - Click **Advanced**. Enter your **Proxy address to use** and **Port** in the **HTTP** or **Secure** sections. Click **OK**.

Security Provider for Windows uses the end user's Internet Explorer settings to connect to the application proxy server. Once the connection is made, the message is passed to the target server through the application proxy server. If the **Use a Proxy Server for your LAN** option is not set, the message is sent directly to the target server.

Application proxy server authentication

Some application proxy servers require authentication before allowing access to a server on the Internet. The application proxy server supports the NTLM, Kerberos, and Anonymous authentication methods. The application proxy server determines if the application proxy server requires authentication before sending the message.

Note: If the authentication method is any other than NTLM, Kerberos, or Anonymous, an error message appears and the error is logged to `logmain.xml`.

Using Security Manager Proxy

Security Manager Proxy allows Security Provider for Windows to communicate with the Security Manager and back-end servers over the Internet, without making major changes to existing firewall settings. Security Manager Proxy encapsulates data packets with HTTP so that they can tunnel through firewalls.

Note: When connecting to Security Manager through the Security Manager Proxy, Security Provider for Windows does not follow LDAP search referrals.

You do not require a client-side proxy when using the Security Manager Proxy in your Security Provider for Windows architecture. Security Provider for Windows acts as the client-side proxy by wrapping data packets in HTTP (or HTTPS/TLS). Security Provider sends the wrapped data packets to the server-side proxy, which you will need to install and configure.

Once the server-side proxy receives the messages, they are unwrapped and forwarded to the appropriate server (for example, Entrust Authority Security Manager (CA), Entrust Authority Roaming Server, or the directory). The response information from the server is then re-wrapped by the server-side proxy in HTTP (or HTTPS/TLS) so that it can proceed back through the firewall to the Security Provider for Windows.

Security Provider for Windows supports the use of multiple Security Manager Proxies for failover purposes. If a connection to a Security Manager Proxy Server (a hostname and port number pair) is not successful, Security Provider caches tries the next available proxy server on the list until a successful connection is established. Failed connections remain inactive for one hour.

The instructions for configuring Security Manager Proxy are contained in the *Entrust Authority Security Manager Proxy Administration Guide*. Additionally, you may need to configure a few more variables to have the proxy work with Security Provider. See the procedure below for details.

To configure Security Manager Proxy for use with Security Provider

- 1** Install and configure Security Manager Proxy as described in the *Entrust Authority Security Manager Proxy Administration Guide*.
- 2** If you want to enable HTTPS/TLS between Security Provider and the proxy, ensure that you:
 - Follow the instructions in the *Security Manager Proxy Administration Guide* for enabling TLS/HTTPS.
 - Add these settings:

```
sf.tls.clientAuthenticationRequired 0
proxy.srv.tunnelhttp 1
```

to the server's `config.tcl` file. The first setting disables client certificate authentication, which is not supported with Security Provider. The second setting ensures that HTTP traffic is allowed, which is required in order for CRLs to be retrieved. (CRLs can only be retrieved over HTTP.)

- 3** If you want to use non-standard HTTP or HTTPS ports (the standard ports being 80 and 443, respectively), you must add:

```
port.srv.http.port <port_number>
```

or

```
port.srv.https.port <port_number>
```

to the server's `config.tcl` file. Replace `<port_number>` with the non-standard port number.

Using smart cards

Security Provider for Windows supports the use of smart cards in its architecture. Ensure that the smart card and smart card drivers are supported by Security Provider for Windows before installing the smart card drivers. Once the smart card drivers are installed, the Security Manager administrator must specify the smart card vendor's Cryptographic Service Provider (CSP). See the topic [“Configuring the smart card CSP” on page 182](#) for further information.

Topics in this section:

- [“Enrolling with a smart card” on page 180](#)
- [“Recovering with a smart card” on page 181](#)
- [“Logging in with a smart card” on page 182](#)
- [“Updates with a smart card” on page 182](#)
- [“Configuring the smart card CSP” on page 182](#)
- [“Generating keys within the smart card CSP” on page 183](#)
- [“Configuring Windows Smart Card Logon” on page 185](#)
- [“Moving an Entrust digital ID onto a smart card” on page 185](#)
- [“Using smart cards with Security Provider and EDS” on page 185](#)
- [“Troubleshooting smart card problems” on page 186](#)


Note: In order to use a smart card with Security Provider for Windows, you must have access to the CSP that supports that smart card on the machine where you insert the smart card.

Enrolling with a smart card

When users enroll for an Entrust Digital ID, their certificates can be stored on a smart card. Entrust recommends that the end user insert the smart card into the reader when the first page of the **Enroll for Entrust Digital ID** wizard appears.

When a user enrolls using a smart card vendor's CSP, the certificates are copied onto the smart card. The smart card is referred to as the smart card security store, because it stores the keys and certificates. Depending on the smart card in use, propagation of certificates from the smart card to the local certificate store may behave differently. Some smart card vendors only propagate one certificate to the local certificate store, while others propagate all certificates. For more information about certificate propagation, contact your smart card vendor.

Recovering with a smart card

Certificates stored on a smart card are automatically monitored and managed by a Security Provider for Windows feature called the Digital ID Monitor. The user is prompted with an Entrust Digital ID Recovery Request icon  in their taskbar notification area when their verification certificate on their smart card is expired or revoked. Clicking the icon opens the **Entrust Digital ID Recovery Request** dialog box. The end user can click one of the following buttons:

- **Recover**
Launches the **Recover Entrust Digital ID** wizard.
- **Remind me later**
Displays the dialog box at regular intervals until the end user begins the recovery process.
- **Delete Digital ID**
Allows a user to delete the Entrust digital ID associated with the certificate that needs to be updated. An example of an appropriate time to delete a digital ID is when a user's certificate stored on a smart card needs to be recovered, but the user no longer possesses the smart card.

Recovering a credential using the Recover Entrust Digital ID wizard

The user is expected to contact their administrator to obtain activation codes and possibly other information, to complete all steps in the wizard. Entrust recommends the user insert the smart card into the reader when the first page of the **Recover Entrust Digital ID** wizard appears.

When a user recovers using a smart card vendor's CSP, the certificates are copied onto the smart card. Depending on the smart card in use, propagation of certificates from the smart card to the local certificate store may behave differently. Some smart card vendors only propagate one certificate to the local certificate store, while others propagate all certificates. For more information about certificate propagation, contact your smart card vendor.


Note: Entrust digital ID recovery should be performed onto a clean smart card. Obsolete certified key pairs may not be deleted. Space can be taken up unnecessarily if they are not removed. Use the smart card vendor's administration utility to remove them, before the recovery.

Logging in with a smart card

Note: When using a smart card with Security Provider for Windows, the end user does not log in using the **Entrust Security Store Login** dialog box. The end user logs in to the smart card vendor's dialog box that corresponds with the smart card. When a user has keys and certificates stored on a smart card and in the Entrust security store, the end user is prompted to log in using the smart card vendor's dialog box and the **Entrust Security Store Login** dialog box.

By default, certificates are not removed from the user's personal certificate store when the smart card is removed from the reader. This feature is configurable. The certificates can be removed from the user's personal certificate store when the Smart Card is removed using the `EnableSmartCardCertificateRemoval` registry setting. See [page 381](#) for details about using this setting.

Updates with a smart card

Certificates stored on a smart card are monitored and managed by a Security Provider for Windows feature called the Digital ID Monitor. When keys and certificates on a smart card need to be updated, the user is prompted with an Entrust Digital ID Update Request icon  in their taskbar notification area. Clicking this icon opens the **Entrust Digital ID Update Request** dialog box. The end user can click one of the following buttons:

- **Update**
Updates the Entrust digital ID automatically.
- **Remind me later**
Displays the dialog box at regular intervals. If the end user continues to click this button they may miss the opportunity to update their digital ID and they may need to recover it.
- **Delete Digital ID**
Allows a user to delete the digital ID associated with the certificate that needs to be updated. An example of an appropriate time to delete a digital ID is when a user's certificate stored on a smart card needs to be updated, but the user no longer possesses the smart card.

Configuring the smart card CSP

When using smart cards with Security Provider for Windows, you must configure the name of the smart card vendor's CSP in the appropriate location for the certificates to be stored on the smart card.

Note: If you're using a CardMS (see [“Using a Card Management System” on page 188](#) for details), you do not need to specify the smart card vendor's CSP.

Security Manager 8.x or higher

Using Security Manager 8.x or higher, you configure the smart card vendor's CSP in a setting called **CSP to manage keys** in the certificate definition policy. The value can be a specific CSP name, which is useful if your enterprise has standardized on one smart card. Alternatively, the value can be set to `Any SC`. This allows the user to select a smart card CSP from a list during enrollment or recovery.

You also need to configure a setting allowing you to identify the algorithm to be used for the user's key pair, called the **Algorithm for key pair** setting in the certificate definition policy.

Note: You do not need to configure either setting if you are integrating with a CardMS. For details on the integration, see [“Using a Card Management System” on page 188](#).

Consult your smart card vendor's documentation to ensure that you configure a supported algorithm. See [“Certificate definition policy settings” on page 259](#) for further information on configuring certificate definition policies and certificate definition policy settings.

Generating keys within the smart card CSP

During an enrollment, recovery, or key update of an Entrust digital ID, the CSP does not generate client-generated, non-archived, encryption, or dual-usage key pairs. Instead, Security Provider generates the key pair securely in memory and imports it (in a protected manner) into the destination CSP.

You may want to change the default behavior so that the smart card CSP does generate key pairs. Having key pairs generated within the CSP ensures that they are created directly on the user's smart card rather than imported onto the smart card.

Note: Signing key pair generation always occurs within the CSP and is therefore not affected when you configure key generation following the procedure below.

Configuring this behavior is supported with Security Manager 8.x and higher. The following instructions describe how to enable key generation within the CSP.

To generate keys within the CSP

- 1 Have a Security Officer use Security Manager Administration to do the following:

Note: If this attribute is already in the `master.certspec` file and you just need to change the setting, you can skip this step and proceed directly to [Step 2](#).

- a** In the `master.certspec` file, under the `[polcert_certdefn Attributes]` heading, add:

```
; -----  
; certificate key generation settings  
; -----  
cd_key_gen_in_csp=1.2.840.113533.7.77.46.5.10,Boolean,<cd_key_gen_in_csp>
```

- b** Under the `[Variables]` heading, add:

```
; -----  
; certificate key generation settings  
; -----  
cd_key_gen_in_csp=Boolean,Force client key generation in CSP:,Create key (if not  
backed up) directly in the CSP.,Range,0,1
```

Note: The identifier `cd_key_gen_in_csp` can be replaced with any string. The OID, however, is registered with Security Manager Administration and is not arbitrary.

- c** In the `entmgr.ini` file, under the `[Default Variable Values]` heading, add:

```
cd_key_gen_in_csp =0
```

- 2** In Security Manager Administration, expand the **User Policies** node.
- 3** Select the encryption or dual-usage certificate policy that you are using.
- 4** On the **General Information** tab, under **Policy Attributes**, enable **Force client key generation in CSP**.
- 5** Click **Apply**.
- 6** In Security Manager, ensure that the symmetric algorithm is supported by the destination CSP. To set the symmetric algorithm, use the Security Manager Control Command Shell and set the `policy proto-enc` policy management command. For more information, see your Security Manager documentation.
For example, if CAST is set as the symmetric algorithm in Security Manager, and the user's key pair is generated by a smart card CSP, the smart card CSP must support CAST. If it does not, the enrollment, recovery, or key update will fail.
- 7** Ensure that the certificate policy is associated with a certificate type, and that the certificate type is associated with your smart card users.

Configuring Windows Smart Card Logon

Windows Smart Card Logon is a Windows feature that forces users to use their smart cards to log in to Windows. For more information on how to configure Security Provider with Windows Smart Card Logon, see the *Windows Smart Card Logon and Entrust Entelligence Security Provider for Windows Integration Guide* available on the Entrust Entelligence Security Provider for Windows pages at <https://www.entrust.com/trustedcare/>.

Moving an Entrust digital ID onto a smart card

You can change a digital ID storage location, from an Entrust security store (.epf) to a smart card. This process is done using Security Manager.

The details of moving a security store to a smart card are provided in the section [“Moving an Entrust digital ID from one security store to another”](#).

Using smart cards with Security Provider and EDS

After migrating users from Entrust Desktop Solutions (EDS) to Security Provider (see [“Migrating smart cards from EDS to Security Provider” on page 103](#)), you can enable a feature that allows users to use their smart cards on both Entrust Desktop Solutions (EDS) and Security Provider for Windows without needing to recover or perform any additional configurations on their digital ID. For example, a user could log in to Entrust Desktop Solutions to encrypt a file (for example, `file1.txt`), and then switch to a different computer with Security Provider installed and sign another file using Security Provider. The user could then switch back to EDS and decrypt `file1.txt` without any problems.

Some preparation is required to enable this feature, as described in the following procedure.

Note: While logged in to Entrust Desktop Solutions, there is no digital ID management available. The digital ID becomes manageable as soon as users log in to Security Provider.

To enable the use of smart cards with EDS and Security Provider

- 1 If users' Entrust digital IDs were created with EDS, ensure you migrate these digital IDs from EDS format to Security Provider format using the smart card migration utility. See [“Migrating smart cards from EDS to Security Provider” on page 103](#) for details.
- 2 Create a Security Provider installation package by running through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#). Fill out the pages in the wizard, as described in the

following table.

Note: Instead of using the Custom Installation wizard, you can use Microsoft Group Policy to push out the registry setting described below. The registry value is written to your users' registries.

On this page in the wizard...	Do this...
Select Application Features	Under Entrust Digital ID for Users , enable the Smart Card Compatibility option.
Specify Additional Registry Values	<ul style="list-style-type: none">• Add the <code>RemoveEDSSupport</code> registry setting, if required. By default, the setting is '0' which means that users can switch back to EDS after logging in to Security Provider. Set it to '1' to prevent users from switching back to EDS. For details, see "RemoveEDSSupport" on page 386.• Some eTokens or smart cards require additional registry settings. Check the registry settings marked <i>EDS notification plugin</i> (in the left column of the table) starting on page 386 to see if these settings apply to your installation.

- 3 Proceed to the end of the wizard and click **Finish** to save your settings.
The `.mst` file is updated with your new settings. You have now enabled smart card users to switch between EDS and Security Provider.
- 4 Package, test, and distribute the installation to your users. For details, see ["Deploying Security Provider for Windows" on page 281](#).

Troubleshooting smart card problems

This section describes possible problems when using smart cards in a Security Provider for Windows environment.

Smart card CSP

If you have trouble enrolling a smart card, you may need to update your system. To determine if the CSP is on your system, see the Microsoft knowledge base article at <http://support.microsoft.com/kb/909520>.

Once the CSP is on your system, ensure that the registry key `AllowPrivateExchangeKeyImport` is set to 1. It is located under either:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ Microsoft Base Smart Card Crypto Provider
```

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\ Microsoft Base Smart Card Crypto Provider

Key or certificate updates fail

Old encryption keys and certificates in an Entrust digital ID are archived. The key history grows over time due to key rollovers and forced updates. These events add information to a smart card. If the smart card becomes full, Security Provider for Windows does not delete old keys and certificates in order to make room for new data. Once the card is full, the user must do one of the following; otherwise, key updates will fail:

- recover to a larger card
- remove old key data and let Security provider for Windows manage old smart card keys (see [“Additional Entrust digital ID management for smart cards” on page 88](#))

Smart card only users

When you deploy Security Provider for Windows to smart card only users, you may want to configure Security Provider for Windows to not display the taskbar status icon. This way, the **Log in** menu option does not display, as smart card users never use the **Entrust Security Store Login** dialog box to log in. The disadvantage of removing the taskbar status icon is that it also removes the **Help** menu option. The end user then has to navigate to the default installation path C:\Program Files\Entrust\ESP\1033\eesp.chm (32 bit) or C:\Program Files (x86)\Entrust\ESP\1033\eesp.chm (64 bit) to access the online help files. The folder 1033 contains the English version of the help files. If your version of ESP has been localized, the translated files will be in the folder with the language code ID for that language (for example, French (France) is 1036).

Smart cards and the nonrepudiation private key

The Entrust Enhanced CSP forces secure signing authentication, through the use of password prompts, whenever the nonrepudiation private key is accessed. It is up to smart card CSP vendors to support these authentication rules, through the use of password prompts, whenever the nonrepudiation key is accessed.

Smart cards and Microsoft roaming support

Smart cards are supported in a Microsoft roaming environment, when the CA root certificate exists on the Trusted Root store on the computer you are roaming to.

Using a Card Management System

A Card Management System (CardMS) is a third-party server application that performs basic smart card management functions such as disabling a card. To give the CardMS additional functionality, you can integrate it with the Entrust Authority Security Toolkit for the Java Platform. With this integration enabled, the CardMS is able to create and recover Entrust digital IDs on smart cards; however, updating these digital IDs is still not possible. To enable update functionality, you must integrate the CardMS with Security Provider. When the integration is complete, Security Provider detects when a key update is required, and sends a message to the CardMS telling it to perform the update.

For more details on the Security Provider/CardMS integration, see the following sections:

- [“Functionality not available with a CardMS” on page 188](#)
- [“Integrating Security Provider and a CardMS” on page 189](#)

Functionality not available with a CardMS

The following functionality and features are not available for users specified as CardMS users. The functionality is still available to all non-CardMS users managed by Security Provider.

Table 18: List of unavailable features and functionality

Feature or functionality not available	Details
Key updates on V1 Entrust digital IDs	A CardMS cannot update V1 Entrust digital IDs. When an update is required, users with V1 digital IDs see an error message stating that the update failed and a recovery must be performed. When they recover, Security Manager 8.x migrates their digital IDs to V2 and subsequent updates should succeed. For details on V1 digital IDs, see “Entrust digital ID and security store versions and contents” on page 499 .
Automatic move user	The automatic move user feature in Security Manager 8.x is not available when a CardMS is present. Users must manually recover their certificates signed by the new CA.
Mixed Entrust digital IDs	Entrust digital IDs with keys in more than one security store—for example, an Entrust security store (.epf) and a smart card security store—are not supported when a CardMS is present.

Table 18: List of unavailable features and functionality

Feature or functionality not available	Details
Update notifications and other management dialog boxes	<p>When a CardMS is configured, Security Provider no longer displays key management dialog boxes (for example, the key update notification). It is up to the CardMS components to determine what to display.</p> <p>Note: Even though Security Provider no longer displays dialog boxes, it continues to display errors related to key management.</p>

Integrating Security Provider and a CardMS

You can integrate a Card Management System with Security Provider for Windows to manage smart cards. The following steps describe how.

To integrate Security Provider and a CardMS

- 1 Ensure you installed a supported CardMS. For details about the software you require in a CardMS deployment with Security Provider, see the Entrust TrustedCare Platform Support and Integration site.
- 2 Using a Security Manager interface such as Security Manager Administration, do the following:
 - a Create a new user policy. You should now have a user policy with **Client Management** set to CardMS.
 - b Create a role. You should now have a role associated with the CardMS user policy.
 - c Ensure that the CardMS role is associated with the users who will use the CardMS to manage their Entrust digital IDs. Users with this role lose the functionality listed in [“Functionality not available with a CardMS” on page 188](#).

For information on creating policy and roles, see the *Entrust Authority Security Manager Administration User Guide*.

- 3 Obtain the CardMS client .dll file from the smart card vendor and place it in the root folder of the unzipped Security Provider software package.
- 4 Determine the CardMS client's name as follows:
 - a At a command prompt, type a command like this:
`regsvr32 <path_to_client_dll>`
For example:
`regsvr32 c:\EESP_extracted_zip\CardMSclient.dll`
 - b At a command prompt, type `regedit`. The Registry Editor opens.

- c In the tree view on the left, expand
HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\ESP\CardMS\
 - d Write down the CardMS name exactly as it appears under \CardMS key in the tree view. You need this name in a later step.
- 5** Using the **Custom Installation** wizard, enable the CardMS feature as follows:
- a Run through the wizard, as described in [“To customize the installation using the wizard only” on page 290](#), until you reach the **Specify PKI Information** page.
 - b On that page, select the Entrust CA with which you want to integrate your CardMS.
 - c Click **Edit**.
 - d Select the **CardMS** tab.
 - e Select **Enable Card Management System Integration (CardMS)**.
 - f In the text box, type the CardMS client name that you wrote down in [Step 4](#).
 - g Proceed through the wizard until you reach the **Include Additional Files** page.
 - h Click **Add**.
 - i In **File name and source path**, specify the CardMS client .dll file.
 - j In **Destination path and folder name**, specify the folder on the end user's computer to place the .dll when the user installs Security Provider.
 - k Select **Self-Register** and **Remove during uninstall**.
 - l Click **OK**.
 - m Proceed to the end of the wizard and click **Finish** to save your settings.
The .mst file is updated with your new CardMS settings.
- 6** Package the installation, test it, and distribute it to your users. For details, see
- [“Packaging the installation” on page 297](#)
 - [“Testing the installation” on page 303](#)
 - [“Distributing the installation package” on page 304](#).

The following CardMS-related settings are written to the user's registry when the user installs Security Provider:

- DLLPath
- CardMSUpdatesPerformedBy

For details on these settings, see [“CardMS settings” on page 368](#).

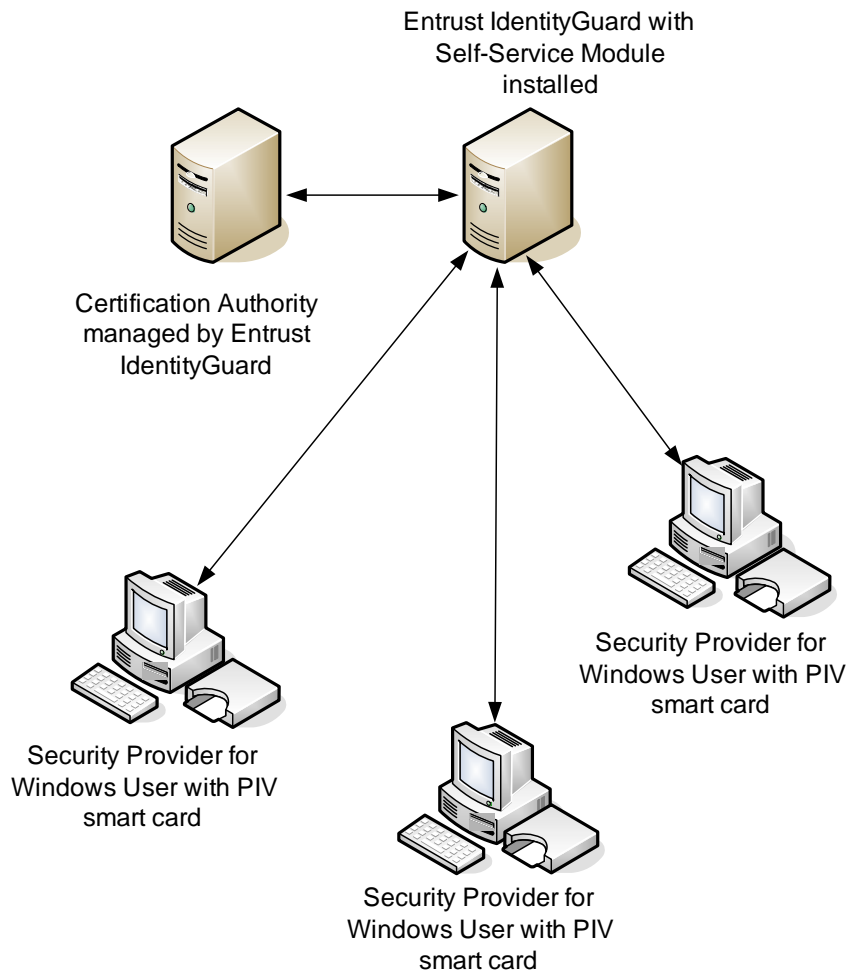
You have now integrated the CardMS and Security Provider. The CardMS now performs key updates on Entrust digital IDs, when required.

Using PIV smart cards with Entrust IdentityGuard

This section includes the following topics:

- [“Managing an Entrust PIV Card” on page 192](#)
- [“Resolving a blocked Entrust smart card” on page 193](#)
- [“Changing a PIN” on page 194](#)
- [“Using the PIV smart card” on page 196](#)

Figure 15: Entrust IdentityGuard and Security Provider For Windows



Managing an Entrust PIV Card

Companies using Security Provider and Entrust IdentityGuard Self Service Module can use them together to manage PIV smart cards. If you have decided not to make the Self-service Module available to your Security Provider users, some Administrator intervention is required.

- Security Provider uses the Microsoft Base Smart Card Cryptographic Provider for cryptographic operations. This CSP is included with Windows operating systems and does not need to be specified in the Security Provider installation.
- Security Provider provides a client-side interface for such operations as PIN unblock and reset and allows the user to initiate operations such as digital ID recovery. Security Provider can also generate keys on the client when key updates or recoveries are required.
- Because PIV smart cards have a limited storage space, older keys may not be stored on the PIV card. These keys may still be required to access secured documents and email. Security Provider works with Entrust Authority Security Manager (the CA) to download these keys and provides a CSP.
- Security Provider for Windows works with Entrust IdentityGuard Self-service Module to recover user credentials when required.
- Security Provider monitors the user credential and notifies the user when it approaches the certificate's end-of-life.

Updating a PIV smart card credential

The procedure in this section requires the user to be connected to Entrust IdentityGuard Self-service module. The `IdentityGuardURL` registry setting (see [page 372](#)) must be populated. The URL can be specified when the .mst file is configured using the Custom Installation Wizard.

To update the smart card credential

- 1** The user receives a message from Security Provider that an update is required.
- 2** In the **Digital ID Update Request** dialog, the user clicks **Update**.
- 3** In the **Select Entrust Smart Card** dialogue the user selects the PIV smart card (the card should already be highlighted in the list) and clicks **OK**.
- 4** In the **Encode Entrust Smart Card** dialog, the user selects **OK**.
- 5** The user is prompted for their PIN.
- 6** When the card is encoded a success message appears.
- 7** The user is prompted to remove and re-insert their card.

- 8 Keys that are not current but may be required to access encrypted files and messages (spillover keys) may not fit on the PIV card. These keys are downloaded to the user's machine.
 - 9 The user is asked to provide their PIN.
 - 10 When the additional keys have been installed, a success message appears.
- See [page 381](#) for details about using this setting.

Resolving a blocked Entrust smart card

Entrust smart cards are blocked if the user enters an incorrect PIN several times, exceeding the maximum number of login attempts.

The card is unblocked if the user initiates a PIN reset.

When the card is blocked it can be unblocked from the **Unblock Entrust Smart Card** dialog.

Security Provider generates a challenge which is used by IdentityGuard to create a response. The response is entered into the response field of the unblock dialog. Enter and confirm a new PIN.

The card can be unblocked using Entrust IdentityGuard Self Service module.

Note: Not all smart cards can be unblocked using Security Provider. The smart card must be capable of generating a challenge. See the *Entrust IdentityGuard Administration Guide* for information about this feature.

To unblock the card using the Entrust IdentityGuard Self-Service Module

- 1 Log into the Self-Service Module.
- 2 Enter the challenge into the correct field in Entrust IdentityGuard.
- 3 Record the response returned by Entrust IdentityGuard and enter it into the **Response** field in the Security Provider **Unblock Smart Card** page.
- 4 Enter and confirm a new PIN (that satisfies the PIN rules).
- 5 Click **OK**.

If your organization is not using Entrust IdentityGuard Self Service Module, the user should to call their administrator. The administrator uses the challenge from the user's **Unblock Entrust Smart Card** dialog to obtain a response from Entrust IdentityGuard. The administrator verifies the identity of the user and relays the response so the smart card can be unblocked.

Note: The unblocking operation may fail if too much time elapses and the challenge or response become stale. It may also fail if the card is removed from the reader before the operation completes. If it fails, after the error message is accepted, the information in the dialog is cleared and the user can start again.

Changing a PIN

When a user changes their PIN on an Entrust smart card, the PIN policy is retrieved from the smart card and displayed on the **Change Entrust Smart Card PIN** dialog. If card is not an Entrust smart card, the policy is not displayed.

The default PIV PIN policy is:

- Min Length: 6
- Max Length: 8
- Only Numeric characters are allowed

Entrust PIV smart card PINs can have the following characteristics:

- minimum length of 1 to 8 characters
- numeric characters: Allowed, Required, or Not Allowed
- lower case alphabetic characters: Allowed, Required, or Not Allowed
- upper case alphabetic characters: Allowed, Required, or Not Allowed
- non-alpha-numeric characters: Allowed, Required, or Not Allowed

Note: PIN rules are configurable using Entrust IdentityGuard. See the Entrust IdentityGuard documentation for information.

Security Provider can force users to change their administrator-assigned smart card PIN either immediately or after a set number of uses. The number of uses is configured using Entrust IdentityGuard and enforced by Security Provider when the `PIVEnforceAdminAssignedPINChange` registry setting is enabled. By setting the `PIVEnforceAdminAssignedPINChange`, the Administrator causes Security Provider not to accept the administrator-supplied PIN when the set number is reached. See `PIVEnforceAdminAssignedPINChange` on page 382 for information about configuring this registry setting.

Note: When using the `PIVEnforceAdminAssignedPINChange` be sure that the number of PIN uses is set to a high enough number. The smart card is blocked unless the PIN is changed before the maximum number of successful authentications is reached.

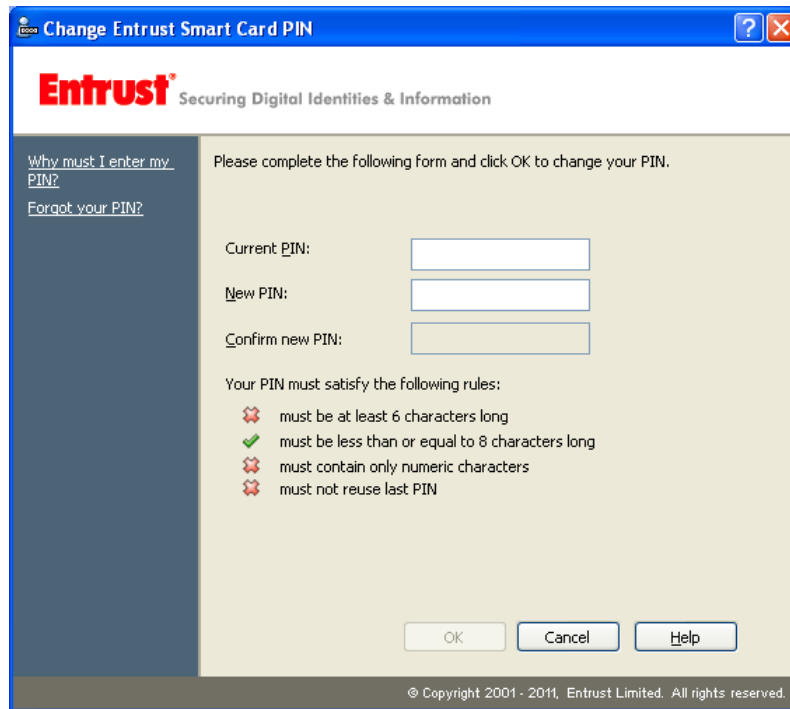
The card counts the number of times the PIN is presented, and each successful Windows login may present the PIN several times. Because the number of PIN authentications counted by the smart card for each successful Windows login varies, the card may allow a smaller number of Windows logins without a PIN change than expected.

To change a PIN

- 1 From the Windows **Start** menu, select **Change Entrust Smart Card PIN**.
- 2 If more than one smart card is available, a dialog appears asking the user to select a smart card. A message asking the user to insert the smart card in the reader is displayed if the smart card is not found.

Note: Administrators can limit the number of options that appear in the **Select Entrust Smart Card** dialog by hiding reader options using the `PIVHiddenReaders` registry setting. See page 402 for information about this registry setting.

- 3 This opens the **Change Entrust Smart Card PIN** dialog.



- 4 After a PIN is entered that conforms to the rules, click **OK** to complete the change.

Using the PIV smart card

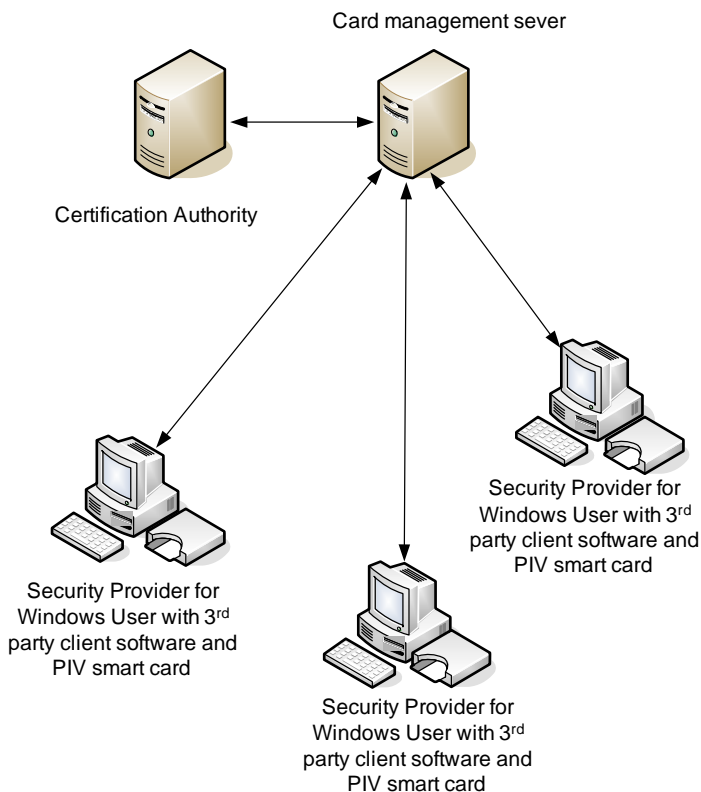
When the user accesses secure network resources or performs another cryptographic operation (for example, encrypting a file), the Cryptographic Service Provider (CSP) may ask the user for a PIN. The PIN is used to authenticate the user. If authentication is unsuccessful the dialog displays the number of allowed retries.

The PIN may not be required if the keys being used do not require the user to authenticate each time (see the *Entrust IdentityGuard Administration Guide* for details). If the smart card is not connected to the smart card reader, the user is asked for a smart card. When the card is connected to the reader, the requested process continues.

Using Security Provider for Windows with non-Entrust PIV smart card management software

Security Provider for Windows works with some third party PIV smart card management software. See the Platform Support and Integration page in Entrust's TrustedCare Web pages for information about specific management software and PIV smart cards.

Figure 16: Security Provider used with non-Entrust management system



Depending on what features are supported by your management software and how the software is configured, Security Provider for Windows is capable of supporting all of the features mentioned in the section, [“Managing an Entrust PIV Card” on page 192](#) with the exception of recovering and updating the smart card user credential. Some features may not be supported with non-Entrust smart card

management systems and departures from the procedures in the previous section may be noticed. Features supported with third party may include:

- PIN reset and PIN change
- Key recovery
- Key update
- managing older keys that cannot be stored on the PIV card (spillover keys)
- notifying the user when their credential approaches end-of-life

Note: If you are not using Entrust IdentityGuard self-service Module, and want to include specific information for the user in this message, use the registry setting `PIVMessageForRequiredUpdatesWithNonConfiguredIDG` (see [page 372](#)).

Using Microsoft Application Virtualization (App-V)

Security Provider for windows will work with virtual CAPI enabled applications. To function, Security Provider must be installed on the client machine.

- 1** Configure the virtualized application(s) (for example Microsoft Office 365) as recommended by Microsoft's App-V documentation.
- 2** Security Provider must be installed normally on the client machines that will use the virtualized application.
- 3** Security Provider will treat the CAPI enabled application(s) as if they were installed locally.

Attention: Security Provider does not work as a virtualized application and will not function properly if it is installed as a virtualized application. Install the Security Provider software locally, on client machines.

Bundled applications

This chapter provides information on end-user applications within Security Provider for Windows. These applications require a directory, and can be deployed with or without the Entrust Authority Security Manager CA.

The following end-user applications are available with Security Provider:

- [“File Security application” on page 202](#)
- [“Password Encrypt application” on page 221](#)
- [“TrueDelete application” on page 230](#)
- [“Certificate Explorer application” on page 234](#)
- [“Customer support utility” on page 248](#)

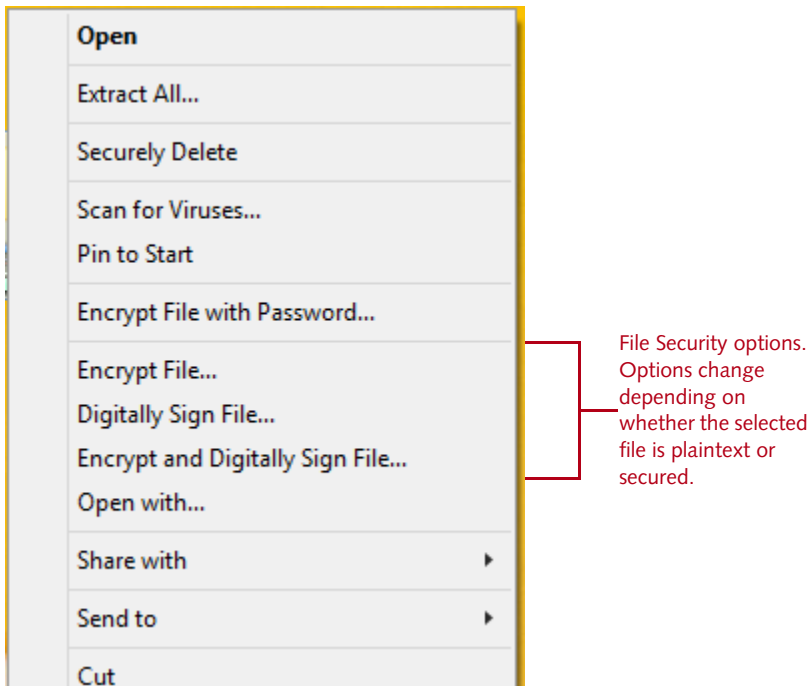
File Security application

Security Provider for Windows includes a File Security application that allows users to encrypt, decrypt, sign, timestamp, and verify files. Users must have a digital ID for these features to work.

Note: The file security feature considers a semicolon to be an illegal character in a filename. Files with a semicolon in the filename do not decrypt correctly.

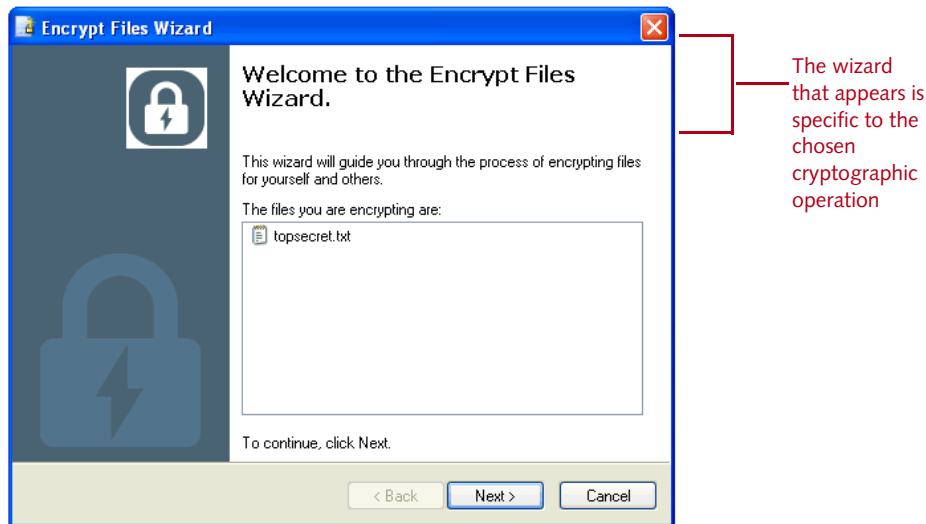
To use the File Security applications, users right-click a file and select the appropriate cryptographic option from the pop-up menu (see [Figure 17 on page 202](#)). A wizard then appears, guiding the user through the encryption and digital signature operation ([Figure 18 on page 203](#)). Users can also view the security properties of the file.

Figure 17: File security pop-up menu



Note: You can control which of these menu items appear in the right-click menu. See [page 442](#) for details about the registry setting.

Figure 18: Encryption wizard



For more on the File Security application, see the following sections:

- [“File security functionality, in detail” on page 203](#)
- [“Enabling the File Security application” on page 205](#)
- [“Using the File Security application” on page 210](#)

File security functionality, in detail

The File Security application includes the functionality described in Table 19. For information on the **Custom Installation** wizard options related to file security, see [“Entrust File Security settings” on page 430](#). For steps on how to digitally sign and encrypt files, see the Security Provider online help or the *Security Provider for Windows and Outlook Quick Start Guide*.

Table 19: File security functionality

Functionality	Description
sign and encrypt files with a certificate	Users can sign and encrypt files for themselves, other individuals, and Personal Encryption Groups. (Personal Encryption Groups are logical groupings of people.) The files are encrypted and/or digitally signed using the S/MIME format and are appended with a .p7m or .ent extension. All file types can be encrypted and/or signed except .ent or .p7m files, which are already secured. You cannot encrypt and digitally sign folders.

Table 19: File security functionality (continued)

Functionality	Description
timestamp a signature	<p>When users digitally sign a file, they can choose to timestamp the signature. A timestamp provides proof of the date and time when a document was digitally signed. Timestamping requires a Timestamp server that supports RFC 3161.</p> <p>The timestamp server options are configured when you configure the file security options from the installation wizard. After you click Add, in the popup page, enter the server name, a friendly name, the hash algorithm from pull down menu (SHA-1, SHA-256, SHA-384, SHA-512), and the URL of that server. If you want to use different hash algorithm for the same server, add a policy OID, specify a meaningful friendly name for the policy (for example three names might be, internal, external, and proprietary information), and select the algorithm to use. The friendly name of each policy can be selected from the user's file encryption wizard.</p> <p>Security Provider accepts multiple timestamp servers and multiple policies for each server. If you have multiple policies, you can to specify a default policy.</p> <p>See "Timestamp server settings" on page 445 for information about specific settings.</p>
decrypt and verify	<p>Users can decrypt and verify files with .p7m or .ent file extensions created by Security Provider, Entrust Solo.</p> <p>When decrypting and opening a file, Security Provider creates a plaintext version in the same location as the original .ent or .p7m file. The plaintext version launches inside the associated application (for example, Microsoft Word). If users modify the file, they must save it, delete the original .ent or .p7m file, and then re-encrypt and/or sign the modified plaintext file.</p>
decrypt to local drive	<p>When Security Provider decrypts a file in a network folder, the default action is to create a plaintext version in the same network folder. You can use the Prevent network folder decryption option in the Custom Installation wizard or the registry setting <code>PreventNetworkFileDecrypt</code> to prevent creation of the plaintext version on the network. When this key is set, the user is prompted for a local folder to hold the plaintext version.</p>
view properties of signed and/or encrypted files	<p>By right-clicking a file and selecting Properties, users can view the security properties of signed and/or encrypted files, such as who signed a file, when, with what algorithm, and whether a timestamp was applied. If the file's signing certificate is untrusted, an additional two buttons appear. One lets you view the certificate and the other tells Security Provider to trust the signer.</p>

Table 19: File security functionality (continued)

Functionality	Description
check for weak or insecure hashing algorithms	Security Provider for Windows lets you flag specific hashing algorithms as weak or insecure to provide protection as current hashing algorithms become less secure. Designate specific algorithms as weak or insecure using the <code>InsecureFileHashAlgorithms</code> and <code>WeakFileHashAlgorithms</code> registry settings.
monitoring of opened, decrypted files	<p>You can configure Security Provider to monitor open decrypted files. When users close the application associated with a decrypted file, Security Provider displays a notification asking whether they want to delete the plaintext file. This notification comes in two varieties: one for users who have not modified the plaintext file and one for users who have modified the file.</p> <p>The monitoring feature ensures that plaintext files are not left behind on users' systems. This is especially important if an encrypted file is being opened from a temporary folder, such as one created by Outlook when users open attachments.</p> <p>If a user edits and saves a file that was previously encrypted with a <code>.p7m</code> extension, they are asked if they want to re-encrypt the file. This feature does not work with <code>.ent</code> files.</p> <p>Note: Occasionally, Security Provider cannot monitor opened files, or must end the monitoring before users close the application. These issues arise from a lack of compatibility between Security Provider's monitoring service and the low-level design of the application in which the file is opened. In such cases, Security Provider displays a notification indicating the problem and asks whether the user wants to delete the plaintext file.</p>
command line operations	You can encrypt, decrypt, sign, and verify files from the command line. See "Using the File Security application" on page 210 for details.

Enabling the File Security application

The following instructions describe how to enable and customize the File Security application:

- ["Preconfiguration step" on page 205](#)
- ["Enabling and customizing the File Security application" on page 208](#)

Preconfiguration step

Sometimes, users' key pairs have extended key usages (EKUs) that restrict which applications can use the keys. For example, if a key pair has the Microsoft EFS EKU, only the EFS application can use the key pair. Furthermore, certain applications look

for a specific EKU, and if it is not present, will not use the key pair. Microsoft EFS is an example of such an application.

In order to allow other applications to use a key pair with an EKU, including Security Provider's File Security application, you must give the key pair the `anyExtendedKeyUsage` EKU. The `anyExtendedKeyUsage` EKU is used when other EKUs are present, and indicates that any application can use the key pair; it also allows other EKUs to remain so that applications that require them, like Microsoft EFS for instance, can continue to use the key pair.

The following instructions describe how to check for EKUs and add the `anyExtendedKeyUsage` EKU, if necessary.

Note: All instructions in the following procedure assume you are using Security Manager. If you are not, consult your third-party documentation for information on how to check and set EKUs.

Note: If your certificates contain the Secure Email EKU (OID 1.3.6.1.5.5.7.3.4.), you do not have to set the `anyextendedkeyusage` EKU. Instead, you can enable the `FileAllowEmailProtectionEKU` registry setting, which accomplishes the same goal. You might find that enabling this setting is easier than setting the `anyExtendedKeyUsage`. For more on the registry setting, see page 443.

To check for EKUs, and add the `anyExtendedKeyUsage` EKU

- 1 Have a Security Officer use Security Manager Administration to export and open the `master.certspec` file.
- 2 Scroll to the [Extension Definitions] section. It is about 1/8th of the way down the file.
- 3 Under the [Extension Definitions] section, look for the certificate type that your users are using. For example, the section for the two key-pair certificate type looks similar to the following:

```
[ent_twokeypair Certificate Definitions]
;-----
;- Two Key-pair Certificate Type -
;- -
;- This certificate type defines two key pairs -
;- Encryption: has keyEncipherment key usage bit set -
;- Verification: has digitalSignature key usage bit set -
```

```

;-----
1=Encryption
2=Verification

[ent_twokeypair Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_twokeypair Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1

```

- 4 Check whether the key pairs for the certificate type have any extended key usages (EKUs) defined. EKUs are defined using the `extkeyusage` setting. The following is an example of an EFS key pair extension that has an EKU:

```

[ent_nonrepud_and_efs EFS Extensions]
keyusage=2.5.29.15,n,m,BitString,001
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.4.1.311.10.3.4

```

Extended key usage for EFS key pair

- 5 If an `extkeyusage` setting is present, add the OID 2.5.29.37.0 (shown in bold in the next example) to the end of the string, separating it from the other OIDs using a space. If `extkeyusage` is not present, do not add the OID.

Note: Due to space constraints, the OID appears on a separate line in this example. It must be on the same line in your `master.certspec` file.

```

[ent_nonrepud_and_efs EFS Extensions]
keyusage=2.5.29.15,n,m,BitString,001
extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.4.1.311.10.3.4
2.5.29.37.0

```

anyExtendedKeyUsage

The OID in bold, above, represents the `anyExtendedKeyUsage` EKU. This EKU allows any application to use the key pair.

- 6 Save the `master.certspec` file and then import it back into Security Manager Administration.
- 7 If your users have existing Entrust digital IDs, update their key pairs.
You have now defined the `anykeyusage` for key pairs that have other EKUs defined.

Enabling and customizing the File Security application

The following instructions describe how to enable and customize the File Security application using the **Custom Installation** wizard and Microsoft Group Policy. See the instructions that apply to you:

- [“To enable and customize the File Security application using the wizard” on page 208](#)
- [“To enable and customize the File Security application using Group Policy” on page 209](#)

To enable and customize the File Security application using the wizard

- 1 Run through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#). Fill out the pages in the wizard, as described below:

On this page in the wizard...	Do this...
Select Application Features	<p>Ensure that the File Security option is selected.</p> <p>Optionally, disable the Encryption/Digital Signature option. With this option disabled, users can still decrypt and verify files as long as the root File Security option is activated.</p>
Specify Directory Information	<p>If you activated the Encryption/Digital Signature option, add the LDAP directories that you want Security Provider to connect to in order to find users' encryption certificates. The directories do not have to be associated with Security Manager, an Entrust CA. To add a directory, do one of the following:</p> <ul style="list-style-type: none"> • click Add and fill out the fields For detailed descriptions of each setting, see “Directory settings” on page 331. • click Import and specify your Security Manager's <code>entrust.ini</code> file The directory information is contained in the <code>entrust.ini</code> file.

On this page in the wizard...	Do this...
Entrust File Security Options	<p>Optionally, fill out the fields. For descriptions of each setting, see “Entrust File Security settings” on page 430. The settings specify:</p> <ul style="list-style-type: none"> • whether the File Security application is able to use certificates with the Secure Email ECU to perform secure operations • which algorithms are used or available for use and how they appear in the GUI • which directory attribute is searched • the explanatory text in the Search for People dialog box • whether plaintext file monitoring is on (default is on)

- 2 Proceed to the end of the wizard and click **Finish** to save your settings.
The .mst file is updated with your new file security settings. You have now customized the File Security application.
- 3 Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

To enable and customize the File Security application using Group Policy

- 1 Specify the file security registry settings described in [“Entrust File Security settings” on page 430](#). The settings specify:
 - which algorithms are used or available for use and how they appear in the GUI
 - which directory attribute is searched
 - the explanatory text in the **Search for People** dialog box
 - whether plaintext file monitoring is on (default is on)
- 2 Push out your settings to your users through Microsoft Group Policy. The registry values are written to your users' registries.
- 3 Ensure the **File Security** option and, optionally, the **Encryption/Digital Signature** option, are activated. To enable them, use the **Custom Installation** wizard and then distribute the installation package to your users.

Note: If you enable the **Encryption/Digital Signature** option, you must specify the LDAP directory registry settings described in [“Directory settings” on page 331](#). Security Provider searches these directories for encryption certificates.

There is no need to associate the directories with Security Manager.

You have activated and customized the File Security application.

Using the File Security application

The File Security application comes with two user interfaces:

- a right-click menu in Windows Explorer
This menu is described on page 202. For more details, see the File Security application’s online help.
- a command-line
From the command-line, you can encrypt, decrypt, sign, and verify files. This option is useful if you want to perform batch operations. For example, you could use a batch file to encrypt the contents of a folder on a nightly basis.
For details on using the command line, see:
 - [“To encrypt files with a password from the command line”](#)
 - [“To sign files with a certificate from the command line”](#)
 - [“To sign and encrypt files with certificates from the command line”](#)
 - [“To decrypt or verify files from the command line”](#)

To encrypt files with certificates from the command line

Only a person knowledgeable about the command line should attempt this procedure.

- 1** Ensure you have Entrust Entelligence Security Provider for Windows installed.
- 2** Open a command line. (Click **Start** > **Run** and enter `cmd.`)
- 3** Enter the following command to encrypt:

Note: Examples of how to use this command are provided at the end of this procedure.

```
eeencrypt.exe -encrypt <user_DN> [-encalgorithm <algorithm_name>] [-recipient  
<recipient_DN|PEG_name>] [-output <folder>] [-deleteoriginal] [-overwrite]  
<filename> [<filename2>]
```

where:

Option	Description
<user_DN>	<p>Mandatory.</p> <p>The distinguished name (DN) of the user who is initiating the encryption. This user's encryption certificate is used to encrypt the file. <user_DN> can be specified as:</p> <ul style="list-style-type: none">• "" — Use "" if the user has already encrypted a file using the file encryption wizard. The encryption certificate selected in this wizard is used to encrypt the files. For example, if Bob Smith's Encryption Certificate was selected in the file encryption wizard, then Bob's Smith's encryption certificate is used to encrypt the file.• full DN — For example "cn=Bob Smith,o=Acme,c=US".• partial DN — For example "Bob Smith".
-encalgorithm <encalgorithm_name>	<p>Optional.</p> <p>The name of the encryption algorithm that is used to encrypt the files. If you do not specify an algorithm, the default encryption algorithm is used. The default is set by the administrator who configured Security Provider for Windows. If an administrator did not explicitly set a default algorithm, 3DES is used.</p> <p>Your choices are: DES, 3DES, AES-256, AES-192, AES-128, RC2-128, RC2-64, RC2-56, RC2-40, CAST-128, CAST-80, CAST-64, CAST-40, IDEA-128.</p>
-recipient <recipient_DNIP EG_name>	<p>Optional.</p> <p>An additional recipient for whom you want to encrypt. This recipient must be someone other than the person specified by <user_DN>. You can specify multiple recipients. If no -recipient is specified, then the file is encrypted only for the user specified by <user_DN>.</p> <p>Recipients can be specified as:</p> <ul style="list-style-type: none">• The full DN of the recipient, for example, "cn=Alice Jones, o=Acme, c=US" . Note: Do not use a partial DN. For example, "Alice Jones" does not work.• A personal encryption group (PEG) name, for example "Sales Team".

Option	Description
-output <folder>	Optional. The name of the folder in which to place the encrypted version of the file. If no folder is specified, the encrypted file is placed in the current folder.
-deleteoriginal	Optional. If specified, the original plaintext file is deleted upon successful execution of the command. For example, if you encrypt <code>TopSecret.txt</code> , then <code>TopSecret.txt</code> is deleted when <code>TopSecret.p7m</code> is generated.
-overwrite	Optional. If specified, any <code>.p7m</code> files with the same name as the new output files are overwritten automatically. For example, if a <code>TopSecret.p7m</code> file exists, it is overwritten when you generate a new <code>TopSecret.p7m</code> .
<filename> and <filename2>	Mandatory. <filename> and <filename2> — the names of the files that you want to encrypt. The filename can contain standard command line variables such as <code>*.*</code> .

Encryption example 1:

```
eeencrypt.exe -encrypt "" "c:\TopSecret\fileone.txt" "c:\TopSecret\filetwo.doc"
```

In example 1, the user (say John) encrypts two files for himself: `fileone.txt` and `filetwo.doc`. The default encryption algorithm is used. John does not need to specify his own DN because he has already encrypted files using the file encryption wizard prior to using the command line.

Encryption example 2:

```
eeencrypt.exe -encrypt "cn=Alice Smith,ou=business,o=Organization,c=US"
-encalgorithm 3DES -recipient "cn=Bob Jones,dc=Company2,dc=com" -recipient
"Sales PEG" -output c:\EncryptedFiles c:\FilesToEncrypt\*.*
```

In example 2, Alice Smith encrypts all files in the folder `c:\FilesToEncrypt`. Encrypted files are placed in the output folder, `c:\EncryptedFiles`. Files are encrypted for herself, Bob Jones, and all the members of the `Sales PEG` that she created earlier. Alice specifies her own DN because she has never used the file encryption wizard before. Alternatively, Alice could have specified a portion of her DN such as `"Alice Smith"`.

To sign files with a certificate from the command line

Only a person knowledgeable about the command line should attempt this procedure.

- 1** Ensure you have Entrust Entelligence Security Provider for Windows installed.
- 2** Open a command line. (Click **Start** > **Run** and enter `cmd.`)
- 3** Enter the following command to sign:

Note: Examples of how to use this command are provided at the end of this procedure.

```
eeencrypt.exe -sign <user_DN> [-hashalgorithm <algorithm_name>] [-timestamp  
<ts_server>] [-timestamppolicy <policy>] [-output <folder>] [-deleteoriginal]  
[-overwrite] <filename> [<filename2>]
```

where:

Option	Description
<user_DN>	<p>Mandatory.</p> <p>The distinguished name (DN) of the user who is applying the digital signature. This user's signing key is used to sign the file. <user_DN> can be specified as:</p> <ul style="list-style-type: none">• "" — Use "" if the user has already signed a file using the file signing wizard. The signing certificate (also known as the verification certificate) selected in this wizard is used to sign the files. For example, if Bob Smith's Verification Certificate was selected in the file signing wizard, then Bob's Smith's signing certificate is used to sign the file.• full DN — For example "cn=Bob Smith,o=Acme,c=US".• partial DN — For example "Bob Smith".
-hashalgorithm <algorithm_name>	<p>Optional.</p> <p>The name of the hashing (signing) algorithm. If you do not specify an algorithm, the default hashing algorithm is used. The default hashing algorithm is set by the administrator who configures Security Provider for Windows. If an administrator did not explicitly set a default algorithm, SHA-256 is used.</p> <p>Your choices are: SHA-1, SHA-256, SHA-384, SHA-512.</p>
-timestamp <ts_server>	<p>Optional.</p> <p>The name of the timestamp authority that will timestamp the signature. If no timestamp authority is specified, then no timestamp is applied. The timestamp authority can be specified using:</p> <ul style="list-style-type: none">• "" — Use "" if there is only one timestamp server configured.• its friendly name (if one has been configured) Note: You can find the timestamp server friendly name in the file signing wizard.• its host name and port, for example, http://timestamp.com:2345/verificationserver/rfc316timestamp

Option	Description
-timestamppolicy <policy>	<p>Optional.</p> <p>The timestamp policy you want to use. If no policy is specified, then the default policy is used. The default policy is set by the administrator who configured Security Provider for Windows.</p> <p>The timestamp policy can be specified using its:</p> <ul style="list-style-type: none"> friendly name (if one has been configured), for example "My Timestamp Policy". Note: You may find the policy's friendly name in the file signing wizard; if it is not there, then you must ask the Security Provider administrator for it. OID, for example, 1.2.840.113533.7.75.0.
-output <folder>	<p>Optional.</p> <p>The name of the folder in which to place the signed version of the file. If no folder is specified, the signed file is placed in the current folder.</p>
-deleteoriginal	<p>Optional.</p> <p>If specified, the original plaintext file is deleted upon successful execution of the command.</p> <p>For example, if you encrypt <code>TopSecret.txt</code>, then <code>TopSecret.txt</code> is deleted when <code>TopSecret.p7m</code> is generated.</p>
-overwrite	<p>Optional.</p> <p>If specified, any <code>.p7m</code> files with the same name as the new output files are overwritten automatically.</p> <p>For example, if a <code>TopSecret.p7m</code> file exists, it is overwritten when you generate a new <code>TopSecret.p7m</code>.</p>
<filename> and <filename2>	<p>Mandatory.</p> <p><filename> and <filename2> — the names of the files that you want to sign. The filename can contain standard command line variables such as <code>*.*</code>.</p>

Signing example 1:

```
eeencrypt.exe -sign "" "c:\TopSecret\fileone.txt" "c:\TopSecret\filetwo.doc"
```

In example 1, the user (say John) signs two files: `fileone.txt` and `filetwo.doc`. The default hashing algorithm is used. John does not need to

specify his own DN because he has already encrypted files using the file signing wizard prior to using the command line.

Signing example 2:

```
eeencrypt.exe -sign "cn=Alice Smith,ou=business,o=Organization,c=US"  
-hashalgorithm SHA-256 -timestamp "" -timestamppolicy "Top Secret Policy"  
-output c:\SignedFiles\ c:\FilesToSign\*.*
```

In example 2, Alice Smith signs all files in the folder `c:\FilesToSign` using the SHA-256 hashing algorithm. Her signature is timestamped using the default timestamp server and the Top Secret Policy. After the digital signature is applied, files are placed in the output folder, `c:\SignedFiles\`. Alice must specify her own DN because she has never used the file signing wizard before. Alternatively, Alice could have specified a portion of her DN such as "Alice Smith".

To sign and encrypt files with certificates from the command line

Only a person knowledgeable about the command line should attempt this procedure.

- 1** Ensure you have Entrust Entelligence Security Provider for Windows installed.
- 2** Open a command line. (Click **Start** > **Run** and enter `cmd.`)
- 3** Enter the following command to sign (all on one line):

Note: Examples of how to use this command are provided at the end of this procedure.

```
eeencrypt.exe -sign <user_DN> -encrypt <user_DN> [-hashalgorithm  
<hashalgorithm_name>] [-timestamp <ts_server>] [-timestamppolicy <policy>]  
[-encalgorithm <encalgorithm_name>] [-recipient <recipient_DN|PEG_name>]  
[-output <folder>] [-deleteoriginal] [-overwrite] <filename> [<filename2>]
```

where:

where:

Option	Description
<user_DN>	<p>Mandatory.</p> <p>The distinguished name (DN) of the user who is initiating the digital encryption and signing operation. This user's signing key and encryption certificate are used to sign and encrypt the file.<user_DN> can be specified as:</p> <ul style="list-style-type: none">• "" — Use "" if the user has already signed or encrypted a file using the file signing or encryption wizard. The encryption and signing certificates selected in these wizards are used to sign the files. For example, if Bob Smith's Verification Certificate was selected in the file signing wizard, then Bob's Smith's signing certificate is used to sign the file.• full DN — For example "cn=Bob Smith,o=Acme,c=US".• partial DN — For example "Bob Smith".
-hashalgorithm <hashalgorithm_name>	<p>Optional.</p> <p>The name of the hashing (signing) algorithm. If you do not specify an algorithm, the default hashing algorithm is used. The default hashing algorithm is set by the administrator who configures Security Provider for Windows. If an administrator did not explicitly set a default algorithm, SHA-256 is used.</p> <p>Your choices are: SHA-1, SHA-256, SHA-384, SHA-512.</p>
-timestamp <ts_server>	<p>Optional.</p> <p>The name of the timestamp authority that will timestamp the signature. If no timestamp authority is specified, then no timestamp is applied. The timestamp authority can be specified using:</p> <ul style="list-style-type: none">• "" — Use "" if there is only one timestamp server configured.• its friendly name (if one has been configured) Note: You can find the timestamp server friendly name in the file signing wizard.• its host name and port, for example, http://timestamp.com:2345/verificationserver/rfc316timestamp

Option	Description
-timestamppolicy <policy>	<p>Optional.</p> <p>The timestamp policy you want to use. If no policy is specified, then the default policy is used. The default policy is set by the administrator who configured Security Provider for Windows.</p> <p>The timestamp policy can be specified using its:</p> <ul style="list-style-type: none"> friendly name (if one has been configured), for example "My Timestamp Policy". Note: The policy's friendly name may be displayed in the file signing wizard; if it is not there, then you must ask the Security Provider administrator for it. OID, for example, 1.2.840.113533.7.75.0.
-encalgorithm <encalgorithm_name>	<p>Optional.</p> <p>The name of the encryption algorithm that is used to encrypt the files. If you do not specify an algorithm, the default encryption algorithm is used. The default is set by the administrator who configured Security Provider for Windows. If an administrator did not explicitly set a default algorithm, 3DES is used.</p> <p>Your choices are: DES, 3DES, AES-256, AES-192, AES-128, RC2-128, RC2-64, RC2-56, RC2-40, CAST-128, CAST-80, CAST-64, CAST-40, IDEA-128.</p>
-recipient <recipient_DNIP EG_name>	<p>Optional.</p> <p>An additional recipient for whom you want to encrypt. This recipient must be someone other than the person specified by <user_DN>. You can specify multiple recipients. If no -recipient is specified, then the file is encrypted only for the user specified by <user_DN>.</p> <p>Recipients can be specified using:</p> <ul style="list-style-type: none"> The full DN of the recipient, for example, "cn=Alice Jones, o=Acme, c=US". Note: Do not use a partial DN. For example, "Alice Jones" does not work. A "personal encryption group (PEG)" name, for example "Sales Team".

Option	Description
-output <folder>	Optional. The name of the folder in which to place the signed and encrypted version of the file. If no folder is specified, the signed and encrypted file is placed in the current folder.
-deleteoriginal	Optional. If specified, the original plaintext file is deleted upon successful execution of the command. For example, if you encrypt <code>TopSecret.txt</code> , then <code>TopSecret.txt</code> is deleted when <code>TopSecret.p7m</code> is generated.
-overwrite	Optional. If specified, any <code>.p7m</code> files with the same name as the new output files are overwritten automatically. For example, if a <code>TopSecret.p7m</code> file exists, it is overwritten when you generate a new <code>TopSecret.p7m</code> .
<filename> and <filename2>	Mandatory. <filename> and <filename2> — the names of the files that you want to sign and encrypt. The filename can contain standard command line variables such as <code>*.*</code> .

Sign and encrypt example 1:

```
eeencrypt.exe -sign "" -encrypt "" "c:\TopSecret\fileone.txt"
"c:\TopSecret\filetwo.doc"
```

In example 1, the user (say John) signs and encrypts two files for himself: `fileone.txt` and `filetwo.doc`. The default signing and encryption algorithms are used. John does not need to specify his own DN because he has already signed or encrypted files using one of the file signing or encryption wizards prior to using the command line.

Sign and encrypt example 2:

```
eeencrypt.exe -sign "cn=Alice Smith,ou=business,o=Organization,c=US" -encrypt
"cn=Alice Smith,ou=business,o=Organization,c=US" -hashalgorithm SHA-1
-encalgorithm 3DES -recipient "cn=Bob Jones,dc=Company2,dc=com" -recipient
"Sales PEG" -output c:\SignedEncryptedFiles c:\FilesToSignEncrypt\*.*
```

In example 2, Alice Smith signs and encrypts all files in the folder `c:\FilesToSignEncrypt`. She chooses SHA-1 as the signing algorithm, and 3DES as the encryption algorithm. Encrypted files are placed in the output folder, `c:\SignedEncryptedFiles`. Files are encrypted for herself, Bob Jones, and all the members of the Sales PEG that she created earlier. Alice must specify her own DN because she has never used one of the file encryption/signing wizards before.

To decrypt or verify files from the command line

Only a person knowledgeable about the command line should attempt this procedure.

- 1** Ensure you have Entrust Entelligence Security Provider for Windows installed.
- 2** Open a command line. (Click **Start** > **Run** and enter `cmd.`)
- 3** Enter one of the following commands:

To decrypt and verify:

```
eedecrypt.exe -decrypt [-output <folder_name>] [-overwrite] <filename>
[<filename2>]
```

To verify only (no output files are generated, and only the signature status is displayed):

```
eedecrypt.exe -verify <filename> [<filename>...]
```

When specifying file names, you can use command line variables such as `*.*`.

Example 1:

```
eedecrypt.exe -decrypt -output "c:\Program Files\DecandVerified\" -overwrite
"C:\Program Files\EncandSigned\*.*"
```

In Example 1, all files in the `\EncandSigned` folder are decrypted and verified and placed in the `\DecandVerified` folder. The `-overwrite` option indicates that any files with the same name as the new decrypted and verified files are overwritten automatically. For example, if a `TopSecret.txt` file exists in the `\DecandVerified` folder, then `TopSecret.txt` is overwritten when you decrypt and verify `TopSecret.p7m`.

Example 2:

```
eedecrypt.exe -decrypt "C:\TopSecret\file1.p7m" "C:\Private\file2.ent"
```

In Example 2, `file1.p7m` and `file2.ent` are decrypted and verified. Their plaintext versions are placed in the current folder.

Password Encrypt application

Password Encrypt is an application that is bundled with Entrust Intelligence Security Provider for Windows. It allows users to encrypt a file or files with a password of their choosing. The password is then asked for whenever anybody tries to open the file. Users can keep this password to themselves, or distribute it to trusted people. Users do not require a digital ID to password-encrypt files.

Files are encrypted using AES 256 (this is not configurable for password protection). Compression is defined in the S/MIME standard RFC 3274 as ZLIB.

Note: Users can also opt to encrypt files with their encryption certificate, as a backup, in case they forget the password. For details, see [“Password Encrypt functionality” on page 222](#).

Figure 19: Password Encrypt application



Topics in this section:

- [“Why use Password Encrypt?” on page 222](#)
- [“Password Encrypt functionality” on page 222](#)
- [“Customizing Password Encrypt” on page 223](#)
- [“Using the Password Encrypt application” on page 224](#)

Why use Password Encrypt?

Use Password Encrypt to encrypt files for users outside of your organization, such as partners, distributors, and customers, who might not have digital IDs or certificates.

External users simply double-click the password-encrypted file, specify the password that was given to them, and are granted access to the file. To successfully decrypt a password-encrypted file, users need:

- one of the following software applications on their computers: Security Provider for Windows, Entrust Solo, or the free password unprotect utility.
OR
- no software, if the person who initially password-encrypted the file bundled it into a self-decrypting output file (.exe). See ["Password Encrypt functionality" on page 222](#) for details.

Password Encrypt functionality

Password Encrypt has the following functionality:

Functionality	Description
Password encrypt	To encrypt one or more files with a password, users right-click the selected files and select Encrypt File with Password . A wizard appears where users specify the password with which to encrypt the files. After completing the wizard, the files are saved with a .pp7m extension. Any file type can be password-encrypted.
Password decrypt	To decrypt a file that has been encrypted with a password, users double-click the password-encrypted file and supply the correct password when prompted.
Self-decrypt	When a user password-encrypts a file, they have the option to Generate a self-decrypting output file . When this option is enabled, the Password Encrypt application password-encrypts the file and then embeds it within an .exe file. This .exe file contains all the necessary code to password-decrypt the file. The .exe can be distributed, along with the password, to anybody who needs access to the file. They do not require any special software. The main disadvantage of the .exe file is that it most likely cannot be emailed, because .exe files are typically blocked by companies' email gateways in order to prevent the spread of viruses. Even if the recipient successfully receives an .exe over email, this person should not open it, as it could have been tampered with in transit. To work around this problem, users can use a USB stick to transfer .exes from one computer to another.

Functionality	Description
Encrypt files with encryption certificate in addition to password	<p>When a user password-encrypts a file, they may have the option to Encrypt the files for my encryption certificate in addition to password. When this option is enabled, the file is encrypted with the user's certificate (if they have one) and a user-specified password.</p> <p>There are two benefits to encrypting with a certificate:</p> <ol style="list-style-type: none"> 1 The user who originally encrypted the file is prompted to log in to their digital ID when they access the file—they are not prompted for the file's password. The benefit here is that the user is much less likely to forget their digital ID password than the file's password. 2 Even if the user forgets their digital ID password, the digital ID is backed up at the CA, and can be recovered. Once recovered, users can continue to access the encrypted file. If, however, a file is only encrypted with a user-specified password, then the user must have this password to access the file—if the user forgets it, there is no way to decrypt the file. <p>When a file is encrypted with a certificate in addition to a password, other people wishing to access the file are affected in the following way:</p> <ul style="list-style-type: none"> • If the user who is trying to access the file does not have an encryption certificate (for example, they are an external user), they are prompted immediately for the file's password.
Command line operations	You can password-encrypt and decrypt one or multiple files from the command line. See “Using the Password Encrypt application” on page 224 for details.

Customizing Password Encrypt

The following instructions describe how to customize Password Encrypt using either the **Custom Installation** wizard or Microsoft Group Policy:

- [“To customize Password Encrypt using the wizard” on page 223](#)
- [“To customize Password Encrypt using Group Policy” on page 224](#)

To customize Password Encrypt using the wizard

- 1 Run through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#). Fill out the pages in the wizard, as described in the following table.

On this page in the wizard...	Do this...
Select Application Features	Ensure that the Entrust Password Decrypt option is enabled.

On this page in the wizard...	Do this...
Password Encrypt Options	Fill out the page, as required. See “Password Encrypt settings” on page 451 for detailed descriptions of these fields.

- 2 Proceed to the end of the wizard and click **Finish** to save your settings.
The .mst file is updated with your new Password Encrypt settings. You have now customized the Password Encrypt application.
- 3 Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

To customize Password Encrypt using Group Policy

- 1 Specify the registry values described in [“Password Encrypt settings” on page 451](#).
- 2 Push out your settings to your users through Microsoft Group Policy. The registry values are written to your users’ registries.

You have customized the Password Encrypt application.

Using the Password Encrypt application

The Password Encrypt application comes with two user interfaces:

- a right-click menu in Windows Explorer
Users right-click a file in Windows Explorer and select the appropriate cryptographic option from the pop-up menu. A wizard then appears, guiding the user through the password-encryption or decryption operation.
For details on using the right-click menu, see the File Security online help.
- a command-line
From the command-line, you can password-encrypt and decrypt files. This option is useful if you want to perform batch operations. For example, you could use a batch file to password-encrypt the contents of a folder on a nightly basis.
For details on using the command line to password-encrypt and decrypt, see:
 - [“To encrypt files with a password from the command line”](#)
 - [“To decrypt password-encrypted files from the command line”](#)

To encrypt files with a password from the command line

- 1 Ensure you have Entrust Entelligence Security Provider for Windows installed.
- 2 Open a command line. (Click **Start** > **Run** and enter cmd.)

3 Enter the following command to encrypt:

Note: Examples of how to use this command are provided at the end of this procedure.

```
eepe.exe [-cert <user_DN>] [-password <password>] [-selfdecrypt] [-output  
<filename>] [-deleteoriginal] [-overwrite] <filename> [<filename2>]
```

where:

Option	Description
-cert <user_DN>	<p>Optional (although your Security Provider administrator may have made it mandatory).</p> <p>If specified, the distinguished name (DN) of the user who is initiating the encryption. This user's encryption certificate is used to encrypt the file, in addition to the password. <user_DN> can be specified as:</p> <ul style="list-style-type: none">• <i>empty</i> — Specify -cert without <user_DN> if the user has already password-encrypted a file with their certificate using the password-encryption wizard. The encryption certificate selected in this wizard is used to encrypt the files. For example, if Bob Smith's Encryption Certificate was selected in the password encryption wizard, then Bob's Smith's encryption certificate is used to encrypt the file, in addition to the password.• full DN — For example "cn=Bob Smith,o=Acme,c=US".• partial DN — For example "Bob Smith". <p>If unspecified, the file is not encrypted with a certificate.</p>
-password <password>	<p>Optional.</p> <p>If specified, the password with which to encrypt the files.</p> <p>If unspecified, you are prompted for the password at the command line.</p> <p>The password must conform to the password rules. You can view the password rules from the password encryption wizard.</p>

Option	Description
-selfdecrypt	<p>Optional.</p> <p>If specified, the output file will be a single self-extracting <code>.exe</code> file instead of a <code>.pp7m</code> file. The benefit of the <code>.exe</code> file is that it can be shared with people who do not have decryption software or certificates on their computer. For example, you could give the <code>.exe</code> file to an external partner, and as long as this person has the file's password, they can decrypt the file; there are no software requirements. The main disadvantage of <code>.exe</code> files is that they most likely cannot be emailed, because they are typically blocked by companies' email gateways in order to prevent the spread of viruses. Even if the recipient successfully receives an <code>.exe</code> over email, this person should not open it, as it could have been tampered with in transit. To work around this problem, you can use a USB stick to transfer <code>.exes</code> from one computer to another, or create a <code>.pp7m</code> file.</p> <p>If unspecified, a password-encrypt file with a <code>.pp7m</code> file is created. The benefit of a <code>.pp7m</code> file is that it can be emailed, and is smaller than an <code>.exe</code> file. Users must have Entrust Solo, Security Provider for Windows, or the password unprotect utility to access a <code>.pp7m</code> file.</p>
-output <filename>	<p>Optional.</p> <p>If specified, input files are combined into a single output file specified here, for example, two files can be encrypted into a single file called <code>c:\MyPasswordProtectedFiles.<pp7m_exe></code>.</p> <p>If unspecified, each file is separately encrypted, and given the name <code><filename>.<pp7m_exe></code>.</p>
-deleteoriginal	<p>Optional.</p> <p>If specified, the original plaintext file is deleted upon successful execution of the command.</p> <p>For example, if you encrypt <code>TopSecret.txt</code>, then <code>TopSecret.txt</code> is deleted when <code>TopSecret.pp7m</code> is generated.</p> <p>If unspecified, the original plaintext file is kept.</p>

Option	Description
-overwrite	Optional. If specified, any .pp7m files (or self-extracting .exe files) with the same name as the new output files are overwritten automatically. For example, if a TopSecret.pp7m file exists, it is overwritten when you generate a new TopSecret.pp7m.
<filename> and <filename2>	Mandatory. <filename> and <filename2> — the names of the files that you want to encrypt. The filename can contain standard command line variables such as *.*.

Example 1:

```
eepe.exe -password St56Key!* -output "c:\Encrypted Files\Protected.pp7m"  
-deleteoriginal c:\Plaintext\*.*
```

In example 1, the user (say John) encrypts all the files in c:\Plaintext with the password St56Key!*. The encrypted files are bundled into a single file called Protected.pp7m. The original plaintext files are deleted after the password-encryption operation completes.

Example 2:

```
eepe.exe -cert "cn=Alice Smith,ou=business,o=Organization,c=US" -deleteoriginal  
"c:\My files\*.*"
```

In example 2, Alice Smith password-encrypts all files in the folder c:\My files. She also encrypts them with her certificate. Because Alice did not specify a password, when she executes the command, eepe.exe will ask her for a password which she must enter and then confirm. Once the password is specified, a separate .pp7m file is created for each file and placed in the current folder.

Note: you can use two sets of double quotation marks to escape a set of double quotation marks, where necessary. For example:

```
eepe.exe -cert "CN=""espw, cmd3""", O=org1, C=ca" -password  
my!Password file.txt
```

To decrypt password-encrypted files from the command line

- 1 Ensure you have Entrust Entelligence Security Provider for Windows installed.

- 2 Open a command line. (Click **Start** > **Run** and enter cmd.)
- 3 Enter the following command to encrypt:

Note: Examples of how to use this command are provided at the end of this procedure.

```
eepd.exe [-password <password>] [-output <folder>] [-deleteoriginal]
[-overwrite] <filename> [<filename2>]
```

where:

Option	Description
-password <password>	Optional. If specified, the password with which to decrypt the files. If unspecified, you are prompted for the password at the command line.
-output <folder>	Optional. If specified, the folder where the decrypted files are placed. If unspecified, the current folder is used.
-overwrite	Optional. If specified, any existing plaintext files with the same name as the new output files are overwritten automatically. For example, if a TopSecret.txt file exists, it is overwritten when you generate a new TopSecret.txt.
<filename> and <filename2>	Mandatory. <filename> and <filename2> — the names of the files that you want to decrypt. The filename can contain standard command line variables such as *.*.

Example 1:

```
eepd.exe -password St56Key!* -output "c:\Decrypted Files\" c:\Encrypted\*.*
```

In example 1, the user (say John) decrypts all the files in c:\Encrypted with the password St56Key!*. The decrypted files are placed in c:\Decrypted Files\.

Example 2:

```
eepd.exe "c:\My Encrypted Files\*.*)"
```

In example 2, Alice Smith decrypts all files in the folder `c:\My Encrypted Files`. Because Alice did not specify a password, when she executes the command, she is prompted for a password which she must enter and then confirm. Once the password is specified, each file is decrypted and placed in the current folder.

TrueDelete application

TrueDelete is an application that is bundled with Entrust Entelligence Security Provider for Windows. It allows users to securely remove a file from their computer.

TrueDelete will not securely delete files in the following locations:

- Windows\SoftwareDistribution\Download folder
- Software Volume Information folder in each volume

Why use TrueDelete?

When you select a file and press Delete, the file is placed in the Recycle Bin and can be recovered. If you select a file and press Shift+Delete without TrueDelete installed, the file is not permanently removed, as expected; only the reference to the file is removed from the file system table. The file remains on disk until it is overwritten by another file, and even after that, the file data could be recovered using raw disk editors and recovery tools. TrueDelete is configurable, overwriting files a specified number of times. This allows you to delete files according to the standards used by your organization for secure deletion.

With TrueDelete, you can securely and permanently delete files and file slack space (the unused hard drive space allocated to a file). Once configured, TrueDelete securely deletes files regardless of whether the deletion was initiated by you or by an application.

TrueDelete functionality

TrueDelete has the following functionality:

- overwrites the files you delete, as well as their file names
There are many overwriting methods to choose from. For details, see [“About overwriting methods” on page 231](#).
- has many triggers that can be enabled. For example, TrueDelete can be triggered when:
 - (default) a user right-clicks a file or folder and selects **Securely Delete**
 - a file or folder is deleted when a user presses Shift+Delete or when an application deletes the file

Note: See the entry for the registry setting [“IncludedFolders” on page 460](#) for more information about deleting subfolders.

- a file is deleted from a specified folder, drive, fixed disk, or removable disk
- a file with a particular file extension is deleted

- a file is encrypted—in this case TrueDelete securely deletes the original plaintext version leaving only the encrypted version
- after it is activated, runs in the background to increase to allow the user to continue other tasks
- if the computer is turned off before TrueDelete is finished deleting the file, it resumes the deletion the next time the computer is started

When TrueDelete is not triggered

TrueDelete is not triggered in the following instances:

- when a user presses Delete
Pressing Delete results in the file being placed in the Recycle Bin. To trigger TrueDelete, users must press Shift+Delete.
- when a file is deleted from a network
TrueDelete is only triggered when a file is deleted from the local computer.
- when applications such as replication, virtualization, and backup applications are installed
In this case, TrueDelete overwrites the original file, but the copied file is not touched. It is therefore recommended that, if you want to use TrueDelete and have it work as intended, you uninstall all applications that make copies of files.
- when a file is deleted from a USB flash drive
TrueDelete is not supported for USB flash drives.

Note: If you delete a file on a flash drive using TrueDelete it will appear to delete the file, however the file is not overwritten by TrueDelete.

About overwriting methods

An overwriting method is a technique for removing all traces of a file by overwriting it several times with numbers, letters, or other characters. An overwriting method with one, two or three passes is usually sufficient to securely delete file information unless government-strength security is desired.

Note: TrueDelete overwrites files on SSD drives with a single pass of zeros.

TrueDelete supports several overwriting methods, as described in the following table.

Table 20: Overwriting methods

	Overwriting method	Overwriting pattern						
		1st pass	2nd pass	3rd pass	4th pass	5th pass	6th pass	7th pass
1	One Pass Zeroes	0s						
2	One Pass Random	Rs						
3	U.S. DoD 5220.22-M (C)	UD						
4	U.S. DoD 5220.22-M (D)	UD	CUD	R with V				
5	U.S. DoD 5220.22-M (E)	UD	CUD	R				
6	U.S. DoD 5220.22-M (EV)	UD with V	CUD with V	R with V				
7	US Army AR380-19	R	UD	CUD				
8	Canadian RCMP TSSIT OPS-II	0s	1s	0s	1s	0s	1s	Rs with V
9	German VSITR	0s	1s	0s	1s	0s	1s	UD
10	Russian GOST P50739-95	0s	R					
11	British HMG IS5 Baseline	0s with V						
12	British HMG IS5 Enhanced	0s	1s	Rs with V				
13	U.S. DOE-NNSA	R	R	CUD				

0s — overwrite with zeros this pass

1s — overwrite with ones this pass

Rs — overwrite with random characters this pass

R — overwrite with a single random character this pass

UD — overwrite with a user-defined character this pass

CUD — overwrite the complement of the user-defined character this pass

V — verify this pass to ensure the overwriting was performed properly

Customizing TrueDelete

The following instructions describe how to customize TrueDelete using either the **Custom Installation** wizard or Microsoft Group Policy:

- [“To customize TrueDelete using the wizard” on page 233](#)
- [“To customize TrueDelete using Group Policy” on page 233](#)

To customize TrueDelete using the wizard

- 1 Run through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#). Fill out the pages in the wizard, as described in the following table.

On this page in the wizard...	Do this...
Select Application Features	Ensure that the Entrust TrueDelete option is enabled.
TrueDelete Configuration Options	Click Add . Fill out the page, as required. See “TrueDelete settings” on page 455 for detailed descriptions of these fields.

- 2 Proceed to the end of the wizard and click **Finish** to save your settings.
The `.mst` file is updated with your new TrueDelete settings. You have now customized the TrueDelete application.
- 3 Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

To customize TrueDelete using Group Policy

- 1 Specify the registry values described in [“TrueDelete settings” on page 455](#). If you do not specify these settings, TrueDelete is activated with the default settings. These settings customize:
 - which triggers will invoke TrueDelete
 - which overwriting method(s) to use
- 2 Push out your settings to your users through Microsoft Group Policy. The registry values are written to your users’ registries.
You have customized the TrueDelete application.

Certificate Explorer application

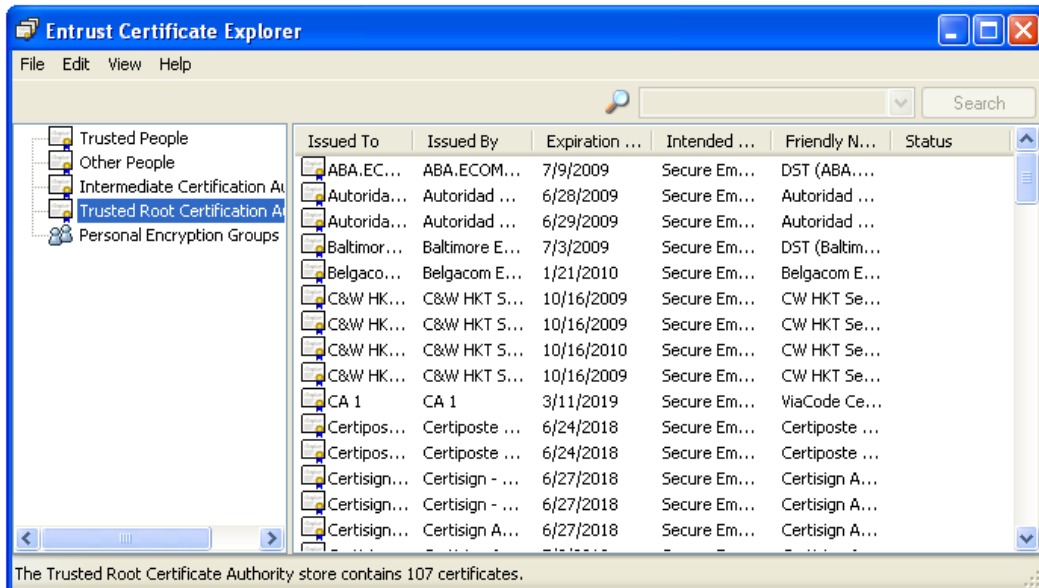
The Entrust Certificate Explorer (Figure 20) is installed when users install Security Provider. The application lets users view and manage the certificates on their computers.

Users can access the application by selecting **Start > All Programs > Entrust Intelligence > Entrust Certificate Explorer** or by right-clicking the Security Provider icon in their taskbar notification area.

For more information on the Entrust Certificate Explorer, see the following sections:

- [“Certificate Explorer functionality” on page 235](#)
- [“Customizing the Certificate Explorer” on page 235](#)
- [“Viewing archived or expired certificates” on page 238](#)
- [“Grouping certificates in a list” on page 239](#)
- [“Checking the revocation status of a certificate” on page 240](#)
- [“Setting up advanced user and debug modes” on page 242](#)
- [“Viewing policy certificates” on page 245](#)

Figure 20: Entrust Certificate Explorer



Certificate Explorer functionality

Users can perform the following tasks through the Entrust Certificate Explorer:

- import certificates, including those in key files and personal address books
- export certificates
- delete certificates
- view certificate contents
- search all configured directories for certificates using simple or advanced search functions
- edit certificate properties
- create Personal Encryption Groups, which are logical groupings of people
- import and export Personal Encryption Groups
- assign priority to the position of specific groups in lists
- adjust the amount of information displayed to the user
- view policy certificate information
- view certificate revocation status

For more information on the functionality available in the Entrust Certificate Explorer, the online help.

Customizing the Certificate Explorer

The following instructions describe how to customize the Entrust Certificate Explorer using either the **Custom Installation** wizard or Microsoft Group Policy:

- [“To customize the Certificate Explorer using the wizard” on page 235](#)
- [“To customize the Certificate Explorer using Group Policy” on page 236](#)

To customize the Certificate Explorer using the wizard

- 1 Run through the **Custom Installation** wizard, as described in [“To customize the installation using the wizard only” on page 290](#). Fill out the pages in the wizard, as described in the following table.

On this page in the wizard...	Do this...
Select Application Features	Ensure that the Entrust Certificate Explorer option is selected.
Entrust File Security Options > Advanced	Fill out the Search Query and Search Prompt fields, as required. Hover your mouse over the fields for information on the field. See “Entrust File Security settings” on page 430 for detailed descriptions of these fields.

On this page in the wizard...	Do this...
Specify Additional Registry Values	<p>Specify the registry values described in “Entrust Certificate Explorer settings” on page 463. These settings customize:</p> <ul style="list-style-type: none"> • which folders appear initially in the tree view • which items under the View menu are activated • whether associated private keys are deleted when users delete certificates • whether Personal Encryption Groups are visible

- 2 Proceed to the end of the wizard and click **Finish** to save your settings.
The `.mst` file is updated with your new Entrust Certificate Explorer settings. You have now customized the Entrust Certificate Explorer application.
- 3 Package, test, and distribute the installation to your users. For details, see [“Deploying Security Provider for Windows” on page 281](#).

To customize the Certificate Explorer using Group Policy

- 1 Specify the registry values described in [“Entrust Certificate Explorer settings” on page 463](#). If you do not specify these settings, the Entrust Certificate Explorer is activated with the defaults. These settings customize:
 - which folders appear initially in the tree view
 - which items under the **View** menu are activated
 - whether associated private keys are deleted when users delete certificates
- 2 Push out your settings to your users through Microsoft Group Policy. The registry values are written to your users’ registries.

You have customized the Entrust Certificate Explorer application.

Using the Certificate Explorer search functions

The top field of the Certificate Explorer lets you enter search terms to find a subset of the certificates available.

To switch between a simple and an advanced search, click the down-arrow on the right side of the **Search** button and select **Advanced Search** on the drop-down menu. This option toggles the advanced search function on and off.

To use the simple search function

- 1 Open the Certificate Explorer.
There should be a single search field at the top of the page. If not, de-select the **Advanced Search** option on the **Search** button.

- 2 From the list pane on the left side of the explorer, select the certificate category that you want to search (such as Personal, Trusted People, Other People) or select Search Results to find certificates not already in a category.
- 3 Enter a name in the search field.
- 4 Click the down-arrow on the right side of the **Search** button and click one of the search scope options, such as **Search All Directories**. (Once selected, the setting remains until de-selected; so you can just click the **Search** button next time.)

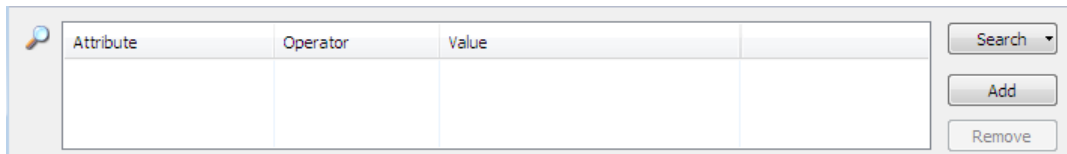
The search results appear.

You can drag and drop a certificate into the applicable category (such as Personal, Trusted People, Other People).

To use the advanced search function

- 1 Open the Certificate Explorer.

If there is a single search field at the top of the page, select the **Advanced Search** option on the **Search** button. The advanced search area looks like this:



Attribute	Operator	Value

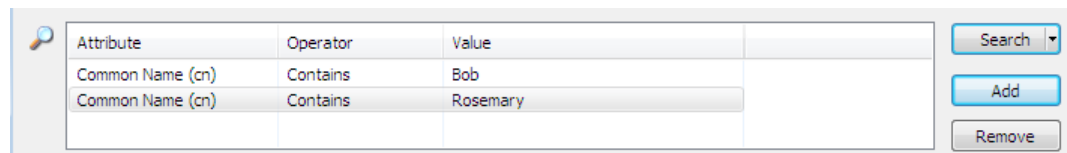
Search ▾

Add

Remove

- 2 From the list pane on the left side of the explorer, select the certificate category that you want to search (such as Personal, Trusted People, Other People) or select Search Results to find certificates not already in a category.
- 3 Click **Add** to enter a search term.
Attribute, **Operator** and **Value** columns appear.
- 4 Enter a search value in the **Value** cell.

You can click **Add** again to enter a second search term.



Attribute	Operator	Value
Common Name (cn)	Contains	Bob
Common Name (cn)	Contains	Rosemary

Search ▾

Add

Remove

To delete a row, select any cell in it and click **Remove**.

- 5 To define the search criteria for any row, you can click a cell under **Attribute** and **Operator** to change the displayed value.

- 6 Once you have added all your search criteria and values, click the down-arrow on the right side of the **Search** button and click one of the search scope options, such as **Search All Directories**.

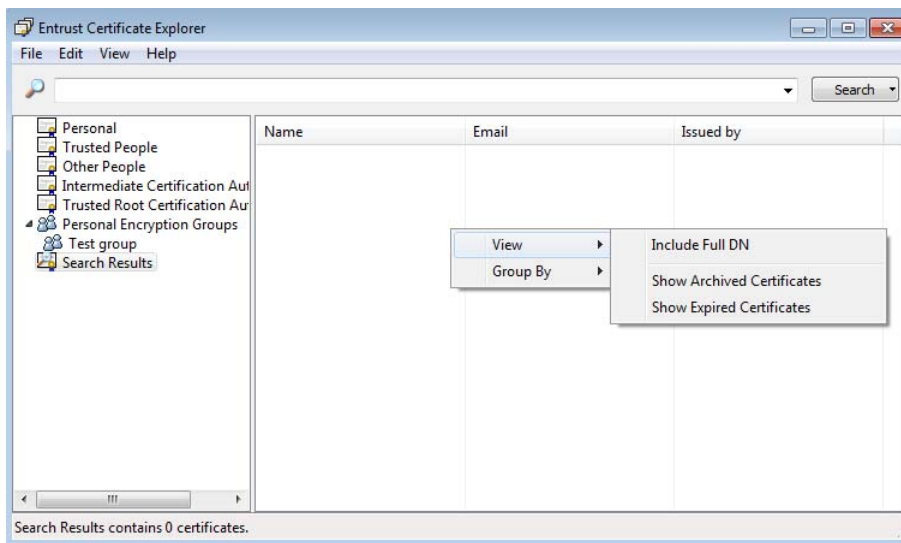
In an advanced search, the Certificate Explorer lets you search for several certificates using the same attribute (such as Common Name). The search uses OR logic to return matching records.

Viewing archived or expired certificates

In addition to allowing the end user to list and view their own certificates, other user's certificates, CA certificates, and personal encryption groups, users can view archived and expired certificates in the Certificate Explorer search results.

To search for archived and expired certificates

- 1 Open the Certificate Explorer (this can be done from the Security Provider menu).
- 2 From the list pane on the left side explorer page, select **Search Results**.
- 3 Right click in the empty pane on the right side of the explorer page.



- 4 Under **View**, select **Show Archived Certificates** or **Show Expired Certificates**.
Selecting either option toggles it on; so, you can search for both by selecting both in sequence. Select an option again to toggle it off.
Now when you execute a search, you will see more than just the current certificates.

You can have the full DN of each user shown in the results. Select **View > Include Full DN**.

Note: An archived or expired certificate must exist in the user's personal store or nothing appears in the list.

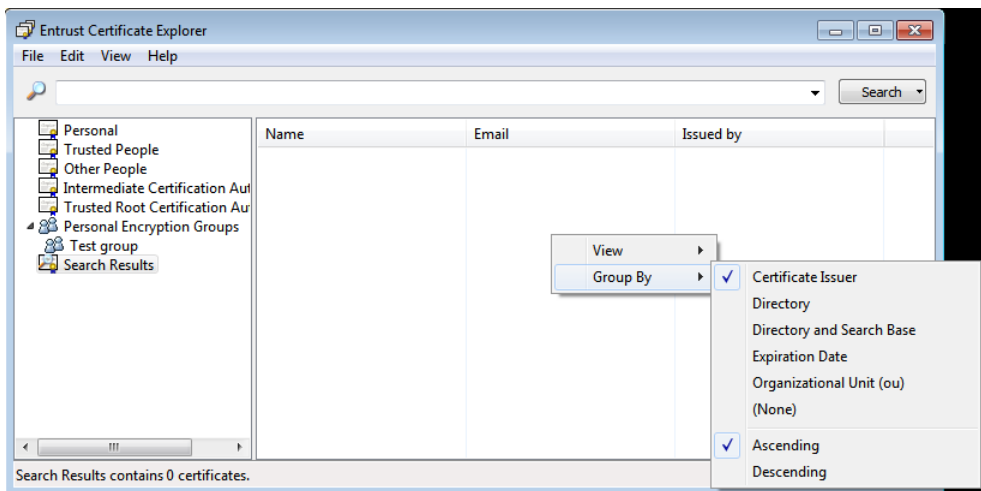
Grouping certificates in a list

To help users find particular certificates in a long list, Security Provider allows you to group certificates in the list. Certificates can be displayed by:

- Issuer
- Digital ID (not available for search results)
- Directory (search results only)
- Directory and Search Base (search results only)
- Expiration Date
- Organization Unit

To group certificates

- 1 Open the Certificate Explorer (this can be done from the Security Provider menu).
- 2 From the list pane on the left side of the explorer, select the certificate category that you want to view (such as Personal, Trusted People, Other People).
- 3 Right click in the pane on the right side of the explorer. A context menu appears.



- 4 Under **Group By**, select grouping criteria that you want. You can also toggle **Ascending** and **Descending** order.

Note: Security Provider lists the groups in alphabetical order, by default. However, you can give individual groups preferred status. Groups listed under Issuer, Directory (with or without Search Base) and Organization Unit can be given preferred status. Preferred groups always appear in the list as specified. For example, you can prioritize the list so specific organizational units will appear first, second, third and so on. For information about configuring preferred groups, see ["Preferred status" on page 467](#).

Checking the revocation status of a certificate

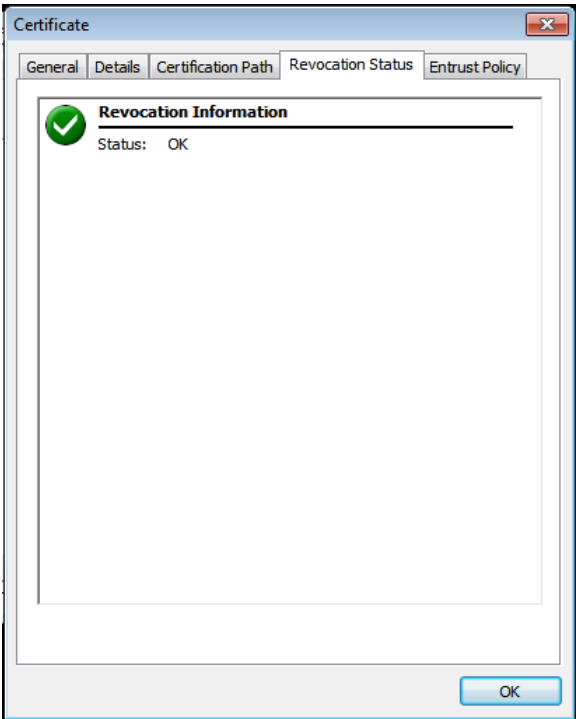
The revocation information of some certificates is displayed on the **Revocation Status** tab of the **Properties** dialog box. The information is available:

- from Certificate Explorer's main window by opening the **Properties** dialog box for certificates in the Personal, Trusted People, Other People certificate store or Personal Encryption Groups
- when the user views the certificate in the **New Personal Encryption Groups** dialog box of Certificate Explorer
- when the user views the certificate in the **Personal Encryption Groups** dialog box of Certificate Explorer
- when the user views the certificate in **Import Personal Address Book** dialog box of Certificate Explorer





To check the revocation status of a person's certificate

- 1 Open the Certificate Explorer.
- 2 From the list pane on the left side of the explorer, select the certificate category that you want to view (such as Personal, Trusted People, Other People).
- 3 On the right side of the explorer, right-click a name and select **Properties**.
- 4 On the **Certificate** dialog box, select the **Revocation Status** tab.

Figure 21: Revocation Status tab



Security Provider displays information about the revocation status of the certificate.

Status	Description
 Pass	OK (the certificate passes the revocation check)
 Warning	The revocation status of the certificate is unknown because revocation checking was not performed.
 Warning	The revocation status of the certificate is unknown because revocation information was unavailable.
 Warning	The revocation status of the certificate is unknown because revocation checking failed.

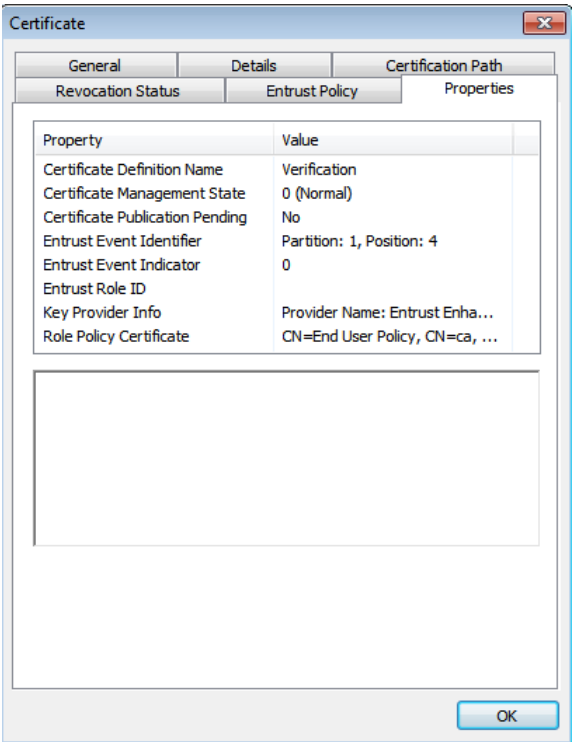
Status	Description
 Fail	Revoked Reason is one of following: <ul style="list-style-type: none"> • Unspecified • Key Compromise • CA Compromise • Affiliation Changed • Superseded • Cessation of Operation • Certificate Hold

Setting up advanced user and debug modes

Certificate Explorer allows you to configure the level of information available to the user. Users who just want to view and find certificates do not usually need the same level of information as advanced users or administrators.

Because Certificate Explorer is a very powerful tool for looking at digital IDs and is useful for troubleshooting problems, the level of information it displays is configurable. In the default mode the user sees the level of information suitable for the average user; Advanced mode displays additional information, and Debug mode displays the largest amount of information.

Figure 22: Properties tab in Debug mode



For information about configuring the mode, see [“Display mode” on page 468](#).

What is displayed in Advanced mode

Advanced mode is designed for knowledgeable users or administrators. In Advanced mode the following additional columns are displayed in the Certificate view and Search Result view:

- Serial Number
- Signature Algorithm
- Not Before
- Public key Algorithm
- Basic Constraints (Extension)
- Key Usage (Extension)
- Extended Key Usage (Extension)
- Entrust Version Info (Extension)
- Subject Alternative Name (Extension)

What is displayed in Debug mode

In Debug mode, Certificate Explorer displays all of the details shown in Advanced mode plus the following:

- **Properties** tab in **Certificate** dialog box
- Additional columns in Certificate view
 - Key Container
 - CSP

Properties tab

The **Properties** tab shows most of the properties of the certificate. Certificate properties data saved with a certificate that apply to that certificate. For example, the specification of the Cryptographic Service Provider and key container name of a certificate's private key are contained within a property.

The properties are displayed by name if the name is known, otherwise the property number is shown. The names are not localized as this information is intended to be used to debug issues.

- Key Provider Info
- Enhanced Key Usage
- Root Program Certificate Policies
- Certificate Publication Pending (Entrust specific)
- Certificate Management State (Entrust specific)
- N-Key Event Identifier (Entrust specific)
- N-Key Event Indicator (Entrust specific)
- Archived
- Roaming Digital ID (Entrust specific)
- Rollover Not Allowed (Entrust specific)
- Mark For Deletion (Entrust specific)
- Missing Certificate History (Entrust specific)
- EDS CAPI Sync (Entrust specific)
- Role ID (Entrust specific)
- Policy Update Timestamp (Entrust specific—deprecated)
- Certificate Definition Name (Entrust specific)
- CSP Exported From (Entrust specific)
- Role Policy Certificate (Entrust specific—deprecated)
- Certificate Definition Policy Certificate (Entrust specific—deprecated)

Viewing policy certificates

Three policy certificates are used by ESP:

- the main policy certificate
- the role policy certificate
- the certificate definition policy certificate

The policy certificates are updated and cached on the local disk if:

- a policy is successfully managed by digital ID manager or the digital ID is logged into Entrust all three policy certificates are updated from the directory and saved
- the policy certificates cannot be downloaded from the directory by the certificate management component, the enrollment component retrieves the role policy certificate and the certificate definition policy certificate if it is available—the main policy certificate is not updated
- enrollment for, or recovery of, a digital ID occurs, the role policy certificate and the certificate definition policy certificate (if it is available) are cached to the local disk—the main policy certificate is not updated

There are two files (the content file and the metadata file) for each policy certificate downloaded from the network. The content file contains the encoded policy certificate. It is saved to:

```
<Local Application Data>\Entrust\ESP \PolicyCertCache\<hashed  
Distinguished Name of policy certificate's issuer>\Content
```

The meta data file contains ASN1 encoded policy certificate download information. It is saved to:

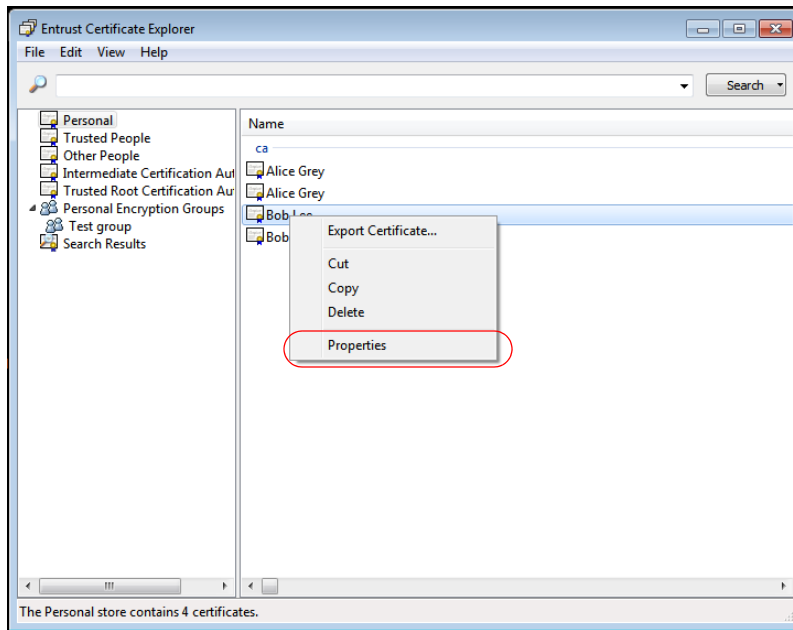
```
<Local Application Data>\Entrust\ESP \PolicyCertCache\<hashed  
Distinguished Name of policy certificate's issuer >\MetaData
```

The content file name and meta data file name are identical—a hash of the policy certificate DirectoryName.

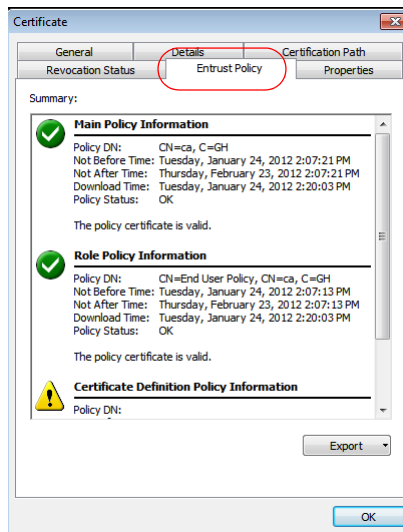
To view policy information from the Certificate Explorer

- 1** Open the Certificate Explorer (this can be done from the Security Provider menu).
- 2** Select the type of certificate from the left pane.

- 3 From the list in the right pane, right click on the certificate that you want and select **Properties**.



- 4 Click the **Entrust Policy** tab.



- 5 If the Export button is active and you want to export a policy certificate to file, click **Export**. If none of the policy certificates exist the button will be greyed out.

- If all three of the policy certificates exist, a drop down list displaying the policy certificate name opens allowing you to select the policy certificate to export. Select the policy certificate and the save file dialog box opens allowing you to save the policy certificate.
- If a policy certificate is missing, the policy certificate name in the drop down list will be grayed-out.

Customer support utility

The customer support utility is a command-line tool that is bundled with Entrust Entelligence Security Provider for Windows. The utility gathers system information and dumps it in a password-protected ZIP file which you can then email to Entrust customer support for troubleshooting purposes. The password-protection ensures the file can successfully pass through email filters. The password on the file is:

Entrust (Note the capital 'E')

Additionally, you can use the utility to clear information cached by Security Provider for Windows.

Topics in this section:

- ["Creating a dump ZIP file" on page 248](#)
- ["Clearing the cache" on page 249](#)

Creating a dump ZIP file

The following instructions describe how to create a simple dump file using the `-DUMPALL` command. This command collects the following information:

- operating system information
- registry data
- log files
- configured CA and LDAP directories
- all certificate stores including Personal, Intermediate CA, Root CA, Other People, and Trusted People stores
- Entrust data (version information, for example)
- cached data, including certificate, policy, and key access information

Note: There are many other commands available that allow you to dump subsets of the information described above. These commands are not documented here. For a list of these commands and their descriptions, run `eesputil.exe` from a command line. This file is located in `c:\Program Files\Common Files\Entrust\ESP`.

To create a dump file

- 1 Open a command prompt.
- 2 Change to `c:\Program Files\Common Files\Entrust\ESP (32 bit)` or `C:\Program Files (x86)\Common Files\Entrust\ESP (64 bit)` and enter:
`eesputil.exe`

A list of available command line operations is displayed.

3 Enter the following:

```
EESPUTIL -DUMPALL <filepath>
```

Where <filepath> is the path and name of your dump file, for example:

```
C:\MyESPdump\ESPdump2012.zip
```

If no location is specified, a file is created in the current user's Temp folder, for example:

```
C:\Documents and Settings\Administrator\Local  
Settings\Temp\eesputil_091001150359Z.zip
```

4 Email the ZIP file to Entrust customer support.

Note: The password for the file is Entrust.

Clearing the cache

Security Provider for Windows caches information from your PKI on the user's local computer. This caching improves performance, and also lets users use Security Provider while not connected to your PKI.

Cached information includes: CA policy data, the CRL data, CA certificate data, the user's certificate data, and key access certificates.

You can clear this information using the `-CLEARCACHE` command.

To clear cached information

1 Open a command prompt.

2 Change to `c:\Program Files\Common Files\Entrust\ESP` and enter:
`eesputil.exe`

A list of available command line operations is displayed.

3 Enter the following:

```
EESPUTIL -CLEARCACHE <argument>
```

Where <argument> is replaced with one of the following:

- `capolicy`—clears the CA policy cache
- `crl`—clears the certificate revocation list (CRL)
- `cacerts`—clears the CA certificate cache
- `usercerts`—clears the user's certificate data cache
- `keyaccess`—clears the key access certificate cache

- `polycyccerts`—clears the policy certificate cache
- `logbinarydetails`—clears the log cache (deletes the `LogBinaryDetails` folder from `\Entrust\ESP\`)

Usually these commands should be executed after the log binary files are harvested using the `eesputil -DUMPLOGS` command line.

Using Security Manager Administration

If you intend to deploy and manage Entrust digital IDs, Security Provider for Windows should be integrated with an Entrust PKI. Before you can enroll for an Entrust digital ID, you must configure policy and roles, and register Security Provider for Windows users and computers with Security Manager.

Note: Any changes to security settings, including certificate specifications, should be implemented in a manner consistent with your organization's security policy. For information on how to make these changes, see the *Entrust Authority Security Manager Administration User Guide*.

This chapter provides conceptual and procedural information on configuring the Entrust PKI in the following sections:

- [“Configuring user policy” on page 252](#)
- [“Certificate definition policy settings” on page 259](#)
- [“Configuring an Entrust computer or Windows service digital ID” on page 267](#)
- [“Registering users or computers” on page 268](#)
- [“Using other Security Manager features” on page 273](#)

Configuring user policy

A user policy allows you to set the environment and restrictions for users or computers. The user policy specifies policy attribute settings such as certificate contents, password rules, and algorithms. You configure these policy attributes by selecting or clearing check boxes, and by entering information into text fields. When you click the check box or text field of a given setting, a brief explanation of the setting appears at the bottom of the property page.

You can configure several user policy attributes for each user policy. Security Provider's Digital ID Monitor periodically checks for these updates and provides the updated policy to affected users and computers, as appropriate.

See the *Entrust Authority Security Manager Administration User Guide* for more information about policies.

Client policy settings

When you create a user or computer identity, a specific client policy is assigned based on the user or computer's role. You can assign client policies to one or more roles.

The following client policy settings are some of the settings that affect Security Provider for Windows users. Security Provider's Digital ID Monitor periodically checks for these updates and provides the updated policy to affected users and computers, as appropriate.

Managing login attempts

The **Maximum bad login attempts** and **Login attempt window** user policy settings only apply to users enrolling using the Entrust Enhanced CSP and an Entrust security store.

This **Maximum bad login attempts** setting lets you to configure the number of bad password attempts allowed before a user's Entrust security store is suspended. You can also configure the **Login attempt window**, allowing you to configure the time span in which to record bad password attempts as set in **Maximum bad login attempts**.

Security Provider for Windows supports the suspension of an Entrust security store after a configurable number of bad password attempts during a configurable length of time. By default, the **Maximum bad login attempts** setting in the user policy is set to 0 (or disabled), and the login attempt window setting in the user policy is set to 1 minute.

You can configure the Windows registry so that Security Provider for Windows supports the suspension of an Entrust security store. (See ["Entrust security store login settings" on page 396](#).) The Windows registry values enforce login attempts until the user successfully logs in to the Entrust security store for the first time. Once the user successfully logs in, the user policy begins to enforce all login attempts.

You enforce Entrust security store suspension by restricting access to the Entrust security store login and reauthentication dialog boxes. This feature also provides the ability to enable an Entrust security store centrally, and to log Entrust security store suspensions.

Use the The **Maximum bad login attempts** and **Login attempt window** user policy settings to control login attempts.

- **Maximum bad login attempts** (X)
Sets the number of unsuccessful login or reauthentication attempts within a time window (`pw_time_window` (Y)) that are suspicious. This value must be an integer between 0 and 32, where 0 is off.
- **Login attempt window** (Y)
Sets the period of time during which unsuccessful login or reauthentication attempts are recorded. This value must be an integer between 1 and 2880, where the value is in minutes. 0 is not an acceptable value.

If X unsuccessful attempts occur within the time period Y, the Entrust security store is suspended until the oldest record expires from the time window (making the number of unsuccessful attempts within the time window Y equal to X-1).

The following example demonstrates how this feature operates. Assuming a configuration where X = 5 attempts and Y = 5 minutes, Table 21 shows a sequence of unsuccessful login attempts.

Table 21: Example of unsuccessful login attempts

Entrust security store ID	Attempt	Time of unsuccessful attempt
12345	0001	12:00.00
12345	0002	12:01.00
12345	0003	12:01.50
12345	0004	12:02.00
12345	0005	12:03.00

Entrust security store ID 12345 becomes suspended at 12:03.00 and stays suspended until 12:05.00, when attempt 0001 expires. If there are no more unsuccessful attempts, the attempt record is empty by 12:08.00, when attempt 0005 expires.

Enabling a suspended security store

A suspended Entrust security store is automatically enabled when the specified time in **Login attempt window** expires. To enable an Entrust security store before the time window expires, an administrator must obtain a reference number and authorization code by recovering the Entrust digital ID, and then provide them to the user. The user

then recovers the Entrust security store using the **Recover Entrust Digital ID** wizard using the codes provided.

Logging security store suspensions

The logging tool built into Security Provider for Windows logs security store suspensions. Data logged includes the Entrust security store name and the date and time when the suspension was enforced. A login attempt with a suspended Entrust security store is considered a security event, and these attempts are logged. Data logged includes the security store name and the date and time of the login attempt.

Configuring password expiry times

The **Password expires in (weeks)** setting only applies to users enrolling using the Entrust Enhanced CSP and an Entrust security store. This setting designates the length of time a user's Entrust security store password is valid. When the set amount of time elapses, the password expires and the user is prompted to create a new password.

Password lifetimes can range from 1 to 52 weeks, or you can set the password lifetime to zero (0), which means the password never expires.

By default, **Password expires in (weeks)** is set to 0 (the password does not expire).

Setting roaming permission

The **Permit roaming** setting only applies to users enrolling using the Entrust Enhanced CSP and using Entrust roaming digital IDs. When **Permit roaming** is selected, users can access their Entrust roaming security store through the Roaming Server, regardless of where they are located or what machine they are using. When **Permit roaming** is not selected, users can only work as desktop users.

By default, the **Permit roaming** setting is selected. You must select at least one of **Permit desktop** and **Permit roaming**.

To force users to only use roaming digital IDs, disable the **Permit desktop** policy attribute.

For further information, see the *Entrust Authority Roaming Server User Guide*.

Note: If you enable roaming and subsequently disable it, roaming users can still log in to Security Provider. This login occurs because Security Provider performs the login operation before it checks the user policy.

Setting desktop permissions

The **Permit desktop** setting only applies to users enrolling using the Entrust Enhanced CSP and an Entrust security store. This setting designates whether or not users have their Entrust security store located on their computer.

You may wish to deselect the **Permit desktop** setting for roaming users as this reduces the risk of roaming users losing their locally stored Entrust security store when they are working outside the office.

By default, the **Permit desktop** setting is selected. You must select at least one of **Permit desktop** and **Permit roaming**.

Algorithm for digital signature

The **Algorithm for digital signatures** setting designates which algorithms users can employ for creating the signing private key. Roaming Server supports 4096-bit RSA or lower.

Configuring the inactivity timeout

The **Login timeout (minutes)** setting only applies to users enrolling using the Entrust Enhanced CSP and an Entrust security store. This setting designates how many minutes of inactivity must pass before the user is automatically logged out of the Entrust security store. The **Login timeout (minutes)** setting ranges from 0 to 300 minutes.

To prevent a timeout of the Entrust security store, set the value to 0. By default, **Login timeout (minutes)** is set to 15 minutes in the user policy.

Note: Users of Security Provider for Windows can use the **Log out after** setting in the **Entrust Security Store Options** dialog box to set a timeout that is less than or equal to the **Login timeout (minutes)** setting configured by the Security Manager administrator. The default in Security Provider for Windows is 15 minutes. You must install the taskbar status icon feature to allow users to configure this option.

Auto-associating certificates in Microsoft Outlook

The **Auto-Associate MS Outlook** setting specifies whether certificates managed by Security Provider for Windows are automatically associated with Microsoft Outlook. Configure this setting to enable the user to encrypt and sign email messages using native Microsoft Outlook security. When this setting is selected, there is no need to set up an association manually in Microsoft Outlook.

By default, the **Auto-Associate MS Outlook** setting is selected.

Managing key export

The **Private key export from CAPI** setting specifies whether users can export their private keys from their security stores. For the Entrust security store, you can update this policy value at any time. It is used the next time users attempt to export their private keys. For third-party security stores, the value is only used during enrollment and recovery; changing the policy afterwards does not affect existing private keys.

By default, the **Private key export from CAPI** setting is disabled.

Attention: Entrust has no control over third-party CSPs. Most smart card CSPs do not permit key export with smart cards. Third-party CSPs may ignore this setting.

Security Manager has a similar setting called **Private key export from CSP**. You configure this setting in the certificate definition policy settings. See [“Private key export from CSP” on page 264](#) for further information.

When you configure both the **Allow CAPI Key Export** and **Private key export from CSP** settings, the **Private key export from CSP** certificate definition policy takes precedence over **Allow CAPI Key Export** and **Private key export from CAPI**. The precedence only applies to the unarchived certificate for that certificate type, and only when the setting is selected (allowed). If the setting is unchecked, the **Allow CAPI Key Export** and **Private key export from CAPI** settings control if private key exporting is allowed. If the setting is selected, then the setting will apply to the unarchived certificate as well as any updated key-pairs that were created with this setting enabled.

Configuring **Allow PKCS#12 Export** allows users to export their profile (certificates) in PKCS#12 format.

Note: This precedence of policies is only true for keys that have not been archived. Certificate definition policies are not applied to archived certificates.

To allow all keys, archived and unarchived, to consistently be exportable, disable the **Private key export from CSP** certificate definition policy setting, and enable the **User Role Policy** setting **Allow CAPI Key Export** and **Private key Export from CAPI**.

For further information on allowing private key export from a CSP in Security Manager, see the *Security Manager Administration User Guide*.

Unprotected CAPI key storage

The **Unprotected CAPI key storage** setting specifies that, when Security Provider for Windows imports or creates a key in a security store, the key is unprotected (no passwords or other user interface appears). When this setting is selected, the user is not prompted when the key is accessed by an application.

When you configure both the **Unprotected CAPI key storage** and **Protected key storage for CSP** settings, the **Protected key storage for CSP** certificate definition policy takes precedence.

By default, this setting is disabled.

Note: Entrust CSPs ignore the **Unprotected CAPI key storage** setting.

Algorithm for profile protection

The **Algorithm for profile protection** setting only applies to users enrolling using the Entrust Enhanced CSP and an Entrust security store. This setting designates whether a user's Entrust security store is protected with Triple-DES instead of CAST.

When protecting an Entrust security store with Triple-DES instead of CAST, you must create a new Entrust security store. You cannot convert an existing Entrust security store from CAST to Triple-DES. To create a new Entrust security store, you must recover the Entrust digital ID, if it already exists, or create a new Entrust digital ID. Before beginning the enrollment or recovery, you must configure the user policy to include the `TRIPLE-DES` value.

The **Algorithm for profile protection** policy attribute is included automatically with Entrust Authority Security Manager 8.1.

To configure Security Manager 8.0

If you are running Security Manager 8.0, have a Security Officer add the following lines in the `master.certspec` file:

- Under the `[polcert_cliset Attributes]` heading:

```
; -----  
; profile protection algorithm policy  
; -----  
profile_protect_alg=1.2.840.113533.7.77.55,UTF8String,"<profile_protect_alg>"
```

- Under the `[Variables]` heading:

```
; profile protection algorithm policy  
profile_protect_alg=TextString,Algorithm for profile protection:,Algorithm used  
to protect the profile.,OneOf, "CAST","TRIPLE-DES"
```

To configure the Security Manager 8.0 `entmgr.ini` file

If you are running Security Manager 8.0, you must also set one of the following default values in the `[Default Variable Values]` section of `entmgr.ini` file:

- `profile_protect_alg=CAST` or `profile_protect_alg=TRIPLE-DES`

- restart Security Manager for the changes to take effect.

Security considerations

Keep in mind the following security considerations:

- For secure password attempt management, end user accounts on computers running Windows must not have administrative access privileges.
- The `HKEY_LOCAL_MACHINE` subtree of the Windows registry maintains the store's state and configuration data.
- Security Provider for Windows uses Windows system time for logging and for determining Entrust security store suspension based on security store state data. Because changing the system time in a Windows environment is only available to administrative users, end user accounts are restricted from tampering with the time used to log suspensions and security store state data.

Certificate definition policy settings

When you create a user or computer identity, and it is assigned a certificate type, each key pair may be assigned a certificate definition policy. The certificate definition policy settings determine the attributes of a user's or computer's keys and certificates.

The following certificate definition policy settings are some of those that affect Security Provider for Windows users.

Topics in this section:

- ["Policy settings for certificate definitions" on page 259](#)
- ["Configuring the certificate definition policy settings" on page 265](#)
- ["Keys and certificates with no certificate definition policy" on page 265](#)

Policy settings for certificate definitions

There are several policy attributes that you can configure for each certificate definition policy. This section describes the policy attribute settings that apply to Security Provider for Windows.

- ["CSP to manage keys" on page 259](#)
- ["Enable cert update date" on page 261](#)
- ["Cert update date" on page 261](#)
- ["Update cert at percentage of lifetime" on page 261](#)
- ["Only latest key can sign CMP" on page 262](#)
- ["Key can sign CMP" on page 262](#)
- ["Algorithm for key pair" on page 262](#)
- ["Back up private key" on page 263](#)
- ["Generate key at client" on page 263](#)
- ["Key usage policy" on page 263](#)
- ["Protect key storage for CSP" on page 264](#)
- ["Private key export from CSP" on page 264](#)
- ["Max key count" on page 264](#)
- ["CSP to export to" on page 264](#)

CSP to manage keys

In the certificate definition policy, you configure which CSP manages the key pair for that policy. If you do not specify the CSP in the certificate definition policy and the Force Token Usage role policy is set, the user will be prompted to select a smart card. If the Force Token Usage role policy is not set, then the CSP will be the one defined

in the CSP registry setting (see [“General CA settings” on page 348](#)). If this setting is not present, then the Entrust Enhanced Cryptographic Security Provider (CSP) is used to store all key pairs in an Entrust desktop security store (.epf) file format.

Attention: Setting the CSP using the registry setting is not recommended. This setting is local to the user’s computer and will not be used if they move to another computer. Use the CA policy instead.

When you want to specify a CSP in the **CSP to manage keys** setting, see [“To locate the list of CSPs in your Windows registry” on page 38](#).

Once you configure the CSP name in each of the certificate definition policies, the configured CSP manages the users’ keys when they enroll for their Entrust digital ID. The value can be a specific CSP name, which is useful if your enterprise has standardized on one smart card. Alternatively, you can set the value for **CSP to manage keys** to `Any SC`. This allows the user to select a smart card CSP from a list during enrollment or recovery.

When creating, recovering, or updating a digital ID, the default CSP is used for any key pair where the certificate definition policy setting **CSP to manage keys** is undefined.

When updating user key pairs, Security Provider retrieves the signing key pair’s CSP using the current signing certificate. Security Provider uses this CSP for any key pair with **CSP to manage keys** set to `Any SC`. Therefore, if the current signing key pair uses the default CSP, this default CSP—typically the Entrust Enhanced CSP—is used.

When you configure an EFS user (3-key-pair), enroll the EFS user using the Entrust Enhanced CSP to ensure that Security Provider for Windows can manage the EFS key pair by adding the key pairs to the Entrust security store.

When you are configuring a Standalone EFS User (2-key-pair), you must choose the Microsoft Enhanced Cryptographic Provider V1.0.

When you configure an Entrust computer or Windows service digital ID, configure a CSP that does not prompt the computer for a password, such as a Microsoft CSP. See [“Configuring an Entrust computer or Windows service digital ID” on page 267](#) for further information.

Use the following information:

- Microsoft does not support the use of smart cards with Microsoft EFS.
- If you are entering a smart card CSP in the Nonrepudiation Policy, ensure that you configure the smart card to prompt the user for a password whenever the nonrepudiation key is accessed.

Note: Check with the third party CSP vendor or their documentation to see if they have this capability and how to implement it.

- If the certificate definition policy is configured for the certificate type, and the **CSP to manage keys** certificate definition policy setting is empty or not specified, Security Provider uses the Entrust Enhanced CSP. In this case, the CSP setting in the registry is not checked.
- Do not configure the **CSP to manage keys** setting if you are integrating with a CardMS because this setting is ignored. For details on the CardMS integration, see [“Using a Card Management System” on page 188](#).

Enable cert update date

The **Enable cert update date** setting lets you enable or disable the date set for certificate update date (see [“Cert update date” on page 261](#)).

By default, the **Enable cert update date** setting is not selected.

Cert update date

The **Cert update date** setting specifies a date after which the client should request a new key pair and certificate.

You can set **Cert update date** to any date and time value. For example, you could enter the date 3/20/14 23:00 to indicate a date of 11:00 p.m. on March 20, 2014. The valid range is 31/12/1989 19:00 to 31/12/2037 19:00.

Update cert at percentage of lifetime

The **Update cert at% of lifetime** setting specifies when to update the user's or computer's certificates. With this setting you specify the time as a percentage of the certificate's lifetime between 0 and 99%. If this setting is defined, the Security Provider does the following:

- 1 checks the certificate lifetime of the latest encryption certificates
- 2 checks the private key lifetime of the latest verification certificates
- 3 updates the certificates when the identified percentage of the lifetime has passed

If you set **Update cert at% of lifetime** to 0, the certificate is updated at 50% of the certificate's lifetime, or 100 days, whichever is closer to the expiry date.

This setting works somewhat differently when the Security Provider registry setting `PrivateKeyUsagePeriodPercentage` is used. See page 388 for information about this registry setting.

Only latest key can sign CMP

The **Only latest key can sign CMP** setting specifies whether Security Manager should ensure that the private key that signed the client request is the latest key. Certificate Management Protocol (CMP) is the protocol used for communication between Entrust clients and Security Manager. This setting applies only to certificates that can sign client request messages.

By default, **Only latest key can sign CMP** is not selected.

Key can sign CMP

The **Key can sign CMP** setting specifies whether or not the client can use the private key to sign request messages. With this policy selected, at least one certificate definition must exist in the certificate type.

By default, if the key usage is for verification, **Key can sign CMP** is true. If the key usage is for encryption, this setting is false.

Note: When you configure certificate definition policy in Security Manager Administration, enable this setting for signing keys.

Algorithm for key pair

The **Algorithm for key pair** setting allows you to identify the algorithm used for the user's or computer's key pair in the case of client-generated keys. You can set **Algorithm for key pair** to one of the following values (using uppercase letters only):

- RSA-1024
- RSA-2048
- RSA-4096
- RSA-6144
- EC-P-256
- EC-P-384
- EC-P-521

This setting only applies when you enable the **Generate key at client** setting (see ["Generate key at client" on page 263](#)).

Do not configure the **Algorithm for key pair** setting if you are integrating with a CardMS because this setting is ignored. For details on the CardMS integration, see ["Using a Card Management System" on page 188](#).

Attention: When you configure algorithms for any third-party CSPs or Entrust Authority Roaming Server, ensure that you use a supported algorithm. With server-generated keys, configure the algorithm using the Security Manager's Control Command Shell.

Back up private key

In the case of client-generated keys, the **Back up private key** setting specifies whether the client should send the key to Security Manager for backup. In the case of Security Manager-generated keys, the **Back up private key** setting indicates whether Security Manager should back up the key.

Attention: You cannot back up verification keys. If you select a **Key usage policy** setting of **verification**, you cannot select the **Back up private key** setting. You must also back up keys generated by Security Manager, so you must select **Back up private key** if you do not select **Generate key at client**.

By default, **Back up private key** is selected for encryption and dual-usage certificates, and not selected for verification certificates.

Generate key at client

The **Generate key at client** setting specifies whether the client (in this case Security provider) generates the key. The client must generate verification keys. If you specify **Key usage policy** of **verification**, you must select **Generate key at client**.

By default, **Generate key at client** is selected for verification and dual-usage certificates, and not selected for encryption certificates.

Key usage policy

The **Key usage policy** setting specifies the purpose of the key pair as **encryption**, **verification**, or **both**.

The **Key usage policy** value must also match the value set in the `master.certspec` file for the certificate definition. If it does not, an error occurs. This setting is mandatory, so do not leave it empty.

Security Manager supports the following **Key usage policy** values:

- **encryption** for encryption and EFS certificates
- **verification** for verification and nonrepudiation certificates
- **both** for dual-usage certificates

Protect key storage for CSP

The **Protect key storage for CSP** setting specifies the level of protection (password protection, notification, or other) applied to keys stored in a CSP key storage medium. This setting is ignored by the following:

- CSPs that are password protected by default, such as Entrust CSPs and smart card CSPs
 - an Entrust computer or Windows service digital ID
- See [“Configuring an Entrust computer or Windows service digital ID” on page 267](#) for further information.

By default, the **Protect key storage for CSP** setting is selected and password-protects the CSP key storage medium.

Private key export from CSP

The **Private key export from CSP** setting specifies whether to allow export of the user's private keys (including archived keys) from the CSP. Some CSPs, such as smart card CSPs, ignore this setting.

By default, **Private key export from CSP** is not selected.

Max key count

The **Max key count** setting specifies the maximum number of keys to store on the smart card. Once the card reaches that number, the Key Access Service of Security Provider removes the oldest key or keys.

By default, the **Max key count** setting is not available. A Security Officer must add it to the `master.certspec` and `entmgr.ini` files.

For information about the Key Access Service and on configuring this attribute, see [“Additional Entrust digital ID management for smart cards” on page 88](#).

CSP to export to

Use this setting if you want the keys stored in an Entrust security store (.epf file) exported to a specific CSP. Once **CSP to export to** is set, the export occurs the next time the user logs in to a computer with that .epf file. If you later change this setting to null (no CSP name), the key is deleted from the CSP.

By default, the **CSP to export to** certificate definition policy attribute is not available. A Security Officer must add it to the `master.certspec` and `entmgr.ini` files.

To add the attribute to Security Manager

- 1 Have a Security Officer export the `master.certspec` file and open it in a text editor.

2 Under the [polcert_certdefn Attributes] heading, add:

```
cd_key_export_csp=1.2.840.113533.7.77.46.5.12,UTF8String,"<cd_key_export_csp>"
```

3 Under the [Variables] heading, add:

```
cd_key_export_csp=TextString,CSP to export key to:,The name of the CSP that the  
private key will be exported to. If no value is given, the key is kept in the  
original CSP.,Range,0,200
```

Save and import the modified master.certspec.

After adding this attribute to the master.certspec file, you can set or change it at any time using Security Manager Administration (see [“Configuring the certificate definition policy settings” on page 265](#)).

Configuring the certificate definition policy settings

Once you determine the policy attribute settings for each certificate definition policy, configure the certificate definition policy settings in Security Manager Administration. See [“Policy settings for certificate definitions” on page 259](#) for information on choosing settings configuration for your certificate definition policy settings.

To configure the certificate definition policy settings

- 1** Log in to Security Manager Administration as a Security Officer or as an administrator with permissions to configure certificate definition policies.
- 2** In the tree view, expand **Security Policy > User Policies**.
- 3** Select the certificate definition policy that you want to configure.
- 4** Click the **General Information** tab.
- 5** Click **Yes** to change policy types.
- 6** Under **Policy Attributes**, enable policy settings that apply to the certificate definition policy chosen in [Step 3](#).
See [“Client policy settings” on page 252](#) for detailed information on all policy settings you can configure.
- 7** Click **OK**.
A confirmation appears.

Keys and certificates with no certificate definition policy

During an enrollment, recovery, or key update, Security Manager uses the following hard-coded default values when you do not configure a certificate definition policy for a certificate definition in the certificate type. Security Provider for Windows cannot control this. The certificate type must contain exactly two definitions, and they must be **Encryption** and **Verification**. If the two definitions are missing, the enrollment, recovery, or update fails.

Attention: Do not change the names or leave the names blank for default certificate definitions or default certificate definition policies in Security Manager Administration. If you change the default names or make them unavailable, Security Provider for Windows cannot determine which keys and certificates to create during the enrollment process.

Table 22: Default Encryption certificate definition policy

Certificate definition policy setting name	Value
Generate key at client	FALSE
Back up private key	TRUE
Key usage policy	encryption
Key can sign CMP	FALSE
CSP to manage keys	CSP value in registry, or Entrust Enhanced CSP if registry value is empty
Private key export from CSP	value of Private key export from CAPI setting in role policy
Protect key storage for CSP	value of Unprotected CAPI key storage setting in role policy

Table 23: Default Verification certificate definition policy

Certificate definition policy setting name	Value
Generate key at client	TRUE
Back up private key	FALSE
Key usage policy	verification
Key can sign CMP	TRUE
CSP to manage keys	CSP value in registry, or Entrust Enhanced Cryptographic Provider if registry value is empty
Private key export from CSP	value of Private key export from CAPI setting in role policy
Protect key storage for CSP	value of Unprotected CAPI key storage setting in role policy

Configuring an Entrust computer or Windows service digital ID

The required capability for an Entrust computer or Windows service digital ID varies depending on the needs of your organization. Authentication is the most common use of a this digital ID. For authentication, you require a signing key pair. If you also need the Entrust computer or Windows service digital ID to encrypt data, which is less likely, then there are two possible choices:

- Include a second key pair for key encipherment (encryption), with your required signing key pair.
- Use one dual-usage key pair instead of the required signing-only key pair. The dual-usage key pair can perform both signing and encryption operations.

Note: Your organization determines the required capability for an Entrust computer or Windows service digital ID. The choices listed are only suggestions offered to help administrators understand how to use an Entrust computer or Windows service digital ID.

To customize certificate types for computer or Windows service digital IDs or other requirements, you need to export the `master.certspec` file using Security Manager Administration, edit it in a text editor, and import it back. Often, you also need to edit the `entmgr.ini` file. Please ask your organization's Security Officers to make the necessary changes. Information on how to configure certificate types using the *Entrust Authority Security Manager Administration User Guide*.

Registering users or computers

When you register a new user, computer, or a domain controller, you must enroll them for an Entrust digital ID using Entrust applications such as Security Manager Administration or Administration Services.

See the following topics for information about Administration Services:

- [“Creating digital IDs in Administration Services” on page 148](#)
- [“Using the Auto-enrollment Service \(Administration Services\)” on page 149](#)

When you register a new user, computer, or domain controller in Security Manager Administration, you need to create an identity and do the following:

- 1** assign a role to the entity
- 2** assign V2-key-pair users a certificate type
- 3** distribute the activation codes (only in the case of manual enrollment or recovery)

When registering users, computers, or domain controllers in Security Manager Administration, Security Manager Administration adds the required entry to your directory if it is an LDAP directory. If you use Active Directory, an entry must already exist in Active Directory before you can add it to Security Manager Administration. In either case, you always register entries using Security Manager Administration that already exist in the directory.

To register new entries with Security Manager Administration

- 1** Log in to Security Manager Administration as an administrator with permissions to create users.
- 2** Select **User > New User** from the menu.
The **New User** dialog box appears.
- 3** In the **Type** drop-down list:
 - For users, select **Person** (LDAP) or **User** (Active Directory).
 - For computers, select **Person** or **Web Server**.
 - For domain controllers, select **Web Server** (LDAP) or **User** (Active Directory).
- 4** Click the **Naming** tab.
- 5** In the **First name** and **Last name** fields, enter the name of the user, computer or domain controller.
If required, enter values in the **Serial number** and **Email** address fields.
- 6** In the **Add to** drop-down list, select the searchbase where you want to store the user information.

Note: Do not select the **Create profile** check box. End users use the wizard in Security Provider for Windows to create their Entrust digital ID.

- 7** Click the **General** tab.
- 8** In the **User role** drop-down list, select a role. The role that you assign has a user policy associated with it.
- 9** Click the **Certificate Info** tab.
- 10** In the **Category** drop-down list, select **Enterprise**.
- 11** In the **Type** drop-down list, select a certificate type.
If you are creating a digital ID for a computer, a Windows service, or domain controller, you may need to create a new certificate type. See ["Configuring an Entrust computer or Windows service digital ID" on page 267](#) for details.
- 12** Click the **Key Update Options** tab and configure any options the user requires.
See the *Entrust Authority Security Manager Administration User Guide* for more information about these options.
- 13** Click **OK** to create the user.
You are prompted to authorize this activity.
- 14** Confirm the prompt.

The **Operation Completed Successfully** dialog box confirms the user creation. The dialog box displays the activation codes (reference number and authorization code) that you must distribute to the user in a secure manner. The activation codes are needed during the enrollment process.

To register an entry Security Manager Administration that already exists in the directory

- 1** Log in to Security Manager Administration as an administrator with permissions to create users.
- 2** Select **Users > Find > By Directory Attributes**.
The **Find Users by Directory attributes** dialog box appears.
- 3** In the **Type** drop-down list, select **Person** (LDAP) or **User** (Active Directory).
- 4** In the **Searchbase** drop-down list, select the searchbase of the entry.
- 5** Use the **First Name**, **Last Name**, **Serial Number**, and **Email** fields to narrow the search results.
- 6** Enter an asterisk in each of the four fields to search for all entries.
You can also use an asterisk in combination with characters in any of the fields to help narrow the search.

Note: Performance improves substantially when you include specific search information.

7 Click **Non-Entrust users**.

This option does not appear for Active Directory.

8 Click **Find**.

When the operation completes, all found entries appear in the right-hand pane.

9 Select the entry you want to modify and then select **User > Selected User > Properties**.

The **User Properties** dialog box appears.

10 Click the **General** tab. The **User DN** field is populated with information from the directory.

11 In the **User role** drop-down list, select the appropriate role.

12 Add a subjectAltName to the entry as follows:

a Click the **SubjectAltName** tab.

b Click **Add**.

The **Add subjectAltName component** dialog box appears.

c Under **Select component name**:

– For users, select and enter an appropriate subjectAltName.

– For computers and domain controllers, select **DNS name** and then enter the value in the **Enter component value** field. You can find the `dNSName` attribute in your directory.

– You must also add `MsGUID` if you need to support SMTP replication between domain controllers. See the Microsoft Knowledge base article 224544 "Determining the Server GUID of a Domain Controller" for more information.

13 Select a **User role** from the drop-down list. The role that you assign the computer has a user policy associated with it.

14 Click the **Certificate Info** tab.

15 In the **Category** drop-down list, select **Enterprise**.

16 In the **Type** drop-down list, select a certificate type.

Attention: Do not use a Netscape Certificate Extension Definition when you use the domain controller certificate to enable SSL on Active Directory.

If you are creating a digital ID for a computer, a Windows service, or domain controller, you may need to create a new certificate type. See ["Configuring an](#)

[Entrust computer or Windows service digital ID" on page 267](#) for details.

17 Click the **Key Update Options** tab and configure any options the user requires.

See the *Entrust Authority Security Manager Administration User Guide* for more information about these options.

18 Click **OK** to create the user.

You are prompted to authorize this activity.

19 Confirm the prompt.

The **Operation Completed Successfully** dialog box confirms the user creation. The dialog box displays the activation codes (reference number and authorization code) that you must distribute to the user in a secure manner. The activation codes are needed during the enrollment process.

End user, computer, or Windows Service activation

Once you register users or computers, or Windows services in Security Manager Administration, the Security Provider administrator needs to distribute the activation codes to the end user or computer to complete the registration. You can activate the registration in one of the following ways:

- Use the activation codes during the **Enroll for Entrust Digital ID** wizard process in Security Provider for Windows.
- Use Entrust Authority Administration Services to register and administer users in Security Manager:
 - Administration Services may or may not require an administrator for end-user registration, depending on the configuration. Users can complete a Web form to initiate a registration operation, and Administration Services can complete the operation automatically.
 - To let Security Provider for Windows users enroll using Administration Services, use the **Custom Installation** wizard to set the URLs they need to access the Administration Services for enrollment or recovery.
- The administrator or computer uses the activation codes during the **Enroll Computer for Entrust Digital ID** (or Windows service) wizard process in the Entrust Computer Digital ID Snap-in (or Windows service) application.
- Use Entrust Authority Administration Services, Auto-enrollment Service to auto-enroll users or computers in Security Manager:
 - Auto-enrollment Service does not require the involvement of an administrator, end user, or person at a computer. Auto-enrollment is completely transparent. It does not display dialog boxes, password-prompts, wizards, or error messages.
 - To let Security Provider for Windows auto-enroll or auto-recover, you must configure Security Provider for Windows to use the Auto-enrollment Service. See ["Using the Auto-enrollment Service \(Administration Services\)"](#)

[on page 149](#) for further information.

Using other Security Manager features

You can configure several other features in Security Manager to work with Security Provider for Windows. This section describes the following Security Manager features:

- [“Updating Entrust digital IDs” on page 273](#)
- [“Obsoleting certificate types” on page 274](#)
- [“Moving users from one Entrust Security Manager CA to another” on page 275](#)
- [“Changing distinguished names” on page 276](#)
- [“Deactivating users” on page 277](#)
- [“Moving an Entrust digital ID from one security store to another” on page 277](#)

Updating Entrust digital IDs

When users have copies of their Entrust digital ID in other Entrust security store locations, the copy can become outdated. When this occurs, you can have Security Manager automatically update each copy to synchronize it with the original Entrust digital ID.

To synchronize an old copy of an Entrust digital ID with the latest version, the Certification Authority (CA) must allow the client to use out-of-date signing keys to protect CMP messages sent to the CA.

Note: If you add a new certificate definition to a user's certificate type, and the user receives this update when logging in to the Entrust security store, you must delete any old copies of the Entrust security store. You cannot synchronize old copies of the Entrust digital ID after you add a new certificate definition.

Certificate types that have certificate definition policy

When users have certificate types with a certificate definition policy, complete the following to enable the Entrust digital ID synchronization feature. Most V2 key pair users are in this category.

When you configure users in Security Manager Administration, you must disable the **Only latest key can sign CMP** setting in the Verification Policy. This setting ensures that all certificate types with Verification Policy can synchronize without a problem. By default, **Only latest key can sign CMP** is disabled.

Certificate types that do not have certificate definition policy

When users have certificate types with no certificate definition policy, complete the following to enable the Entrust digital ID synchronization feature. For example, users with the Default (`ent_default`) certificate type fall into this category.

A master user must log in to Security Manager Control Command Shell and run the following command:

```
db set AllowSignWithOldKeys 1
```

Obsoleting certificate types

If your organization no longer uses a certificate type, you can delete it if you specify a replacement certificate type.

You make a certificate type obsolete by defining its replacement certificate type in Security Manager Administration. When you make a certificate type obsolete, ensure that the replacement certificate type has a superset of the certificate definitions in the obsolete certificate type. For example, if the obsolete certificate type has encryption, verification, and EFS certificate definitions, then the replacement type must include these three certificate definitions plus any other required certificate definitions.

When Security Provider for Windows detects an obsolete certificate type with no key update pending, it does not make any changes if the replacement certificate type has the same certificate definitions. If the replacement certificate type has any additional certificate definitions, Security Provider for Windows updates all certificates with new ones.

See the **Notify Client** feature in the *Entrust Authority Security Manager Administration User Guide* for information on how to alert Security Provider for Windows about changes it may not normally notice.

Moving users from one Entrust Security Manager CA to another

This section describes moving a user from a Security Manager CA to another Security Manager CA. The original and destination CA must have directory connectivity, and be cross-certified or in a hierarchy. Two CAs that simply trust each other cannot accomplish automatic moves.

Once the export is complete at the original CA, the automatic move can take place. The state of the CA is checked for a user during digital ID management. If the state is Export, Security Provider for Windows moves the user to the new CA. Security Manager 8.x provides Security Provider for Windows with the distinguished name of the new CA. This allows Security Provider for Windows to look up the registry data (for example, the `Authority` and `Proxy` name and port) for the new CA, and begin communication.

The move has the same look and feel for the user as a digital ID update.

If a user in your organization needs to be managed by a different CA than the one they were enrolled to, Security Provider for Windows supports moving the user from the original CA to a new CA. For reasons why you would want to move a user, and for the steps required in Security Manager to move a user, see the *Entrust Authority Security Manager Administration User Guide*.

Note: If you did not configure the new CA in the user's registry, you must add it before moving the user.

The Security Manager documentation explains that there are three main steps involved in moving a user in Security Manager. They are:

- 1** The user is exported from the original CA. The user is now in the Export Hold state at the original CA.
- 2** The user is imported into the new CA. The user is now in the Import state at the new CA.
- 3** The export is completed at the original CA. The user's state changes from Export Hold to Export at the original CA.

If the original CA and new CA are both recent versions of Security Manager, users are moved automatically when the Digital ID Monitor detects that the move is required. This feature will not work with Security Manager 6.x or lower.

If users have multiple copies of their Entrust digital ID, they must delete any old copies after the move to the new CA.

Details for Security Manager

The user's certificates and key pairs that were imported to the new CA have the certificate type and certificate definition set to unknown, as the import file does not contain this type of information. The new CA does not know what certificate type the user had at the old CA. In addition, these imported keys and certificates do not have associated certificate definition policy. Regardless of the user's certificate type in the new CA, the imported keys and certificates from the old CA are not mapped to the certificate type in the new CA.

Security Provider for Windows finds the configuration details for the new CA in the registry. It also reads the `CSP` value in the registry to determine where to import the old keys and certificates. The `CSP` value in the registry should be the same as the **CSP to manage keys** setting in the certificate definition policies, for the certificate type at the new CA. This ensures that the user's key pairs from the old CA end up in the same place as the new key pairs.

The Entrust Enhanced Cryptographic Provider is the default CSP when no other CSP is configured in the registry. However, the certificate type may have an associated CSP.

- If no changes are made to the **CSP to manage keys** setting in the certificate definition policies, during the move the user's newly created key pairs exist in that associated CSP.
- Security Provider for Windows reads the `CSP` value in the registry for the key pairs from the old CA (key history) and places them in the (default) Entrust Enhanced Cryptographic Service Provider's security store.
- If you change the `CSP` value in the registry to the CSP associated with the certificate type, all the user's key pairs go to the same place.

Note: Since the `CSP` value in the registry can only have one CSP name, all the imported keys and certificates from the old CA are managed by the same CSP.

Microsoft Base CSP does not support RSA-2048. Security Manager 8.1 and higher enforces a minimum protocol cryptographic key size of RSA-2048. If you try to enroll a user using the Microsoft Base CSP, and if Security Manager is enforcing the default value, the enrollment will fail. You can, however, use Microsoft Enhanced Cryptographic Service Provider v1.0 or Microsoft Strong Cryptographic Service Provider with the secure key size.

For SHA1 support, add SHA1 to the setting `ProtocolSigningAlgs`.

Changing distinguished names

You can change the user's distinguished name in the directory or assign a new name, depending on your directory type. Changing the DN is useful if, for example, the

user's name has changed. You must issue new certificates with the new DN to the user through a key update.

When you update key pairs, they are replaced with new key pairs and new public key certificates are created. Security Provider for Windows receives the new certificates in a secure fashion. Users see an Entrust digital ID **Update Request** icon in their taskbar notification area. The user must click the icon to begin the update process. The Entrust digital ID **Update Request** dialog box appears.

Deactivating users

When you deactivate users, their Entrust information is removed from their entry in the directory and updates no longer occur. A copy of the information is stored in the Security Manager database so you can reactivate them later.

Note: If you added a user to Security Manager, but have not yet enrolled the Entrust digital ID, deactivating it removes all user information, including the information in the Security Manager database.

Activated users can continue to encrypt files for deactivated users if they have their encryption certificates.

Once users are deactivated, they can continue to log in to their Entrust security store or third-party security store. When users are deactivated, if there are no updates pending for the Entrust digital ID, they are not notified about deactivation when logging in to their security store. However, if the digital ID management feature detects a key update is necessary, users see an error message. The error message indicates that a user was deactivated and can no longer receive key updates.

Moving an Entrust digital ID from one security store to another

You can change a digital ID storage location, for example, from an Entrust security store (.epf) to a smart card. This process involves performing these tasks in Security Manager:

- creating a policy certificate for each key pair being transferred (the key pairs must be V2 in the case of a smart card)
You set the **CSP to manage keys** policy attribute name of the desired store (for example, the smart card CSP name).
- creating a certificate type for the previous policy certificates
- changing the user certificate type

After completing these tasks, the user's Entrust security store is migrated automatically to the desired security store (for example, a smart card) the next time the user logs in to their Entrust security store, or the next time the Digital ID Monitor

performs a check. No recovery of the digital ID is required. The details of moving to a different security store are provided below.

For more on the Digital ID Monitor, see [“How the user experiences key management” on page 85](#).

To move an Entrust digital ID from to a different security store

- 1** Log in to Security Manager Administration as a Security Officer or as an administrative user with appropriate permissions. See the *Entrust Authority Security Manager Administration User Guide* for details on logging in.
- 2** Create a policy certificate for each key pair you want to transfer.

The easiest way to do this is to copy the existing policy certificates. In Security Manager Administration, right-click a policy certificate and select **Copy**. Rename the new policy certificate and set the **CSP to manage keys** policy attribute to the desired CSP name (for example, the smart card CSP name). See the *Entrust Authority Security Manager Administration User Guide* for details about changing a user policy.
- 3** Create a certificate type for the policy certificates you created in [Step 2](#).

The easiest way to do this is to copy the user's existing certificate type.

 - a** Export the certificate definitions to the `master.certspec` file.
 - b** Copy the user's certificate type into the `master.certspec` file.

The new certificate type must have a different name.
 - c** Import the modified `master.certspec` file.

See the *Entrust Authority Security Manager Administration User Guide* for details about creating a new certificate.
- 4** Map the policy certificates created in [Step 2](#) to the new certificate type using Security Manager Administration. See the *Entrust Authority Security Manager Administration User Guide* for further details about mapping policy certificates to certificate definitions.
- 5** Find the user whose Entrust digital ID will be transferred.
- 6** Using Security Manager Administration, open the **User Properties** dialog box for that user and select the **Certificate Info** tab.
- 7** In the **Type** list, select the certificate type you created in [Step 3](#).

You have now enabled moving a V2-key-pair user's Entrust digital ID or specified key pairs to a different security store. To move another user's Entrust digital ID, repeat steps 5 to 7.
- 8** To complete the transfer:
 - a** Be sure that the new security store is accessible. For example, if the users will be using smart cards have them insert their smart cards.

b Have the users log in to their Entrust security stores.

Upon login, Security Provider's Digital ID Monitor detects that the user's certificate type has changed, and consequently performs a silent key recovery of the digital ID. The silent key recovery places the appropriate keys and certificates on the smart card without requiring the user to type in activation codes. The original security store (.epf file) is deleted.

If the Digital ID Monitor detects that the user's certificate type has changed before the user has a chance to enter their smart card (assuming that they are using smart cards), the user is asked to insert their smart card so that the digital ID can be transferred.

The digital ID has been transferred.

Deploying Security Provider for Windows

This chapter describes how to deploy, upgrade, and apply patches to Security Provider for Windows.

Topics in this chapter:

- [“Deployment worksheet” on page 282](#)
- [“Customizing the installation” on page 285](#)
- [“Packaging the installation” on page 297](#)
- [“Testing the installation” on page 303](#)
- [“Distributing the installation package” on page 304](#)
- [“Upgrading Security Provider” on page 306](#)
- [“Deploying service packs and patches” on page 308](#)
- [“Deploying language packs” on page 310](#)

Deployment worksheet

The following worksheet describes the high-level steps to deploy Security Provider for Windows. Many steps are feature-specific. For a list of Entrust digital ID features, CryptoAPI enhancements, and bundled applications, see [Table 3 on page 27](#).

Table 24: Deployment worksheet

Step	Details
1 Review system requirements.	System requirements are listed in the <i>Security Provider for Windows Release Notes</i> available on the Entrust TrustedCare Web site (https://www.entrust.com/trustedcare/).
<i>Perform the following steps if you plan to deploy Entrust digital ID features.</i>	
2 If not already done, install Security Manager and its directory and database.	See the <i>Entrust Authority Security Manager Installation Guide</i> .
3 Create entries for users or computers in Security Manager.	See “Using Security Manager Administration” on page 251 .
4 Install other Entrust products, as required.	See the following guides: <ul style="list-style-type: none">• <i>Entrust Authority Administration Services Installation Guide</i>• <i>Entrust Authority Roaming Server Administration Guide</i>• <i>Entrust Authority Security Manager Proxy Administration Guide</i>• <i>Entrust TruePass Installation and Configuration Guide</i>
5 Install and integrate a Card Management Server, if required.	You must install a CardMS if you plan to use the CardMS feature: <ul style="list-style-type: none">• For CardMS installation instructions, consult the CardMS vendor's documentation.• For integration instructions, see “Using a Card Management System” on page 188.

Table 24: Deployment worksheet (continued)

Step	Details
<i>Perform the following steps if you plan to deploy CryptoAPI enhancements.</i>	
6 Install a directory, if you have not done so already.	<p>You must install a directory if you plan to use either of the following CryptoAPI enhancements:</p> <ul style="list-style-type: none"> • Certificate Path Validation • CRL Revocation Provider <p>If you installed Security Manager, you can use its directory; otherwise, install a directory according to the directory vendor's documentation.</p>
7 Install an OCSP responder.	<p>You must install an OCSP responder if you plan to use the OCSP Revocation Provider feature.</p> <p>See the OCSP vendor's documentation.</p>
<i>Perform the following step if you plan to deploy bundled applications.</i>	
8 Install a directory, if you have not done so already.	<p>You must install a directory if you plan to use either of the following bundled applications:</p> <ul style="list-style-type: none"> • Certificate Explorer • File Security <p>If you installed Security Manager, you can use its directory; otherwise, install a directory according to the directory vendor's documentation.</p>
<i>Perform the following steps to configure and deploy Security Provider.</i>	
9 Download the applicable Security Provider for Windows installation package and the Custom Installation wizard and extract the ZIP files. Be sure that use the latest version of Security Provider for Windows, including patches. Note: Always use the latest version of the Custom Installation Wizard.	Obtain the software at the Entrust TrustedCare Web site at https://www.entrust.com/trustedcare/ . To access the site, use the user name and password provided to you in a customer letter.
10 Customize the Security Provider installation package.	See “Customizing the installation” on page 285.
11 Package the installation.	See “Packaging the installation” on page 297.

Table 24: Deployment worksheet (continued)

Step	Details
12 Test the installation.	See “Testing the installation” on page 303.
13 Distribute the installation.	See “Distributing the installation package” on page 304.
14 Install Security Provider.	See “Installing Security Provider” on page 305.
15 Install a language pack.	See “Deploying language packs” on page 310.

Customizing the installation

Security Provider provides a basic installer (.msi) file that you can customize before deploying Security Provider to your users. Table 25. describes two methods to customize the installer.

Note: During an individual installation, after the user has configured the Security Provider options using the Custom Installation wizard, executing the Security Provider setup file starts the Windows installer. The Windows installer offers the usual **Typical**, **Custom**, or **Complete** installation options. **Typical** installs the features you selected in the configuration wizard. **Custom** allows users to reconfirm their choices, **Complete** installs all Security Provider features, no matter what was selected in the wizard.

Attention: If patches are available, be sure that you install Security Provider with the latest patch. Administrators are encouraged to check the installation before distributing it to users.

Table 25: Customization methods

Method	Details
Using a wizard	You can use the Custom Installation wizard to specify basic features and custom settings. When users install Security Provider, the installer enables the basic features and adds all your custom settings to the user's Windows registry. For instructions, see "Customizing the installation using the wizard" on page 290 .
Using a wizard and Microsoft Group Policy	You can use the Custom Installation wizard to specify basic features. You can then add all remaining Security Provider custom settings directly to users' Windows registries through Microsoft Group Policy. For instructions, see "Customizing the installation using the wizard and Group Policy" on page 295 .

Selecting application features

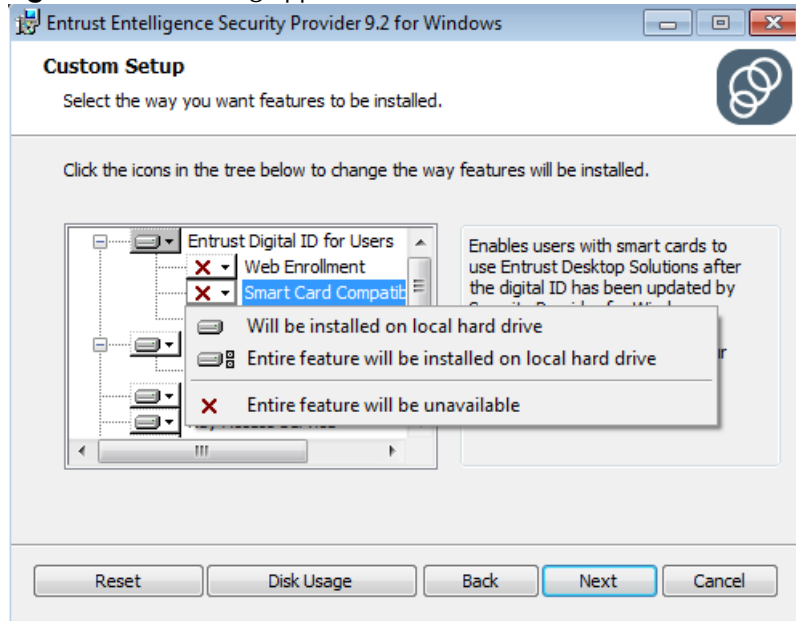
When you work through the **Custom Installation** wizard, as explained in ["Customizing the installation using the wizard" on page 290](#), you need to pay attention to the selections available on the **Select Application Features** page. Not all features are automatically included in an install. To add the non-default features or to remove default features, you create a transform file that adds or

removes the features you want. You configure these features using the **Select Application Features** page.

Adding and removing features

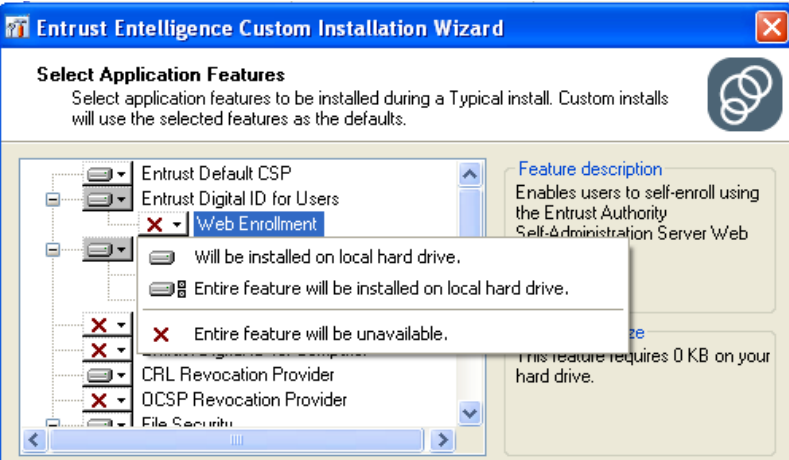
When the **Select Application Features** page of the wizard appears, it looks like the following.

Figure 23: Selecting application features



The standard features included in the install have a hard disk icon beside the feature label. Those features not included in the install have a red X icon beside the feature label. In both cases, there is an option arrow on the right side of the icon. Click this arrow to view options for adding or removing a feature.

Figure 24: Menu for selecting or deselecting application features



To select just one feature in each branch of the feature tree, select **Will be installed on local hard drive**. To select all features in each branch of the feature tree, select **Entire feature will be installed on local hard drive**. The scope of the **Entire feature will be unavailable** option depends on where in the feature tree you select it.

Learning what the features do

Click on any feature. A description of that feature and the resources it requires appears in the text fields on the right. Table 26 provides similar information and links to further details.

Table 26: Application feature descriptions

Feature	Subfeature	Description
Entrust Digital ID for Users		Provides an interface where users can enroll for a digital ID and recover an ID. See “Entrust digital ID enrollment and recovery” on page 64.
	Web Enrollment	Allows users to enroll for a digital ID using Entrust Administration Services. See “Creating digital IDs in Administration Services” on page 148.
	Smart card compatibility	Allows the user to use a digital ID stored on a smart card.

Table 26: Application feature descriptions (continued)

Feature	Subfeature	Description
	PKI Configuration Validation	<p>After the user installs Security Provider for Windows, this feature causes a warning dialog box to be displayed to the user indicating that no PKI or directory server was configured (if this is indeed the case). The warning also indicates that no digital ID management can occur without a PKI or directory.</p> <p>This warning is intended as a troubleshooting tool to catch misconfigurations before they are deployed organization-wide. This insures that an administrator will see this error while testing out the Security Provider installation, and modify the installation with the requisite PKI and directory settings. The properly-configured software can then be deployed to a larger user base.</p>
Entrust Security Store		Provides user login and secure key storage in an .epf file. See “Entrust security store” on page 52 .
	Taskbar Status Icon	Determines if the taskbar icon appears in the system tray. See “Taskbar status icon” on page 55 .
Key Access Service		Allows smart card users to use encryption keys that are no longer stored on the smart card. See “How the Key Access Service works” on page 88 .
Entrust Digital ID for Computer		Provides a way for computers to enroll for an Entrust digital ID or recover a digital ID. See “Entrust digital ID enrollment and recovery” on page 64 .
Entrust Digital ID for Windows Services		Provides a way for Windows Services to enroll for an Entrust digital ID or recover a digital ID. See “Entrust digital ID enrollment and recovery” on page 64 .
CRL Revocation Provider		Enables certificate revocation checking using CRLs. See “CRL Revocation Provider” on page 136 .
OCSP Revocation Provider		Enables certificate revocation checking using an OCSP responder. See “OCSP Revocation Provider” on page 139 .
File Security		Provides encryption, decryption, verification, and timestamping of files. See “File Security application” on page 202 .

Table 26: Application feature descriptions (continued)

Feature	Subfeature	Description
	Encryption/ Digital Signature	Allows user to encrypt and sign files in S/MIME format. See “File Security application” on page 202.
Entrust Password Encrypt		Allows users to encrypt and decrypt files with a password. See “Password Encrypt application” on page 221.
Automatic Additional Certificate Download		Allows automatic retrieval of Security Manager cross-certificates. See “Automatic additional certificate download” on page 100.
Certificate Path Discovery		Enhances certificate path discovery to support retrieving certificates. See “About the Certificate Path Discovery feature” on page 142.
Certificate Path Validation		Enhances certificate path validation. See “About the Certificate Path Validation feature” on page 143.
Entrust TrueDelete		Allows users to delete files in a secure manner. See “TrueDelete application” on page 230.
Entrust Certificate Explorer		Provides an interface where users can view and manage both local certificates and personal encryption groups, as well as search the directory. See “Certificate Explorer application” on page 234.
Certificate exchange using email		Aids users to exchange certificates as email attachments.
Entrust PIV Smart card security store		Provides PIN login and key storage for PIV enabled smart cards working with Entrust IdentityGuard.

About configuring multiple searchbases

Security Provider allows you to configure multiple searchbases when you configure your directory. To minimize the load placed on the directory, you should:

- keep the number of searchbases low, bearing in mind that a search may hit the same directory multiple times (once for each searchbase)
- order the searchbases logically so that a search will most likely find its target in the first few searchbases examined

For example, if a organization has a department called "marketing." To configure a logical order for that department, you could have

- the first searchbase look just at marketing,
- the next few searchbases look at other departments with which marketing commonly communicates, organized according to use
- the last searchbase on the list look at the general organization root directory

The overall number of searchbases should be kept to a minimum, since too many searches can greatly increase the time it takes to get results back from a directory.

Working with Entrust IdentityGuard

If you are using PIV smart cards and interworking with Entrust IdentityGuard, the installation wizard gives you the option of adding the IdentityGuard hostname and port when you configure the Security Provider installation package.

To add the IdentityGuard hostname and port

- 1** In the Installation Wizards, Entrust PKI configuration page.
- 2** Click the IdentityGuard tab.
- 3** In the IdentityGuard page, enter the hostname and port to use to contact the IdentityGuard Server. This is the hostname and port associated with IdentityGuard's Self Service Module. See the Entrust IdentityGuard documentation for more information.

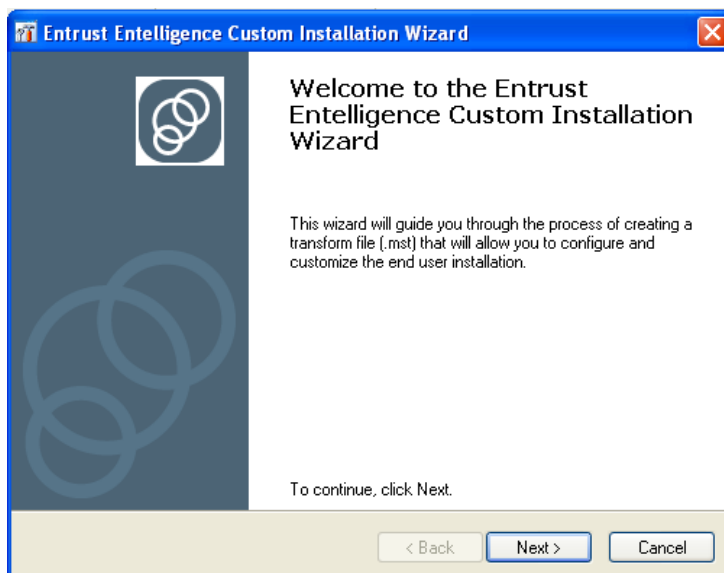
Customizing the installation using the wizard

The following procedure describes how to customize the installer using a wizard.

To customize the installation using the wizard only

- 1** Download and extract the Security Provider for Windows **Custom Installation** wizard from the Entrust TrustedCare Web site. To access the site, use the user name and password provided to you in a customer letter.
- 2** Launch the **Custom Installation** wizard:
 - a** Navigate to the folder where you downloaded the wizard.
 - b** Double-click the `eecustwiz.exe` file.

The **Custom Installation** wizard launches.



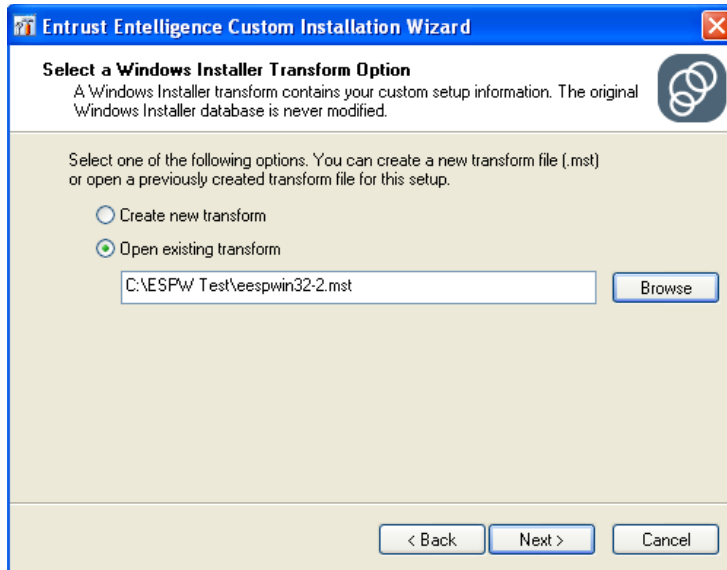
- 3 On the **Welcome** page, click **Next**.

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



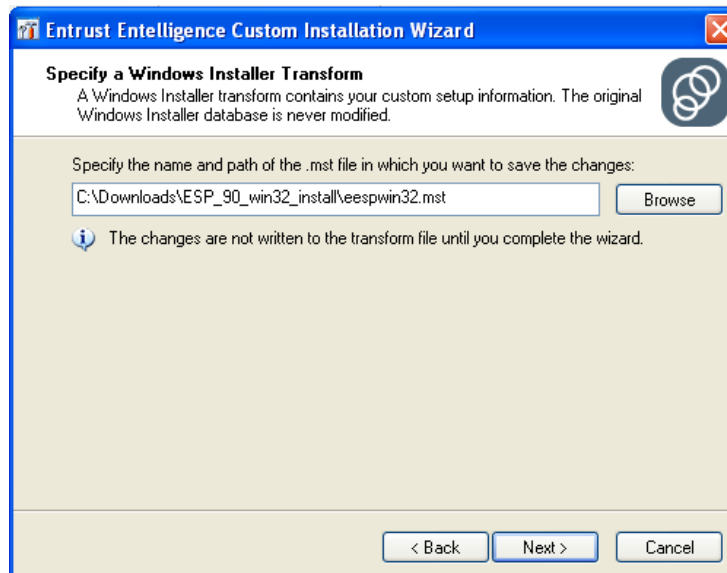
- 4 Browse to the location of the `eespwin32.msi` or `eespwin64.msi` file. Click **Next**.

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

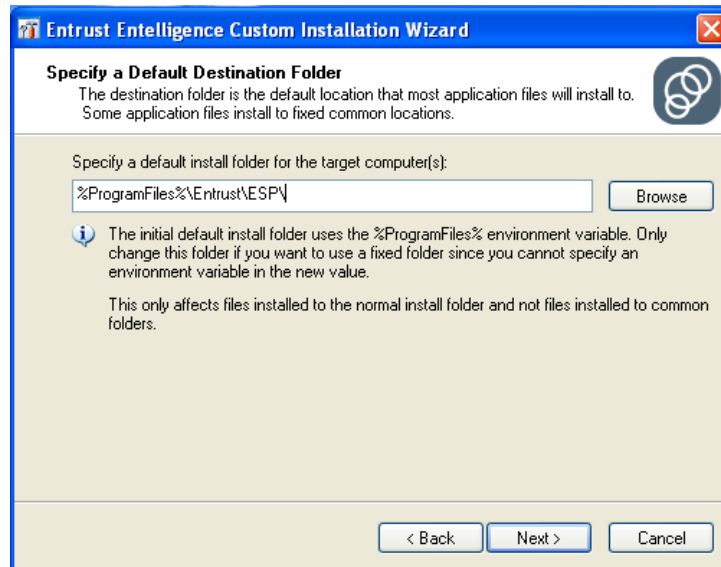


- 5 Do one of the following and then click **Next**:
- If you have not yet run through the **Custom Installation** wizard, click **Create new transform**.
 - If you ran the wizard before, click **Open existing transform** and browse to an existing transform (.mst) file.

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

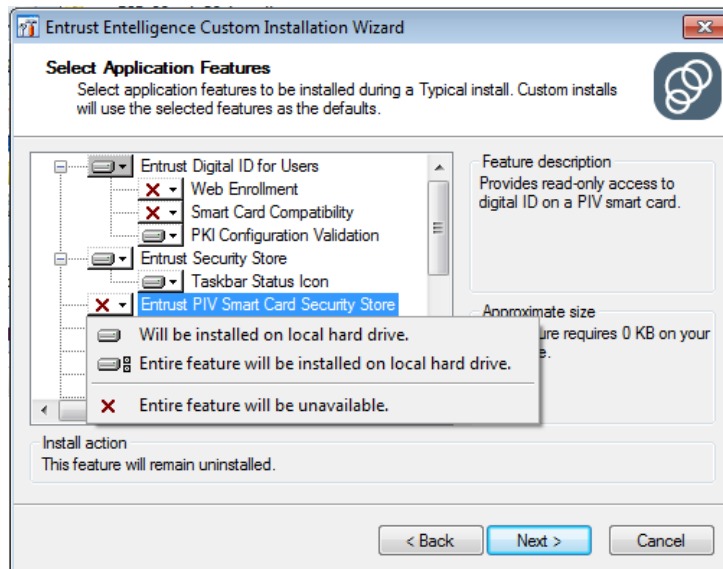


- 6 Confirm the name and path of the transform file. Click **Next**.
The **Select a Default Destination Folder** page appears.



- 7 Specify an installation folder for Security Provider. Users can change this folder during installation unless you specify that they cannot, on a subsequent wizard page. Click **Next**.

The **Select Application Features** page appears.



- 8 Select applicable features to install as part of Security Provider for Windows. For an explanation of each feature, see [“Selecting application features” on page 285](#).
- 9 Fill out all remaining pages of the wizard, hovering your mouse over the input fields and check boxes for help. For detailed information, see [“Security Provider registry settings” on page 327](#).
For settings that relate to registry keys, see [“Security Provider registry settings” on page 327](#).
- 10 Click **Finish** at the end of the wizard.

The wizard creates a transform (.mst file) file containing all your customizations.

The default location of the .mst file is different for different Windows operating systems. Value is different on each OS, because the user's profile folder is in different locations. The path is whatever folder is returned by the operating system for CSIDL_APPDATA with Entrust Security Store appended.

For Windows 7, the default value is:

%APPDATA% (%USERPROFILE%\AppData\Roaming)

For XP, the default value is:

%APPDATA% (%USERPROFILE%\Application Data)

Proceed to [“Packaging the installation” on page 297](#).

Customizing the installation using the wizard and Group Policy

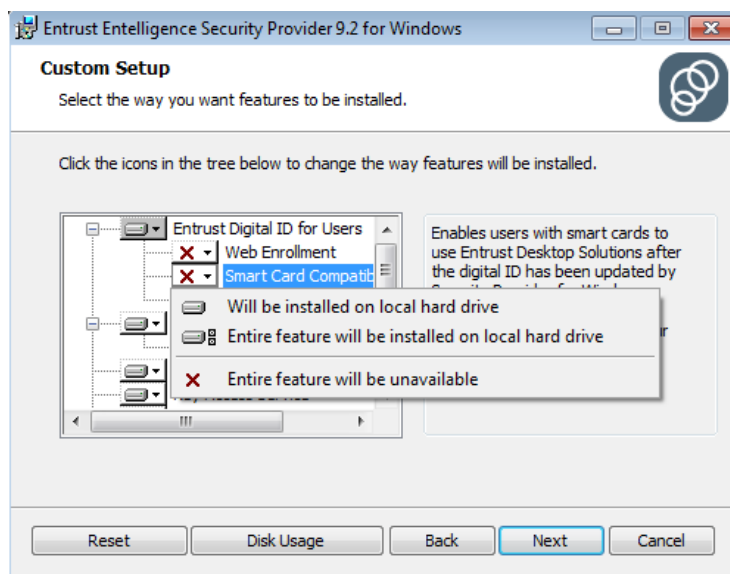
Most Security Provider custom settings can be pushed out to users' Windows registries in bulk through a Microsoft Group Policy application. However, you must make some customizations to the installation itself using the wizard.

The following procedure describes which customizations to make using the wizard, and which customizations to make using Group Policy.

To customize the installation using a wizard and Group Policy

- 1 Download and run the **Custom Installation** wizard following steps 1 through 8 shown under ["To customize the installation using the wizard only" on page 290](#).

After completing steps 1 through 8 you should now have specified a database (.msi file), a transform (.mst) file, and a destination folder. The **Select Application Features** page should now appear with your selections.



- 2 Continue using the wizard to make customizations that can only be made through the wizard, as described in Table 27. You can set and configure all other settings through Group Policy.

Table 27: Installation customizations

On this page of the wizard...	Do this...
Select Application Features	Select the basic features that the installation enables. Figure on page 295 shows a snapshot of some of the features. If you are unsure about what to select, look over "Security Provider features" on page 26 for a general overview of features and links to more detailed information.
Include Additional Certificates	Specify certificates that you want the installation to install. The certificates you specify are copied into the Windows Installer Transform (.mst) file in binary format.
Include Additional Files	Specify files that you want the installation to register in the registry. Some features, such as the CardMS feature, require that a file be added and registered in the registry. Since registering files is impossible through Group Policy, the installation must do it.

- 3 Click **Finish** at the end of the wizard.
The wizard creates a transform (.mst) file containing your customizations.
- 4 Customize the remaining Security Provider settings, and push them out through Group Policy. See ["Security Provider registry settings" on page 327](#) for details about all the settings.

You have now customized the installer and pushed out Security Provider settings through Group Policy. You must now package up the installer and supporting files.

Proceed to ["Packaging the installation" on page 297](#).

Packaging the installation

Before deploying Security Provider, you must package the installation files, namely the .msi, .mst files, and other supporting files. You can package the installation in two ways, as shown in Table 28. Consult the Windows Installer documentation for more ways to create installation packages.

Table 28: Package types

	Type 1: A standard package	Type 2: An administrative package
This package contains...	setup.exe setup.ini .msi .mst	.bat (optional) application files .msi .mst
Creating this package involves...	Modifying a line in a setup.ini file.	Typing a command to run an Administrative Install and then manually creating one .bat file per .mst file.
Distributing this package involves...	Distributing all package contents together.	Distributing the .bat file alone, and making the remaining files available at a network or URL location.
For instructions, see...	“Creating a standard package” on page 298	“Creating an administrative package” on page 299

Creating a standard package

The following instructions describe how to create an installation package containing an .exe file that users can run to launch the Security Provider installer.

To create a standard package

- 1 Open the <Security_Provider_extracted_folder>\setup.ini file in a text editor.

- 2 Specify your transform.mst file, as follows:

- a Locate the following lines at the end of the file:

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

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

- b Remove the semicolon (;) in front of CmdLine=.

- c Change eespwin.mst to the file name of your transform. For example, if you chose the file name "espforwindows1.mst" as your file name, your setup.ini would look like this:

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

```
CmdLine=TRANSFORMS=espforwindows1.mst /i
```

- 3 If you want the installer to run silently—that is, without requiring user input—add the /q parameter noted in bold:

```
CmdLine= TRANSFORMS=espforwindows1.mst /q
```

This parameter is one of many available installation parameters. Type `msiexec` at the command prompt to display a full list of parameters.

- 4 Save the setup.ini file.

You have now created an installation package consisting of a setup.ini file, setup.exe file, .msi file, and .mst file. Before making the package available to users, you must test it. Proceed to [“Testing the installation” on page 303](#).

Creating an administrative package

The following instructions describe how to run an administrative installation and then package it for your users.

Note: Install and patch Security Provider on the machine used to create the administrative package. Some configuration information is only available after you have installed the software on your machine.

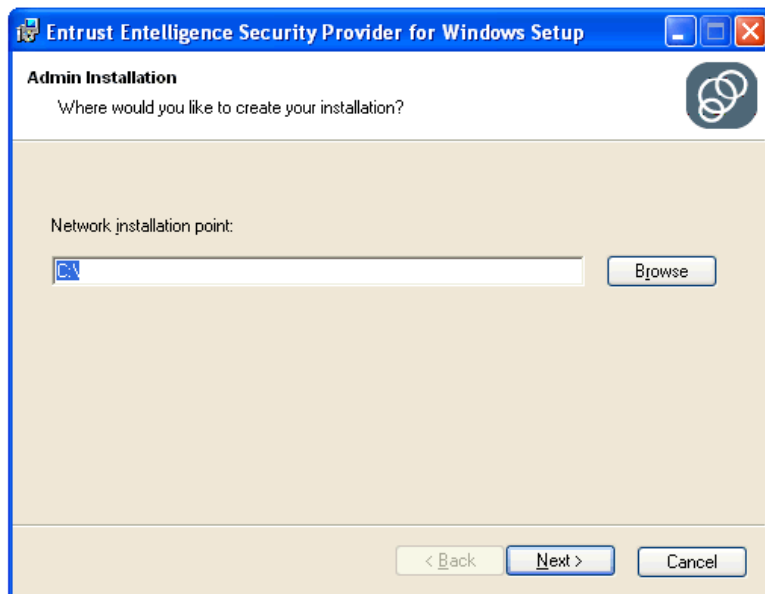
Attention: Additional instructions are required if you are building an administrative install point on IIS 7.x. See the technote [TN 8718 - How do I build and install ESP from an administrative install point on IIS 7.x?](#) for more information.

To create an administrative package

- 1 From a command line, change to the directory containing your installer (.msi) file.
- 2 Run an administrative install by entering the following command:
`msiexec /a <filename>`

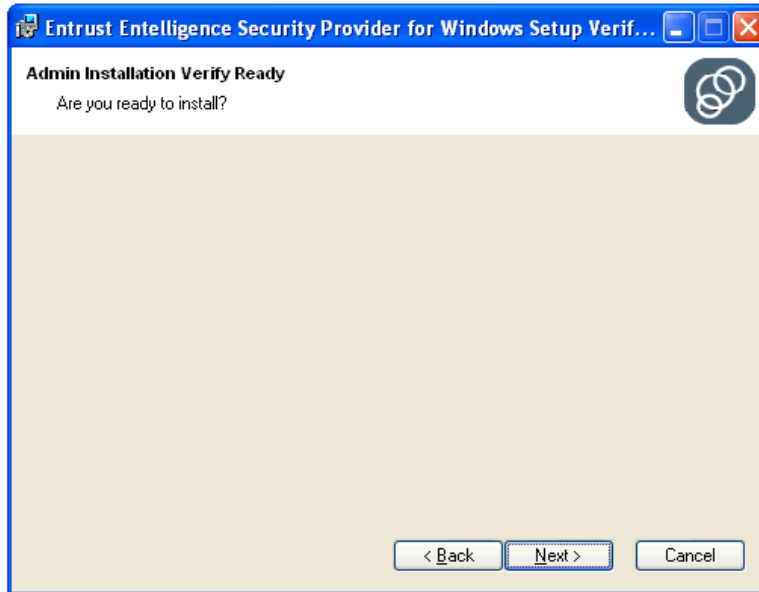
Where <filename> is the name the name of the installer (.msi) file.

The **Admin Installation** dialog box appears.



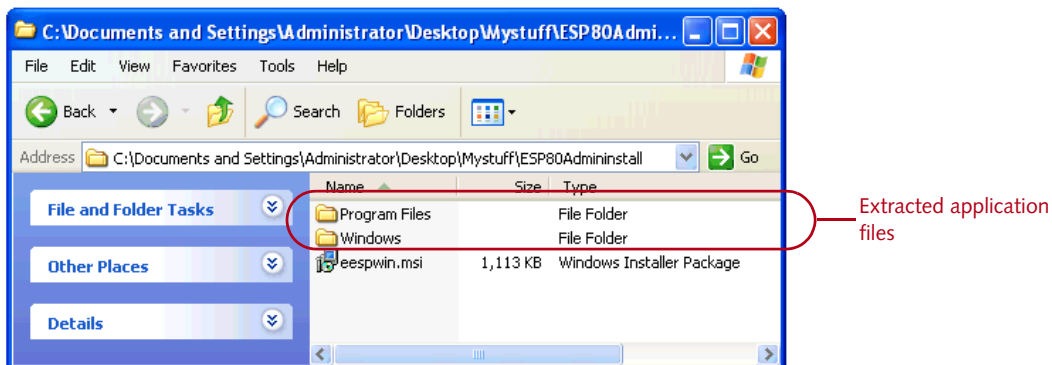
- 3 In the **Network installation point** field, specify a network folder where you want to put the administrative install and then click **Next**.

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



- 4 Click **Next**.

The application files are extracted from the installer (.msi) file. You now have an administrative installation that you can package.



- 5 Copy your .mst files to the administrative install folder.
- 6 If you have not done so already, place the .msi, .mst, and application files at the UNC path or URL that is accessible by your users.

- 7** Create a batch (.bat) file that users can double-click to install Security Provider. The batch file contains a command to run a specified .mst file against the .msi file. To create a batch file:

- a** Open a text editor such as Notepad.
- b** Enter:

```
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\ESP\eespwin32.msi" TRANSFORMS="\\nwksvr\ESP\eespwin.mst"
```

Example of a URL path:

```
msiexec /i "http://websvr/eespwin32.msi" TRANSFORMS="http://websvr/eespwin.mst"
```

Note: Relative paths are not acceptable.

- c** If you want the installation to run silently, add the text in bold:

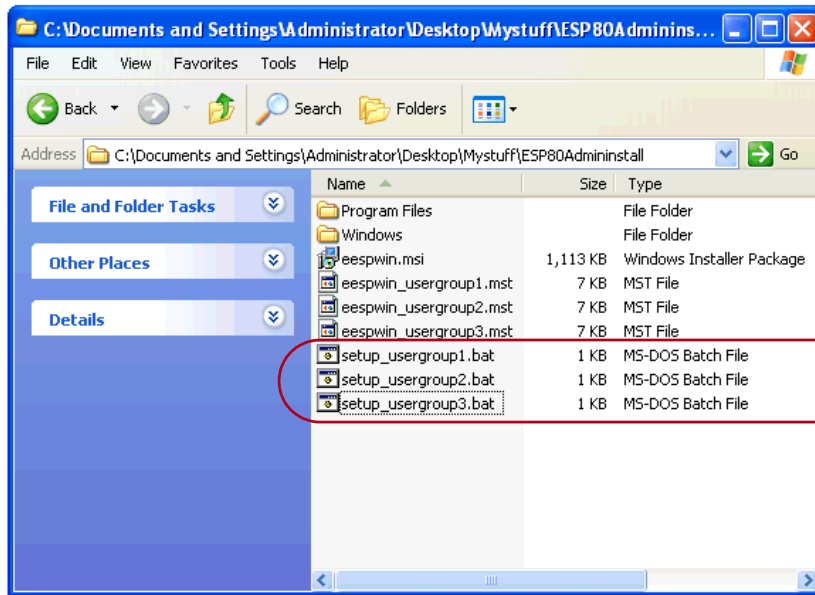
```
msiexec /i <filepath>.msi TRANSFORMS=<filepath>.mst /quiet
```

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

Note: Instead of creating the batch file, have your users manually type in the `msiexec` install command directly.

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

You now have a single administrative install as well as one batch file per .mst file.



You can distribute each .bat file to its respective user group via email, CD, Web site, or third-party distribution tool.

Before distributing the batch file to users, you must test it. Proceed to [“Testing the installation” on page 303](#).

Testing the installation

Entrust recommends that you run the installation package in a test environment before deploying it to your users.

To test the installation package

- 1** If you created a standard package (containing an `.exe` file and supporting files), ensure you removed comment marks from the `setup.ini` file, as described in [Step 2 on page 298](#).
- 2** Install Security Provider by double-clicking the `setup.exe` file (for a standard install package) or the batch file (for an administrative install package).
- 3** If the user account performing the install is different from the one into which Security Provider is installed (for example, a system user installs into a _smith's Windows account), then the Digital ID Monitor and taskbar components are not launched after installation. To launch these components, do one of the following:
 - Restart the computer.
 - Double-click the Digital ID Monitor file (`eecwatch.exe`) and taskbar status icon file (`eesystry.exe`) to start these applications. Both are available in the Security Provider installation folder, by default, under `\Program Files\Common Files\Entrust\ESP\ (32 bit)` or `\Program Files (x86)\Common Files\Entrust\ESP\ (64 bit)`.

For more information about monitoring, see [“Entrust digital ID management” on page 82](#).

For more information about the taskbar status icon, see [“Taskbar status icon” on page 55](#).

- 4** Check whether the features you chose are installed properly by testing them through the Security Provider GUI. If you set up Entrust digital IDs, you must create user entries in Security Manager to test the enrollment and recovery functionality.

See the “Troubleshooting Software Installations” section of the Microsoft Windows Whitepaper *Windows Installer: Benefits and Implementation for System Administrators* for further information.

Distributing the installation package

You can distribute the installation package in different ways, depending on the type of package you created in [“Packaging the installation” on page 297](#).

Table 29: Package types

	Type 1: A standard package	Type 2: An administrative package
This package contains...	setup.exe setup.ini .msi .mst	.bat application files .msi .mst
To distribute this package, do this...	Make all package contents available together (in a .zip file, for example) and then have users copy all files to their computer. Users can run the setup.exe file to install Security Provider.	Distribute the batch file, and then make the remaining files available at a network or URL location. Users can run the batch file to install Security Provider.

Installing Security Provider

Have users install Security Provider according to the instructions below. You may want to provide more detailed instructions to your end users. If you configured the installer properly, users should not have to make any selections during installation.

To install Security Provider

- 1** On the computer where you will be installing Security Provider, ensure you are logged in to Windows as a user with administrative privileges.
- 2** Install Security Provider by double-clicking the `setup.exe` file (for a standard install package) or the batch file (for an administrative install package).
- 3** Reboot, if asked to do so.
- 4** If the user account performing the install is different from the one into which Security Provider is installed (for example, a system user installs into a_smith's Windows account), then the Digital ID Monitor and taskbar components are not launched after installation. To launch these components, do one of the following:
 - Restart the computer.
 - Double-click the Digital ID Monitor file (`eecwatch.exe`) and taskbar status icon file (`eesystry.exe`) to start these services. Both are available in the Security Provider installation folder, by default, under `\Program Files\Common Files\Entrust\ESP\ (32 bit)` or `\Program Files\Common Files\Entrust\ESP\ (64 bit)`.

For more information about monitoring, see [“Entrust digital ID management” on page 82](#).

For more information about the taskbar status icon, see [“Taskbar status icon” on page 55](#).

Upgrading Security Provider

The following instructions describe how to upgrade Security Provider from 9.2 to 9.3. This upgrade is considered a major update in Windows Installer terms.

Attention: A 9.2 transform (.mst) file is not compatible with Security Provider 9.3. You must upgrade your .mst file to 9.3 using the **Custom Installation** wizard.

Note: In some cases, when you upgrade a 9.2 transform file to 9.3 using the **Custom Installation** wizard, you may lose some registry settings made in 9.2 on the **Specify Additional Registry Values** page. This affects modifications to registry settings, such as OverwriteLog, LogLevel, MaxLogSize and similar system settings. The 9.3 **Custom Installation** wizard issues a warning when this occurs.

If you previously installed the Security Provider 9.2 PIV Feature Pack, it is not uninstalled when Security Provider is installed.

To uninstall Security Provider 9.2 and the PIV Feature Pack

- 1 On Windows, select **Start > Control Panel > Add or Remove Programs**.
- 2 Select Entrust Entelligence Security Provider 9.2 PIV Feature Pack from the programs list, and click **Remove**.
- 3 Select Entrust Entelligence Security Provider 9.2 for Windows from the programs list, and click **Remove**.

To upgrade to Security Provider 9.3

- 1 Download the applicable Security Provider 9.3 for Windows installation file from the Entrust TrustedCare Web site at <https://www.entrust.com/trustedcare/>. To access the site, use the user name and password provided to you in a customer letter.

32 and 64-bit versions of the installer are available. Check the latest release or patch notes for supported Windows versions.

Note: The 32-bit version will not install correctly on a 64-bit operating system.

- 2 Download the Security Provider 9.3 for Windows **Custom Installation** wizard from the Entrust TrustedCare Web site at <https://www.entrust.com/trustedcare/>. To access the site, use the user name and password provided to you in a customer letter.

- 3 Extract all the downloaded files.
- 4 Launch the **Custom Installation** wizard as follows:
 - a Navigate to the folder where you extracted the wizard files.
 - b Double-click the `eecustwiz.exe` file.

The **Custom Installation** wizard launches.

For a description of the wizard interface, see [“Customizing the installation using the wizard” on page 290](#).
- 5 For an upgrade, fill out the pages in the wizard as described below.

On this page in the wizard...	Do this...
Specify Windows Installer Database	Select the Security Provider 9.3 installer (.msi) file in <Security_Provider_93_extracted_folder>
Select a Windows Installer Transform Option	Select your Security Provider transform (.mst) file. This can be a new transform file or one created previously for Security Provider 9.2. The wizard upgrades a 9.2 transform (.mst) file to a 9.3 transform (.mst) file. Selecting a transform file populates the remaining pages in the wizard with your configuration requirements.
<i>All remaining pages</i>	Select 9.3 options, as required. Hover your mouse over the input fields and check boxes for information on each. For more detailed information, see “Security Provider registry settings” on page 327 .

- 6 Click **Finish** in the wizard.
- Your transform (.mst) file is upgraded to 9.3.
- 7 Repackage your installation. See [“Packaging the installation” on page 297](#).
- 8 Have users install Security Provider using the new installation package. Users must first manually uninstall the previous version of the product.

Deploying service packs and patches

A Security Provider service pack or patch is contained in a `.msp` file and is considered a small update or minor upgrade in Windows Installer terms.

You can deploy service packs and patches using one of the methods shown in Table 30.

Table 30: Service pack and patch deployment methods

Method...	Use if...	For instructions see...
Distribute the update (<code>.msp</code>) file directly to users	You distributed a <code>setup.exe</code> package directly to users.	“To deploy the service pack or patch file” on page 308
Apply the update to an administrative install	You deployed Security Provider through an administrative install.	“To apply updates to an administrative install” on page 308

To deploy the service pack or patch file

- 1 Ensure you created a `setup.exe` package. For instructions, see [“Creating a standard package” on page 298](#).

Note: The remaining instructions assume that users have previously installed Security Provider using the `setup.exe` file.

- 2 Download and extract the Security Provider 9.3 for Windows patch or service pack. These packages are available from the Entrust TrustedCare Web site at <https://www.entrust.com/trustedcare>. To access the site, use the user name and password provided to you in a customer letter.
- 3 Deploy the `.msp` file to your users through email, on CD, or another method.
- 4 Have users double-click the `.msp` file to install the patch or service pack.

Note: Check the patch *Readme* for changes.

You have now deployed the Security Provider service pack or patch.

To apply updates to an administrative install

- 1 Download and extract the Security Provider 9.3 for Windows patch or service pack. These packages are available from the Entrust TrustedCare Web site at <https://www.entrust.com/trustedcare>. To access the site, use the user name and password provided to you in a customer letter.

- 2 Create a new administrative install and apply the patch at the same time, using this command:

```
msiexec /a <path><filename>.msi /p <path><filename>.msp
```

where:

<filename> is the name of your .msi or .msp files

<path> is the full path to the file and can contain a server and machine name

Examples:

```
msiexec /a eespwin32.msi /p eespwin_91_234765.msp
```

```
msiexec /a \\nwksvr\ESP\eespwin64.msi /p \\nwksvr\ESP\eespwin_91_234765.msp
```

You have now created an administrative install and applied a patch to it. Your .msi file was updated.

- 3 Have users install the patched software by entering the following line at a command-line prompt:

Note: You may place this command in a batch file that you can deploy to users.

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

where <filepath> is replaced with the full path and name of your .mst file and your updated .msi file. The path can be a UNC path or a URL path.

Example of a UNC path:

```
msiexec /i "\\nwksvr\ESP\eespwin32.msi" TRANSFORMS="\\nwksvr\ESP\eespwin.mst" REINSTALL=ALL REINSTALLMODE=vomus
```

Example of a URL path:

```
msiexec /i "http://websvr/eespwin32.msi" TRANSFORMS="http://websvr/eespwin.mst" REINSTALL=ALL REINSTALLMODE=vomus
```

Note: Check the Patch Notes to ensure that this command works with a specific installation.

Deploying language packs

By default, Security Provider for Windows is available in English. If you want a non-English version of the product, you can download a language pack from the Entrust TrustedCare Web site.

A language pack is provided as an .msi file that should be installed after installing Security Provider for Windows. It contains language resources only—no code is included. After the installation, the Security Provider GUI and online help appear in the appropriate language.

Installing Security Provider does not remove existing language packs.

When a new Security Provider version is released, the language pack may not be immediately available. You can use the existing language pack as a temporary solution. Existing text is displayed in the appropriate language. New text is displayed as blank spaces.

Follow the instructions below to deploy a language pack.

Note: If you are installing the language pack on a OS of the same language (for example, you are installing a Japanese language pack on a Japanese OS), all of these steps may not apply.

To deploy a language pack

- 1 Ensure that Security Provider for Windows is installed.
- 2 On the computer where Security Provider is installed, ensure the display language is correct:

Operating system	Instructions
Vista	<ol style="list-style-type: none">1 Click Start > Control Panel.2 Click Clock, Language, and Region (or Regional and Language Options in classic view).3 Click Change display language (or the Keyboards and Languages tab in classic view).4 Under Choose a display language, ensure the appropriate language is selected.5 Click OK.6 Log out and in for any changes to take effect.

Operating system	Instructions
Windows 7	<ol style="list-style-type: none"> 1 Click Start > Control Panel. 2 Click Region and Language (or Regional and Language Options in classic view). 3 Click Keyboards and Languages tab . 4 Click Install/Uninstall languages > Install a display language > Browse computer or network. 5 Either use the Launch Windows Update option or under Select the display languages to install and follow the wizard, ensure the appropriate language is selected. If no options appear or the option you want does not appear browse to location of the Windows Language Interface Pack. See the How can I install additional languages link on the Region and Language page for more information. 6 Log out and in for any changes to take effect.

Note: If the display language configured through the Control Panel does not match the installed language pack, Security Provider displays English.

- 3 Download the applicable language pack from the Entrust TrustedCare Web site at <https://www.entrust.com/trustedcare/>. To access the site, use the user name and password provided to you in a customer letter.
The language pack can be installed on a 32 or 64-bit version of Windows.
- 4 Extract the language pack and double-click the .msi file to install it.
Security Provider for Windows now appears in your chosen language.

Troubleshooting

This section includes troubleshooting information and information about using the Security Provider for Windows log service:

- [“Security Provider for Windows logs” on page 314](#)
- [“Collecting information for customer support” on page 317](#)
- [“Policy certificate messages” on page 318](#)
- [“PKIX-CMP messages” on page 320](#)
- [“Configuring hardened desktop environments” on page 322](#)
- [“Security considerations” on page 323](#)
- [“Displaying version information” on page 324](#)

For problems with roaming servers, see [“Roaming Server problems” on page 175](#).

For problems with smart cards, see [“Troubleshooting smart card problems” on page 186](#).

Security Provider for Windows logs

The log service that is automatically included as part of the installation package allows all Security Provider for Windows features to send log content to a local log service, thereby sharing a single log file and format. The log contents are identified by Security Provider for Windows event identifiers.

Note: Use Microsoft Excel to view the .xml files. Use Internet Explorer to open the logmain.htm file. The XML files may not display well in your browser.

The log service enables all Security Provider for Windows features to send log contents to a local log file. The log service consists of these files:

- logfile.xml is an XML file containing the log file content.
- logfile.xsl is an Extensible Stylesheet Language Transformation (XSLT) file containing the transformations to display the XML file.
- logmain.htm is an HTML file containing the log file contents, displayed and sorted according to the user's settings.
- logopt.htm is an HTML file that enables users to select the options to appear in the logmain.htm file.

The log file contents are identified by Security Provider for Windows event identifiers.

Attention: The local log file and three support files must be located in the same folder. The two HTML files and the XSL files are installed to the location specified in the Windows registry, and the XML file is generated in this location.

Note: If you see an Entrust application failure in a Windows event log file (.evt file), look in the logfile.xml for details.

Setting the logging settings

You can set:

- the log file name and location, level, and size (LogFile, LogLevel, MaxLogSize)
- the log file overwrite behavior (OverwriteLog)
- the number of log file backups (MaxBackupLogFiles)
- a standard set of details about the certificate context, certificate chain context, or CRL context for a user or computer (LogBinaryDetails)

For details about configure these settings, see [“Logging settings” on page 489](#).

Viewing the log file

View the log file by opening the `logmain.htm` file in Internet Explorer, or by double-clicking the file. You can also save the log file by using the **Save As** menu item in Internet Explorer, and refresh the log file either by selecting the refresh icon or by pressing F5.

The date for events logged to the log service is formatted to `mm/dd/yyyy`, and the time is formatted to `hh:mm:ss`.

Note: If you change the log file name from the default name `logfile.xml`, you cannot view the log unless you also change the log file name that is hard-coded in the `logmain.htm` file as well.

Setting the log viewing options

The `logopt.htm` file lets users set the options to appear in the `logmain.htm` file. Access the `logopt.htm` file by opening the `logmain.htm` file in a browser. It contains a link to the `logopt.htm` file.

Users can set the following options in the `logopt.htm` file:

- the log level
- whether the date appears
- whether the time appears
- whether the Security Provider for Windows feature name appears
- whether the process name appears
- whether the process ID appears
- whether the thread ID appears
- whether the session ID appears
- whether the event ID appears
- whether the log message appears

You can also:

- filter by Security Provider for Windows features
- set the starting and ending time and date
- set the order of display (first to last, or last to first)

Security Provider for Windows log file location

By default, the log file is located in the `\Program Files\Common Files\Entrust\ESP\Logging` folder (32 bit systems) or `\Program Files`

(x86)\Common Files\Entrust\ESP\Logging folder (64 bit systems). Users can send you the logfile.xml file, which contains the log file contents.

Windows installer logging

Windows Installer has a built-in logging mechanism that can help identify any installation issues that may occur during the setup. You can activate logging through the command-line option, registry key configuration, or other methods specified in Microsoft documentation. For further details on Microsoft Windows Installer logging, see the white papers entitled *Windows Installer Service Overview* and *Windows Installer: Benefits and Implementation for System Administrators*, published by Microsoft.

Error messages

For a complete list of Security Provider for Windows errors that appear in dialog boxes, see the *Entrust Entelligence Security Provider for Windows Error Message Guide*. This guide lists possible causes and solutions for these errors.

Collecting information for customer support

If you are unable to troubleshoot a problem yourself, you can contact Entrust customer support. To provide you with the fastest service, it is recommended that you include system information and log files with your trouble ticket. This information can be collected and dumped to a ZIP file using the customer support utility included with Security Provider. See [“Customer support utility” on page 248](#).

Policy certificate messages

You can choose to create a dump file for different types of policy certificates used during enrollment, recovery, and certificate management, as well as messages:

- main policy (referred to as CA Policy)
- role policy (also referred to as client settings policy or user policy)
- certificate definition policy
- auto-enrollment, CardMS and OCSP messages

Certificate management dump files

The certificate management component dumps all available policy certificates for the Entrust digital ID that it is managing. It creates a subfolder within the folder specified in the `PolicyCertDumpLocation` registry value. This subfolder is created for the certificate management files. The folder name will be the Entrust digital ID's distinguished name. Within this subfolder, each policy certificate is dumped into a separate file with its corresponding file name:

- `Main_policy.der`
- `Role_policy.der`
- `Cert_Defn_policy.der`

Enrollment and recovery policy

The enrollment, update, and recover component dumps all available policy certificates that pertain to the Entrust digital ID being created or recovered. All three types of policy (main, role, and certificate definition) are always dumped during an enrollment or recovery.

A subfolder is created within the folder specified in the `PolicyCertDumpLocation` registry value. The name of the enrollment or recovery folder is `Enroll<reference_number>` or `Recover<reference_number>`, where the reference number is the one used to enroll or recover. Within this subfolder, each policy certificate is dumped into a separate file with its corresponding file name:

- `Main_policy.der`
- `Role_policy.der`
- `Cert_Defn_policy.der`

Reading policy certificate dump files

All policy certificate dump files are DER-encoded. You must decode the `.der` files with a DER decoder, to read these files.

Note: A DER decoder is not packaged with the Security Provider for Windows software.

Setting the policy certificate dump location

You can choose to create a dump file for all policy certificate messages. See the `PolicyCertDumpLocation` registry setting in the section [“Logging settings” on page 489](#) for further information about creating a dump file location for all policy certificate messages.

Auto-enrollment, CardMS, and OCSP message dump files

You can create dump files for auto-enrollment, CardMS and OCSP messages using the `AutoEnrollMessageDumpLocation`, `CardMSUpdaterMessageDumpLocation`, and `OCSPDumpLocation` settings. For details about these settings, see [“Logging settings” on page 489](#).

PKIX-CMP messages

Security Provider for Windows communicates with Security Manager by sending and receiving DER-encoded messages. These messages are in PKIX-CMP format. A PKIX-CMP message is either a request sent to the CA or a response received from the CA.

The lists below give the PKIX-CMP message name and the file name used when this message is saved in the PKIX-CMP dump file:

The following requests and responses are created or received during an enrollment:

- ask for policy - `cmp_genm_policy.der`
- receive policy - `cmp_genp_policy.der`
- ask for CA protocol encryption certificate - `cmp_genm_prot_enc.der`
- receive CA protocol encryption certificate - `cmp_genp_prot_enc.der`
- enrollment request - `cmp_enroll_request.der`
- enrollment response - `cmp_enroll_response.der`
- confirmation - `cmp_conf.der`

The following requests and responses are created or received during recovery:

- ask for policy - `cmp_genm_policy.der`
- receive policy - `cmp_genp_policy.der`
- ask for CA protocol encryption certificate - `cmp_genm_prot_enc.der`
- receive CA protocol encryption certificate - `cmp_genp_prot_enc.der`
- recovery request - `cmp_recovery_request.der`
- recovery response - `cmp_recovery_response.der`
- confirmation - `cmp_conf.der`

The following requests and responses are created or received during a key update:

- ask for information from Event Server - `cmp_genm_event_svr.der`
- receive information from Event Server - `cmp_genp_event_svr.der`
- ask for policy - `cmp_genm_policy.der`
- receive policy - `cmp_genp_policy.der`
- ask for CA protocol encryption certificate - `cmp_genm_prot_enc.der`
- receive CA protocol encryption certificate - `cmp_genp_prot_enc.der`
- update request - `cmp_update_request.der`
- update response - `cmp_update_response.der`
- confirmation - `cmp_conf.der`

Key update dump files

The certificate management component dumps all available information into a subfolder. The subfolder is created within the folder specified in the `PKIXCMPDumpLocation` registry value. This subfolder is created for the key update files and the folder name is the Entrust digital ID's distinguished name. The one exception to this is the event server messages (`cmp_genm_event_svr.der` and `cmp_genp_event_svr.der`). When these messages are sent or received, only the CA DN is known. Therefore, the subfolder name will be the CA's distinguished name.

Enrollment and recovery dump files

The enrollment or recovery component dumps all available information that pertains to the Entrust digital ID that is being created or recovered. A subfolder is created within the folder specified in the `PKIXCMPDumpLocation` registry value. The name of the enrollment or recovery folder is `Enroll<reference_number>` or `Recover<reference_number>`, where the reference number is the one used to enroll or recover. Within the subfolder, each of the `.der` file names listed is dumped into a separate file. If a file by the same name already exists in the subfolder, Security Provider for Windows overwrites that file with the new one.

Reading PKIX-CMP dump files

All PKIX-CMP dump files are DER-encoded. You must decode the `.der` files with a DER decoder, to read these files.

Note: The Security Provider for Windows software package does not include a DER decoder.

Setting the PKIX-CMP dump location

You can choose to create a dump file for all PKIX-CMP messages. See the `PKIXCMPDumpLocation` registry setting in [Table 61 on page 489](#).

Configuring hardened desktop environments

Security hardened desktop environments are usually part of an organization's security policy. When configuring a hardened desktop environment for your end users, ensure they have the following permissions to enable them to use the Security Provider for Windows software.

Permissions	Location
Read and Write	HKEY_CURRENT_USER\Software\Entrust\ESP\
Read	HKEY_LOCAL_MACHINE\Software\Entrust\ESP\ (32 bit systems) OR HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Entrust\ESP (64 bit systems)
Read	C:\Program Files\Common Files\Entrust\ESP\ (32 bit systems) OR C:\Program Files (x86)\Common Files\Entrust\ESP (64 bit systems)
Read	C:\Program Files\Entrust\ESP\ (or wherever you installed Security Provider)

In addition:

- Full administrative permissions are required by the account installing the Security Provider software.
- The Security Provider for Windows log service needs Write permission to the log file folder.
- Security Provider for Windows services (such as the Computer Digital ID Service) need Read and Write permissions to the HKEY_LOCAL_MACHINE\Software\Entrust\ESP\ (32 bit systems) or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Entrust\ESP (64bit systems) registry subtree.

Security considerations

This section provides some general security guidelines for administrators and users.

Securing your environment

Despite precautions against software attacks from viruses or Trojan horses, applications can be affected by malicious software on most operating systems. Therefore, it is important to make your users aware of this possible danger, warning them against intentionally or unintentionally installing and executing potentially malicious software.

Securing your password

General password security management rules include:

- Do not share your password with anyone.
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.
- Do not cut and paste, or copy and paste security-critical information (such as a password), because this information is stored in memory. This causes a potential security risk. Alternatively, when passwords are typed in (not copied and pasted) they are erased from memory.

Evaluating your cryptographic security

Over time, cryptographic algorithms become less secure as computing capacity becomes less expensive. Therefore, it is important to re-evaluate and update the cryptographic algorithms you are using. When choosing cryptographic algorithms, consider the time period you want your information to remain protected if it is captured and stored by an attacker waiting for mechanisms to decrypt it.

For a list of algorithms and keys currently supported by Security Provider, see the section [“Entrust Cryptographic Service Providers” on page 129](#).

Also see algorithm settings and registry entries under [“Entrust File Security settings” on page 430](#).

Displaying version information

Use one of the following methods to determine the version of Security Provider:

- [“To locate the version from the login dialog box” on page 324](#)
- [“To locate the version using a version .dll file \(Windows XP\)” on page 324](#)

To locate the version from the login dialog box

- 1 Right-click the taskbar status icon and select **Log In**.
- 2 Click the icon in the upper left shown in Figure 25.

Figure 25: Login dialog box

Click to display
the menu.



- 3 In the menu, select **About Entrust**. The **About Entrust Intelligence Security Provider** dialog box appears.
- 4 Locate the **Build** section for version information.

To locate the version using a version .dll file (Windows XP)

- 1 On the end-user machine, locate the `eeveresn.dll` file. The default location is:
`C:\Program Files\Common Files\Entrust\ESP\`
- 2 Right-click the file and select **Properties**.
- 3 Click the **Version** tab.
- 4 Select the **Product version** in the **Item name** box.

The information in the **Value** box on the left displays the installed version of Security Provider for Windows.

To locate the version using a version .dll file (Windows 7 and above)

- 1** On the end-user machine, locate the `eeversn.dll` file. The default location is:
`C:\Program Files (x86)\Common Files\Entrust\ESP\`
- 2** Right-click the file and select **Properties**.
- 3** Click the **Details** tab.

Security Provider registry settings

This appendix contains a set of tables that describe the Security Provider for Windows registry settings, show you where in the registry each setting belongs, and where to configure each setting in the **Custom Installation** wizard, if the setting is available through the wizard. For information on using the wizard, see [“Customizing the installation using the wizard” on page 290](#).

Settings are grouped into the following categories:

- [“Directory settings” on page 331](#)
- [“PKI settings” on page 347](#)
- [“Entrust digital ID settings” on page 373](#)
- [“Entrust security store settings” on page 396](#)
- [“CRL Revocation Provider settings” on page 419](#)
- [“OCSP Revocation Provider settings” on page 425](#)
- [“Entrust File Security settings” on page 430](#)
- [“Timestamp server settings” on page 445](#)
- [“Password Encrypt settings” on page 451](#)
- [“TrueDelete settings” on page 455](#)
- [“Entrust Certificate Explorer settings” on page 463](#)
- [“Entrust Ready identity device setting” on page 469](#)
- [“Certificate path discovery, validation, download, and extensions settings” on page 470](#)
- [“HTTP connection and timeout settings” on page 476](#)

- “GUI customization settings” on page 478
- “Miscellaneous settings” on page 484
- “Logging settings” on page 489
- “Entrust email certificate exchange settings” on page 495

What is the ESP registry location?

The <ESP_registry_location> variable used throughout this appendix maps to one of the locations shown in the middle column of Table 31. Logging registry settings (see [“Logging settings” on page 489](#)) should always be configured under the system account, never under the local user account.

Table 31: ESP registry key locations

If you configure a setting through...	Then the setting is placed here in users' registries....	By...
Group Policy and specify that the setting should apply only to the current user	HKEY_CURRENT_USER\ Software\Policies\Entrust\ESP	the Group Policy application
Group Policy and specify that the setting should apply to all users of the machine	On a 32-bit operating system: HKEY_LOCAL_MACHINE\ Software\Policies\Entrust\ESP On a 64-bit operating system: HKEY_LOCAL_MACHINE\ Software\WOW6432Node\Policies\Entrust\ESP	the Group Policy application
the Specify Additional Registry Values page of the Custom Installation wizard	On a 32-bit operating system: HKEY_LOCAL_MACHINE\ Software\Entrust\ESP On a 64-bit operating system: HKEY_LOCAL_MACHINE\ Software\WOW6432Node\Entrust\ESP	the Security Provider installer
the Specify Additional Registry Values page of the Custom Installation wizard	HKEY_CURRENT_USER\ Software\Entrust\ESP	the Security Provider installer

Note: If you uninstall Security Provider for Windows, any registry settings that you customize or add for Security Provider are not removed.

Registry settings are read in the precedence shown in Table 31. For example, if the Proxy setting appears under HKEY_LOCAL_MACHINE\Software\Policies\Entrust\ESP and HKEY_LOCAL_MACHINE\Software\Entrust\ESP, the setting under

HKEY_LOCAL_MACHINE\Software\Policies\Entrust\ESP is the one that Security Provider reads.

Directory settings

You must configure a directory if you want to use:

- Entrust digital ID features, including Entrust digital ID enrollment, recovery, management, automatic additional certificate download
- the Certificate Explorer's search functionality
- the File Security feature
- the Certificate Path Discovery feature
- the CRL Revocation Provider feature
- integration with a CardMS

For an overview of these features, see ["Security Provider features" on page 26](#).

Directory settings include:

- ["Directory connection settings" on page 332](#)
- ["Directory search settings" on page 340](#)
- ["Default directory setting" on page 344](#)

Note: A directory setting that is specific to your Security Manager installation is available. See ["CA-specific directory setting" on page 352](#) for details.

Directory connection settings

If you use the **Custom Installation** wizard, most directory connection settings are configurable through the **Directory Connection** tab (Figure 26). To navigate to this tab, click **Add** on the **Specify Directory Information** page.

Table 32 describes the directory connection settings. Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 26: Directory Connection tab

The screenshot shows the 'Directory Configuration' wizard with the 'Directory Connection' tab selected. The 'Server information' section contains the following fields and controls:

- Friendly name:** A text input field.
- Type:** Radio buttons for 'Active Directory' and 'LDAP'. 'LDAP' is selected.
- Host Name or IP Address / Port:** A table with two columns. The 'Host Name or IP Address' column is empty. The 'Port' column is empty. To the right of the table are buttons: 'Add...', 'Edit...', and 'Remove'.
- Communication protocol:** A dropdown menu showing 'LDAPv3'.
- Connection time limit (in seconds):** A text input field containing the value '5'.
- Authentication method:** A dropdown menu showing 'Auto-select'.

At the bottom of the wizard are 'OK' and 'Cancel' buttons. In the background, another window titled 'on Wizard' is partially visible, showing a list of items and buttons: 'Add...', 'Edit...', 'Remove', 'Import...', 'Default', 'Next >', and 'Cancel'.

Table 32: Directory connection settings

Setting name and location in Custom Installation wizard	Description and value name
<p>Specify Directory Information page ></p> <p>Add ></p> <p>Directory Connection tab ></p> <p>Friendly Name</p>	<p>Gives the friendly name of a directory. The directory can be any LDAP directory, including Active Directory. This setting is mandatory and maps to a registry key and a registry value. For example, if you set the Friendly Name setting through the Custom installation wizard to MyDir, two things happen:</p> <ul style="list-style-type: none">• A registry key called <ESP_registry_location>\Directory\MyDir is created• A registry entry called Name is created under <ESP_registry_location>\Directory\MyDir. The value of Name is MyDir. <p>If you want to specify this setting by hand or through Group Policy, you must create a registry key with your directory's friendly name under <ESP_registry_location>\Directory\, and then, under this key, add a registry value of Name=<Your_Directory_friendly_name>.</p> <p>The name registry entry is described below:</p> <p>Key: <ESP_registry_location>\Directory\ <Directory_friendly_name></p> <p>Value Name: Name</p> <p>Value Type: REG_SZ</p> <p>Value Data: <Directory_friendly_name></p> <p>Example:</p> <p>Value Data: MyDir</p>

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
Specify Directory Information page > Add > Directory Connection tab > Add > Host Name or IP Address Port	<p>Specifies the host (server) name or IP address and port of your directory. This setting is mandatory if the directory is not Active Directory. If you want to use Active Directory, see instead the <code>ActiveDirectory</code> setting in the next row of this table.</p> <p>If you are using Kerberos authentication, you must use the host (server) name. Do not use an IP address.</p> <p>The host name or IP address and port settings map to the following registry value:</p> <p>Key: <code><ESP_registry_location>\Directory\ <Directory_friendly_name></code></p> <p>Value Name: <code>Directory</code></p> <p>Value Type: <code>REG_SZ</code></p> <p>Value Data: <code><server:port></code></p> <p>Example:</p> <p>Value Data: <code>test_dc:389</code></p> <p>If you are using multiple values, enter one space between each <code>server:port</code>.</p> <p>Example: <code>server:port server2:port2</code></p>

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
Specify Directory Information page > Add > Directory Connection tab > Active Directory	<p>Designates a directory as an Active Directory. This setting is recommended if you use Active Directory. Only one Active Directory can exist per Security Provider deployment.</p> <p>When you designate a directory as Active Directory, Security Provider:</p> <ul style="list-style-type: none">• Finds the address and port of the closest Active Directory automatically at runtime. This information is cached in the Directory registry value (described in the preceding table row) under the <code>HKEY_CURRENT_USER\</code> root key.• Finds attributes listed in Active Directory's Global Catalog, and caches them on users' computers. Caching of Global Catalog attributes makes searches faster because Security Provider can search the Global Catalog if it contains the search attributes. <p>The discovery process occurs when the Digital ID Monitor starts for the first time, and every seven days thereafter, by default. The Active Directory setting maps to the following registry value:</p> <p>Key: <code><ESP_registry_location>\Directory\ <Directory_friendly_name></code> Value Name: <code>ActiveDirectory</code> Value Type: <code>REG_DWORD</code> Value Data: <code><0-1></code></p> <p>0 (default) = Directory is a not an Active Directory. 1 = Directory is an Active Directory.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting is used only if you designated your directory as an Active Directory. (See the preceding table row.) This setting is optional.</p> <p>Sets the interval to wait (in days) before Security Provider's Digital ID Monitor tries to discover new host name and port information for Active Directory, as well as new Active Directory Global Catalog attributes.</p> <p>This setting maps to the following registry value:</p> <p>Key: <code><ESP_registry_location>\Directory\ <Directory_friendly_name></code> Value Name: <code>ADDISCOVERYINTERVAL</code> Value Type: <code>REG_DWORD</code> Value Data: <code><1-n_days></code></p> <p>The default is 7 days.</p>

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
Specify Directory Information page > Add > Directory Connection tab > Communication protocol	<p>Specifies the LDAP version of your directory. LDAP version 3 (LDAPV3) is the default. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Directory\ <Directory_friendly_name> Value Name: LDAPVersion Value Type: REG_SZ Value Data: <LDAP_Version></p> <p>Example:</p> <p>Value Data: LDAPV2</p>
Specify Directory Information page > Add > Directory Connection tab > Connection time limit (in seconds)	<p>Limits how long to wait (in seconds) while connecting to a directory. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Directory\ <Directory_friendly_name> Value Name: DirectoryConnectTimeLimit Value Type: REG_DWORD Value Data: <time_in_seconds></p> <p>Example:</p> <p>Value Data: 5</p> <p>The default is 5 seconds.</p>

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
Specify Directory Information page > Add > Directory Connection tab > Authentication Method	<p>Forces Security Provider for Windows to authenticate to the directory. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Directory\ <Directory_friendly_name> Value Name: AuthenticationMethod Value Type: REG_DWORD Value Data: <0-4></p> <p>Example:</p> <p>Value Data: 3</p> <ul style="list-style-type: none">- 0 (default) = Auto-select. This method tries Kerberos/NTLM authentication, and if that fails, it tries Anonymous authentication.- 1 = Anonymous authentication. This method works in environments with or without firewalls. <p>Attention: Do not use Anonymous authentication if you are using Active Directory.</p> <ul style="list-style-type: none">- 2 = NTLM. This method does not support firewalls.- 3 = Kerberos/NTLM. This method does not support firewalls.

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
Specify Directory Information page > Add > Directory Connection tab > Proxy Server section > Host Name or IP Address Port Number	<p>Use this setting if you want Security Provider for Windows to connect to the directory through the Entrust Authority Security Manager Proxy.</p> <p>Provides the host (server) name or IP address plus the IP port of your proxy servers. If no port is specified, port 80 is assumed for HTTP, and port 443 for HTTPS. See the next table row for more information on HTTP and HTTPS.</p> <p>When multiple proxy servers are specified, Security Provider attempts to connect to them in the order they are listed, until it a successful connection is established. See also the Proxy Order setting on page 339.</p> <p>Note: If you set the Proxy setting to use non-standard ports (standard ports being 80 and 443), you must set certain parameters. See “To configure Security Manager Proxy for use with Security Provider” on page 178.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Directory\<Directory_friendly_name> Value Name: Proxy Value Type: REG_SZ Value Data: <proxyserver1:httpport:httpsport>;<proxyserver2:httpport:httpsport></p> <p>Examples:</p> <p>Value Data: proxyserver1;proxyserver2 (use this syntax if you are using default HTTP and/or HTTPS ports, which are 80 and 443, respectively)</p> <p>Value Data: proxyserver1:81;proxyserver2:81 (use this syntax if you are using HTTP with non-default ports)</p> <p>Value Data: proxyserver1:81:444;proxyserver2:81:444 (Use this syntax if you are using HTTPS with non-default ports. Both HTTPS and HTTP ports must be specified because CRLs can only ever be retrieved over HTTP.)</p> <p>You can also configure connection timeout setting for the proxy server. See “HTTP connection and timeout settings” on page 476 for details.</p>

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Determines whether the connection to Security Manager Proxy is over HTTP or HTTPS. This setting maps to the following registry value: Key: <ESP_registry_location>\Directory\<Directory_friendly_name> Value Name: ProxyForceHttps Value Type: REG_DWORD Value Data: <0_or_1> 0 (default) = Use HTTP 1 = Use HTTPS Note: For HTTPS to work, you must set certain parameters on Security Manager Proxy. For details, see "To configure Security Manager Proxy for use with Security Provider" on page 178.
Specify Directory Information page > Add > Directory Connection tab > Proxy Order	Determines whether Security Manager Proxy Server or the directory is contacted first. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location>\Directory\<Directory_friendly_name> Value Name: ProxyOrder Value Type: REG_DWORD Value Data: <1-4> 1 = Proxy, Direct. A connection to the proxy servers is attempted first. If no connection to any of the proxy servers can be established, a direct connection to the directory is attempted. 2 (default) = Direct, Proxy. A connection to the directory is attempted first. If that fails, a connection to the proxy servers is attempted. 3 = Direct only. A connection to the directory is attempted. If that fails, connections to other components are not attempted. 4 = Proxy only. A connection to the proxy servers is attempted. If no connection to any of the proxy servers can be established, a connection to the directory is not attempted.

Table 32: Directory connection settings (continued)

Setting name and location in Custom Installation wizard	Description and value name
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting lets you rearrange how the friendly name appears when viewing certificate properties. By default, the user's name appears first. A very long user name can cause truncation of other information. In this case, you can have the user name appear in a different position.</p> <p>The setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: CertPropFriendlyNameFormat Value Type: REG_SZ Value Data: string</p> <p>The default is: "%1!s! %2!s! Certificate"</p> <p>For example, to place the user name last, enter:</p> <p>Value Data: "%2!s! certificate for %1!s!"</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>In some environments, an LDAP bind may incur unneeded overhead during authentication. In such cases, you can specify to try the anonymous method first.</p> <p>Use this key to set the priority on the binding method. In any case, if the first method fails, a second method is used.</p> <p>When this is set to 1, you will see this DETAILED LEVEL message in the logs: "Authenticating a client to a server using anonymous method."</p> <p>If this binding method fails, you will see a DETAILED LEVEL message like this in the logs: "Authenticating a client to a server using either Kerberos v5 or NTLM method."</p> <p>Key: <ESP_registry_location> Value Name: LDAPBindAnonymousFirst Value Type: REG_DWORD Value Data: <0_or_1></p> <p>0 (default) = do not try the anonymous method first 1 = try the anonymous method first</p>

Directory search settings

If you use the **Custom Installation** wizard, all directory search settings are configurable through the **Directory Search** tab (Figure 27). To navigate to this tab, click **Add** on the **Specify Directory Information** page.

Table 33 describes the directory search settings. Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 27: Directory Search tab

The screenshot shows a window titled "Directory Configuration" with three tabs: "Directory Connection", "Directory Search" (which is selected), and "Proxy Server". The "Directory Search" tab contains a "Search base" section with a table and several buttons. The table has two columns: "Friendly Name" and "Search Base". To the right of the table are buttons for "Add...", "Edit...", "Remove", "Up", and "Down". Below the table, there are two text input fields. The first is labeled "Maximum number of entries to return from a Directory search:" and contains the value "50". The second is labeled "Time limit (in seconds) for the Directory to spend on a search:" and contains the value "30". At the bottom right of the window are "OK" and "Cancel" buttons.

Friendly Name	Search Base
---------------	-------------

Maximum number of entries to return from a Directory search:
50

Time limit (in seconds) for the Directory to spend on a search:
30

Table 33: Directory searchbase settings

Setting name and location in Custom Installation wizard	Description and Value Name
Specify Directory Information page > Add > Directory Search tab > Add > Search Base	Sets a searchbase to use. You must specify a searchbase if you use the File Security and Certificate Explorer applications bundled with Security Provider. For details on these applications, see “Bundled applications” on page 201 . This setting maps to the following registry key: Key: <ESP_registry_location>\Directory\ <Directory_friendly_name>\<Searchbase>
Specify Directory Information page > Add > Directory Search tab > Add > Friendly Name	Sets the friendly name of your searchbase. If you do not specify a friendly name, the default value is the searchbase. A friendly name must be configured for each searchbase, if you plan to configure the SearchBaseOrder setting. This setting maps to the following registry value: Key: <ESP_registry_location>\Directory\ <Directory_friendly_name>\<Searchbase> Value Name: Name Value Type: REG_SZ Value Data: <Searchbase_friendly_name> Example: Value Data: My Searchbase
Specify Directory Information page > Add > Directory Search tab > Up/Down buttons	Provides a series of one or more searchbase names, which match the configured <Searchbase>, separated by semicolons. Security Provider searches each searchbase in the order specified. The SearchBaseOrder setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location>\Directory\ <Directory_friendly_name> Value Name: SearchBaseOrder Value Type: REG_SZ Value Data: <SearchBase1 Name>;<SearchBase2 Name>

Table 33: Directory searchbase settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Specify Directory Information page > Add > Directory Search tab > Maximum number of entries to return from a Directory search	Limits the number of entries to return from a directory search. This setting is optional. If the directory is Active Directory and you use its Global Catalog, ensure that this limit is higher than the number of attributes in your Global Catalog. For details on the Global Catalog, see the Active Directory setting described in "Directory connection settings" on page 332 . This setting maps to the following registry value: Key: <ESP_registry_location>\Directory\ <Directory_friendly_name> Value Name: DirectoryOperationSizeLimit Value Type: REG_DWORD Example: Value Data: 50 The default is 50.
Specify Directory Information page > Add > Directory Search tab > Time limit (in seconds) for the Directory to spend on a search	Limits how long (in seconds) to search for entries in the directory. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location>\Directory\ <Directory_friendly_name> Value Name: DirectoryOperationTimeLimit Value Type: REG_DWORD Value Data: <limit_in_seconds> Example: Value Data: 5 The default is 5 seconds.

Table 33: Directory searchbase settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
	<p>Delays can occur when Security Provider looks for certain Certification Authority (CA) certificates during certificate path discovery. If the search is causing delays, use the IgnoreDNsForCAsSearch setting to specify a semicolon (;) separated list of CA distinguished names (DN) for Security Provider to ignore when searching for certificates. Security Provider does not search for CA certificates that correspond to a CA DN in the list.</p> <p>Key: <HKLM or HKCU>\Software\Entrust\ESP or, if using Group Policy: <HKLM or HKCU>\Software\Policies\Entrust\ESP</p> <p>Value Name: IgnoreDNsForCAsSearch Value Type: REG_SZ Value Data: A semicolon (;) separated list of CA DNs to ignore.</p> <p>Example: Value Data: CN=Department1, O=Company, C=CA;CN=Department2,O=Company,C=US</p>

Default directory setting

If you use the **Custom Installation** wizard, the default directory setting is configurable on the **Specify Directory Information** page (Figure 28).

Table 34 describes the default directory setting. The table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 28: Specify Directory Information page

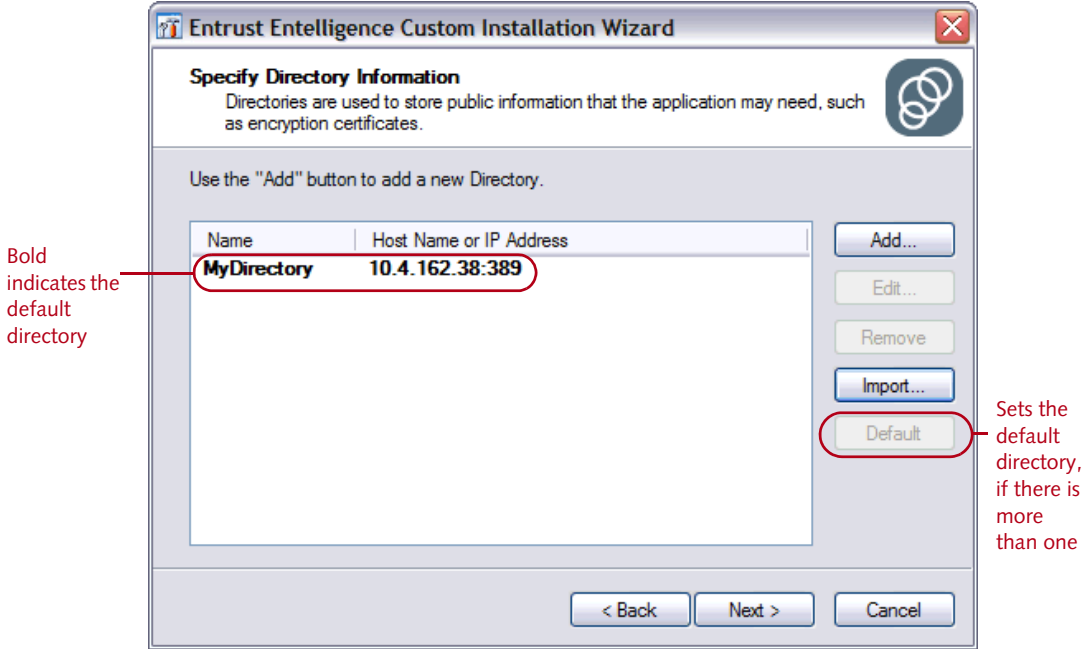


Table 34: Default directory setting

Setting name and location in Custom Installation wizard	Description and Value Name
Specify Directory Information page > Default button	<p>Specifies the default directory. The Certificate Path Discovery feature searches the default directory to find intermediate CA certificates, cross-certificates, and link certificates. Security Provider also searches the default directory to retrieve CRLs when the CDP is DN-based and Security Provider cannot find the associated CA.</p> <p>The default directory can be any LDAP directory; it does not need to be Security Manager's directory.</p> <p>If you have only one directory, this directory is the default. If you have multiple directories and do not specify a default, the first directory listed under the directory key is used.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Directory\ Value Name: Default Value Type: REG_SZ Value Data: <Directory_friendly_name></p> <p>The <Directory_friendly_name> is the directory name exactly as it appears in the subkey under the <ESP_registry_location>\Directory\ key.</p> <p>Example:</p> <p>Value Data: My Directory</p>

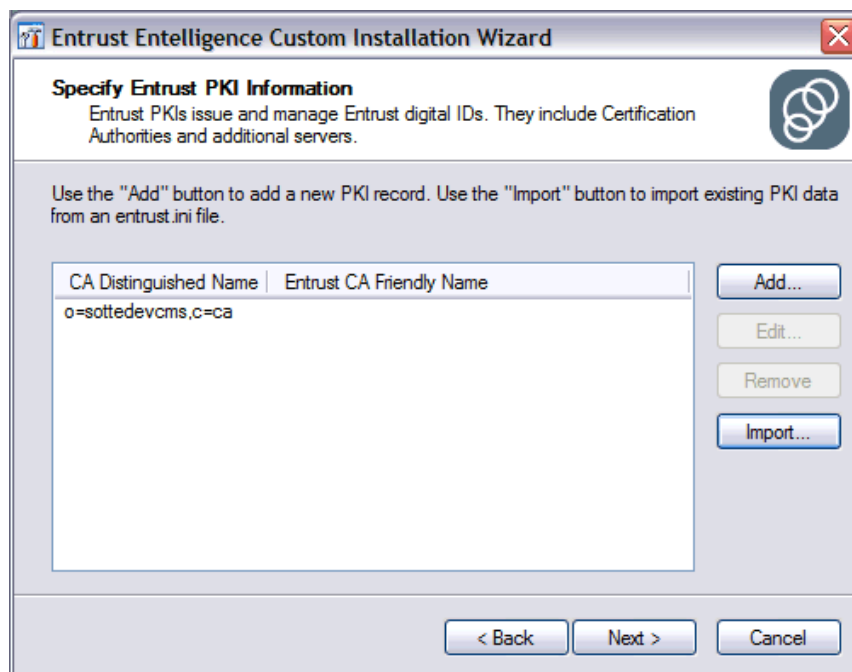
PKI settings

The PKI settings listed here are for the Security Manager CA. You must configure a Security Manager CA if you want to enable Entrust digital ID features. For a list of Entrust digital ID features, see [“Security Provider features” on page 26](#).

PKI settings include:

- [“General CA settings” on page 348](#)
- [“CA-specific directory setting” on page 352](#)
- [“Roaming Server settings” on page 354](#)
- [“Proxy server settings” on page 357](#)
- [“Auto-enrollment settings” on page 361](#)
- [“CA-specific OCSP Responder settings” on page 367](#)
- [“CardMS settings” on page 368](#)
- [“Entrust IdentityGuard settings” on page 370](#)

Figure 29: PKI settings main page



General CA settings

If you use the **Custom Installation** wizard, general CA settings are configurable through the **Certification Authority** tab (Figure 30). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 35 describes the general CA settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 30: Certification Authority tab

The screenshot shows the 'Entrust PKI Configuration' dialog box with the 'Certification Authority' tab selected. The dialog has a yellow title bar and a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: 'Auto-Enrollment', 'OCSP Responders', 'CardMS', 'IdentityGuard', 'Certification Authority' (selected), 'Policy', 'Directory', 'Roaming Server', and 'Proxy Server'. The 'Certification Authority' tab contains the following sections:

- Server information:** Includes a text field for 'Host name or IP address' with the value 'DOCSM.EXAMPLE.COM', a text field for 'Port number' with the value '829', and a 'Check Connection' button.
- Distinguished name:** Includes a text field for 'DN:' with the value 'CN=ca,C=DOC' and a 'Verify' button.
- Display information:** Includes a text field for 'Friendly name:', a radio button for 'Display this CA during enrollment and recovery' (which is selected), a text field for 'Display Order:' with the value '1', and a radio button for 'Hide this CA during enrollment and recovery'.
- Entrust Authority Administration Services:** Includes text fields for 'Enrollment URL:' and 'Recovery URL:'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Table 35: General CA settings

Setting name and location in Custom Installation wizard	Description and registry values
Specify PKI Information page > Add > Certification Authority tab > Host name or IP address Port number	<p>Sets the host (server) name and IP port, or the IP address and IP port of Security Manager. This setting is mandatory if you use an Entrust PKI.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: Authority Value Type: REG_SZ Value Data: <CA_server:port></p> <p>Example:</p> <p>Value Data: test_pki6:829</p>
Specify PKI Information page > Add > Certification Authority tab > DN	<p>Provides the distinguished name (DN) of Security Manager. This setting is mandatory and case-sensitive. You must specify one CA DN per CA that you define.</p> <p>To determine your CA DN, do one of the following:</p> <p>Method 1: On the Specify PKI Information page of the Custom Installation wizard, click Retrieve. The DN is retrieved from the CA installed at the host name or IP address you specify (Authority setting).</p> <p>Method 2: In Internet Explorer, select Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities. Locate your CA's certificate. Double-click the certificate. The Certificate dialog box appears. Select the Details tab. Click Issuer. The DN of your CA appears.</p> <p>Method 3: Access the Entrust Authority Security Manager Control Login Window as a Security Manager administrator. The CA DN appears in this window.</p> <p>Method 4: Log in to the Security Manager Administration as a Security Manager administrator. The CA DN is listed on the General Information page.</p> <p>This setting maps to the following registry key:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA></p> <p>Example:</p> <p>Key: ou=Marketing, o=My Company, c=US</p>

Table 35: General CA settings (continued)

Setting name and location in Custom Installation wizard	Description and registry values
Specify PKI Information page > Add > Certification Authority tab > Display this CA during enrollment and recovery Display order Hide this CA during enrollment and recovery	<p>In a multiple-CA environment, this specifies whether to show or hide Security Manager CAs in the Enrollment and Recovery wizards, and in what order to show them. This setting is optional.</p> <p>The settings in the Custom Installation wizard map to one registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: DisplayOrder Value Type: REG_DWORD Value Data: <0-n></p> <p><none> = The CA appears at the bottom of the list of CAs. 0 = Hide the CA. 1 (default in the Custom Installation wizard) = The CA appears first in the list of CAs in the wizards and is highlighted. 2 - <n> = The CA appears in the position given by <n>; that is, second, third, fourth, and so on.</p> <p>Keep in mind these guidelines when specifying display properties:</p> <ul style="list-style-type: none">• If only one Security Manager is defined, you must set DisplayOrder=1. Do not set it to "0" or users see errors during enrollment and recovery. With DisplayOrder=1, the Specify a Certification Authority page does not appear.• If a set of CAs has the same display order (such as 2), Security Provider displays the set in random order in its relative position in the wizard; for example, after the CA with DisplayOrder=1, and before the CA with DisplayOrder=3.• If a CA does not have a DisplayOrder setting but the other CAs do, the CA with an undefined DisplayOrder is added to the bottom of the list. <p>Example: If you have three CAs and only set DisplayOrder=1 for CA1, then CA1 appears first in the list of CAs (highlighted) while CA2 and CA3 appear in random order after CA1.</p>

Table 35: General CA settings (continued)

Setting name and location in Custom Installation wizard	Description and registry values
Specify PKI Information page > Add > Certification Authority tab > Enrollment URL	<p>Specifies the URL that enables users to self-enroll using the Web, typically using the Administration Services Web page URL. You can use the same URL address for enrollment and recovery. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: SelfAdminEnrollURL Value Type: REG_SZ Value Data: <SAS_enroll_Web_page></p> <p>Example:</p> <p>Value Data: https://www.yourserver/enroll/index.html</p>
Specify PKI Information page > Add > Certification Authority tab > Recovery URL	<p>Specifies the URL that enables users to self-recover using the Web, typically using the Administration Services Web page URL. You can use the same URL address for enrollment and recovery. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: SelfAdminRecoverURL Value Type: REG_SZ Value Data: <SAS_recover_Web_page></p> <p>Example:</p> <p>Value Data: https://www.yourserver/recover/index.html</p>
Specify PKI Information page > Add > Certification Authority tab > Friendly Name	<p>Provides the friendly name for your CA. This setting is optional. If you do not specify a friendly name, the CA DN is used.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: Name Value Type: REG_SZ Value Data: <CA_friendly_name></p> <p>Example:</p> <p>Value Data: My Company PKI</p>

Table 35: General CA settings (continued)

Setting name and location in Custom Installation wizard	Description and registry values
Specify PKI Information <i>page ></i> Add > Certification Authority tab > Name of the Cryptographic Service Provider (CSP) used to protect users' private keys	<p>The name of the CSP that protects the user's keys. If you do not specify a CSP in the certificate definition, the CSP specified in this setting is used, if no CSP is specified in either place, the Entrust Enhanced Cryptographic Provider is used.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: CSP Value Type: REG_SZ Value Data: <name_of_CSP></p> <p>Example:</p> <p>Value Data: Microsoft Base Cryptographic Service Provider v1.0</p> <p>Attention: Setting the CSP using this registry setting is not recommended. Use the CA policy instead. This setting is local to the user's computer and will not be used if they move to another computer.</p>

CA-specific directory setting

If you use the **Custom Installation** wizard, the CA-specific directory setting is configurable through the **Directory** tab (Figure 31). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 36 describes the CA-specific directory setting. The table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Note: Additional directory settings are available. For details, see [“Directory settings” on page 331](#).

Figure 31: Directory tab

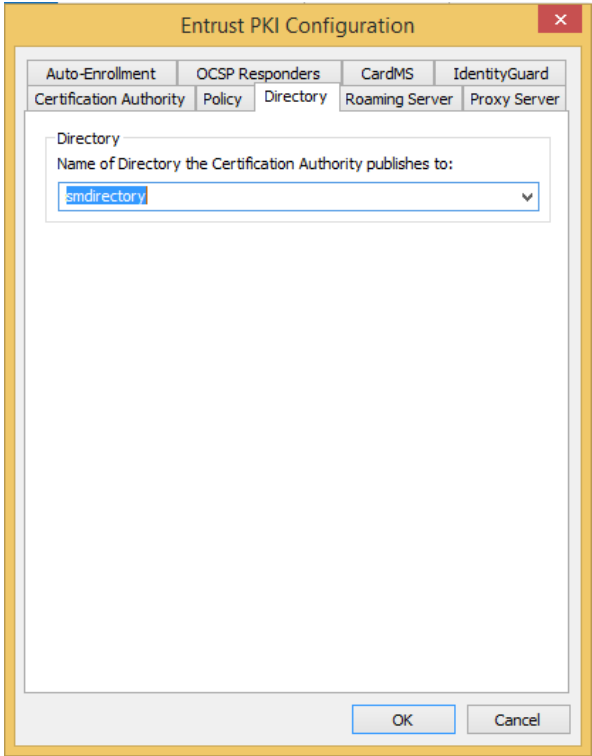


Table 36: Directory settings specific to the CA

Setting name and location in Custom Installation wizard	Description and registry value
Specify PKI Information page > Add > Directory tab > Name of Directory	<p>Specifies the directory associated with the CA. This setting is mandatory if you use Security Manager as your CA.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: DirectoryName Value Type: REG_SZ Value Data: <Directory_friendly_name></p> <p>The <Directory_friendly_name> maps to the name that appears in the subkey under the <ESP_registry_location>\Directory\ key.</p> <p>Example:</p> <p>Value Data: My Security Manager Directory</p>

Roaming Server settings

If you use the **Custom Installation** wizard, Roaming Server settings are configurable through the **Roaming Server** tab (Figure 32). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 37 describes the Roaming Server settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 32: Roaming Server tab

Entrust PKI Configuration

Auto-Enrollment

OCSP Responders

CardMS

IdentityGuard

Certification Authority

Policy

Directory

Roaming Server

Proxy Server

☐ Enable Entrust Authority Roaming Server

Server information

Host Name or IP Address	Port	TLS Port
-------------------------	------	----------

Add...

Edit...

Remove

Encryption algorithm

☒ CAST-128

☐ Triple DES

☐ IDEA

OK

Cancel

Table 37: Roaming Server settings

Setting name and location in Custom Installation wizard	Description and registry value
Specify PKI Information page > Add > Roaming Server tab > Enable Entrust Authority Roaming Server Add > Host Name or IP Address Port TLS Port	<p>Specifies the Entrust Authority Roaming Server's host name or IP address and port. The default Roaming Server port is 640. You can add the TLS port of Roaming Server if it is different from the default port (640). You may specify multiple Roaming Servers. This setting is only required if you use Roaming Server. See "Using the Roaming Server" on page 170 for details.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: RoamingServer Value Type: REG_SZ Value Data: <rs1hostname:port> <rs2hostname:port></p> <p>If you want to specify a TLS port in addition to the Roaming Server port, specify it as follows:</p> <p><rs1hostname:port:tlspport></p> <p>Examples:</p> <p>Value Data: roamsvr6:640 Value Data: roamsvr6:640:443</p>
Specify PKI Information page > Add > Roaming Server tab > Encryption Algorithm	<p>Specifies the encryption algorithm to encrypt users' Entrust roaming security stores. This setting is optional.</p> <p>Note: The algorithm specified must be accepted by your Roaming Server setting.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: RoamingEncryptionAlgorithm Value Type: REG_SZ Value Data: <Encryption_Algorithm></p> <p>Acceptable values:</p> <p>CAST-128 (default) Triple DES IDEA</p> <p>Example:</p> <p>Value Data: Triple DES</p>

Table 37: Roaming Server settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>By default, security provider does not automatically enforce a policy switch made after enrollment is completed.</p> <p>For example, if the administrator modified the Role policy to allow only Roaming, after enrolling a Desktop based user, the user would not be automatically switched to the Roaming server.</p> <p>Previously, the user needed to use the Entrust Security Store Options dialog from the system tray.</p> <p>This action takes place when receiving the role policy after a login.</p> <p>A new registry setting is added to ESP, allowing to automate this process:</p> <p>Key: <ESP_registry_location> Value Name: EnableAutomaticEntrustSecurityStoreTypeSwitch Value Type: DWORD Value Data: <0_or_1></p> <p>Default: 0</p> <p>Values:</p> <p>0: Security Provider does not automatically switch Entrust security store type based on the role policy.</p> <p>1: Security Provider automatically switches from a Roaming to a Desktop only profile or Desktop to Roaming only profile if the role policy is changed.</p>

Proxy server settings

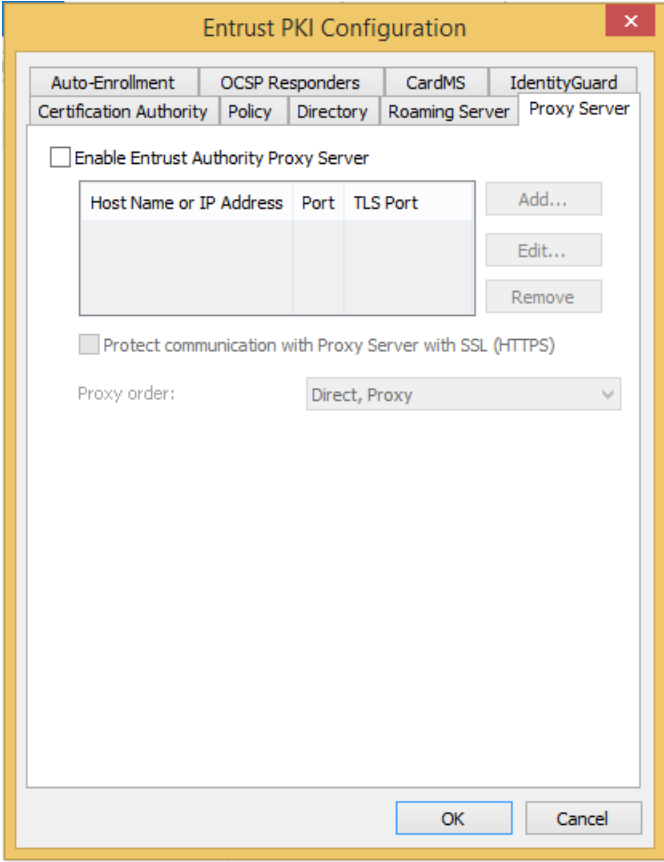
If you use the **Custom Installation** wizard, proxy server settings are configurable through the **Proxy Server** tab (Figure 33). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 38 describes the proxy server settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Note: You can also set connection timeout settings for the proxy server. See [“HTTP connection and timeout settings” on page 476](#).

Figure 33: Proxy Server tab



The image shows the 'Entrust PKI Configuration' dialog box with the 'Proxy Server' tab selected. The dialog has a yellow title bar and a red close button. The tabs are arranged in two rows: Auto-Enrollment, OCSP Responders, CardMS, IdentityGuard in the first row, and Certification Authority, Policy, Directory, Roaming Server, Proxy Server in the second row. The 'Proxy Server' tab contains the following controls:

- An unchecked checkbox labeled 'Enable Entrust Authority Proxy Server'.
- A table with three columns: 'Host Name or IP Address', 'Port', and 'TLS Port'. The table is currently empty.
- Buttons 'Add...', 'Edit...', and 'Remove' to the right of the table.
- An unchecked checkbox labeled 'Protect communication with Proxy Server with SSL (HTTPS)'.
- A label 'Proxy order:' followed by a dropdown menu showing 'Direct, Proxy'.
- 'OK' and 'Cancel' buttons at the bottom right.

Host Name or IP Address	Port	TLS Port
-------------------------	------	----------

Table 38: Proxy Server settings

Setting name and location in Custom Installation wizard	Description and registry value
<p>Specify PKI Information page > Add > Proxy Server tab > Enable Entrust Authority Proxy Server Host Name or IP Address Port Number</p>	<p>Use this setting if you want Security Provider for Windows to connect to PKI components, such as Security Manager and Roaming Server, through the Entrust Authority Security Manager Proxy.</p> <p>Provides the host (server) name or IP address plus the IP port of your proxy servers, separated by a semi-colon. If no port is specified, port 80 is assumed for HTTP, and port 443 for HTTPS. See the next table row for more information on HTTP and HTTPS.</p> <p>When multiple proxy servers are specified, Security Provider attempts to connect to them in the order they are listed, until it a successful connection is established. See also the Proxy Order setting on page 360.</p> <p>Note 1: If the Proxy value is not specified, the Authority value must be specified. This setting is optional.</p> <p>Note 2: If you set the Proxy setting to use non-standard ports (standard ports being 80 and 443), you must set certain parameters. See “To configure Security Manager Proxy for use with Security Provider” on page 178.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: Proxy Value Type: REG_SZ Value Data: <proxyserver1:httpport:httpsport;proxyserver2:httpport:httpsport></p> <p>Examples:</p> <p>Value Data: proxyserver1;proxyserver2 (use this syntax if you are using default HTTP and/or HTTPS ports, which are 80 and 443, respectively)</p> <p>Value Data: proxyserver1:81;proxyserver2:81 (use this syntax if you are using HTTP with non-default ports)</p> <p>Value Data: proxyserver1:81:444;proxyserver2:81:444 (use this syntax if you are using HTTPS with non-default ports. Both HTTPS and HTTP ports must be specified because CRLs can only ever be retrieved over HTTP.)</p>

Table 38: Proxy Server settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Determines whether the connection to Security Manager Proxy is over HTTP or HTTPS/TLS.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: ProxyForceHttps Value Type: REG_DWORD Value Data: <0_or_1></p> <p>0 (default) = Use HTTP 1 = Use HTTPS/TLS</p> <p>Note: For HTTPS/TLS to work, you must set certain parameters on Security Manager Proxy. For details, see "To configure Security Manager Proxy for use with Security Provider" on page 178.</p>
<p>Specify PKI Information page ></p> <p>Add ></p> <p>Proxy Server tab ></p> <p>Proxy Order</p>	<p>Determines whether Security Manager Proxy Server or Security Manager is contacted first. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: ProxyOrder Value Type: REG_DWORD Value Data: <1-4></p> <p>1 = Proxy, Direct. A connection to the proxy servers is attempted first. If no connection to any of the proxy servers can be established, a direct connection to Security Manager is attempted.</p> <p>2 (default) = Direct, Proxy. A connection to Security Manager is attempted first. If that fails, a connection to the proxy servers is attempted.</p> <p>3 = Direct only. A connection to Security Manager is attempted. If that fails, connections to other components are not attempted.</p> <p>4 = Proxy only. A connection to the proxy servers is attempted. If no connection to any of the proxy servers can be established, connections to other components are not attempted.</p>

Auto-enrollment settings

If you use the **Custom Installation** wizard, auto-enrollment settings are configurable through the **Auto-Enrollment** tab (Figure 34). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 39 describes the auto-enrollment settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

- Note:** Auto-enrollment timeout and logging settings are also available. See the following sections for details:
- [“HTTP connection and timeout settings” on page 476](#)
 - [“Logging settings” on page 489](#)

Figure 34: Auto-Enrollment tab

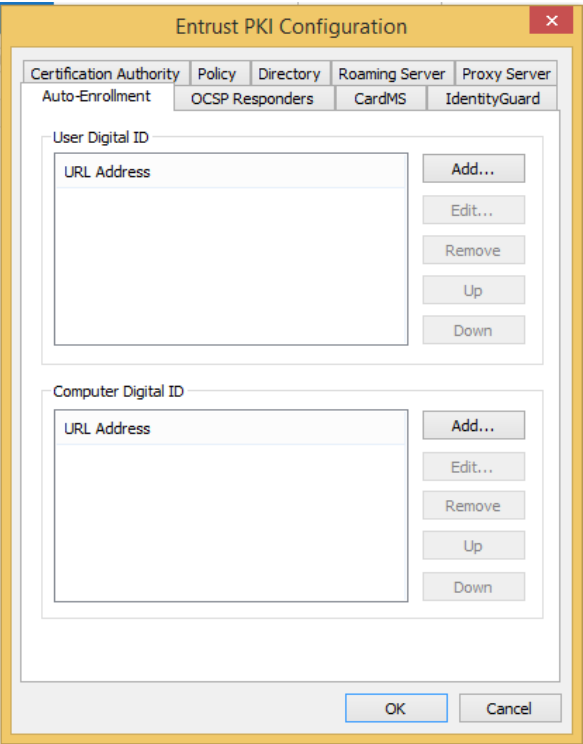


Table 39: Auto-enrollment settings

Setting name and location in Custom Installation wizard	Description and registry value
Specify PKI Information page > Add > Auto-Enrollment tab > Add (beside User Digital ID) > URL Address	<p>Specifies the Auto-enrollment Service HTTPS URL for users. This lets you configure user enrollment through the Auto-enrollment Service. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollUserURL Value Type: REG_SZ Value Data: <URL1>; <URL2></p> <p>Example of an Auto-enrollment Service URL:</p> <p>https://abc.xyz.com/AutoEnrollment/AutoEnroll</p>
Specify PKI Information page > Add > Auto-Enrollment tab > Add (beside Computer Digital ID) > URL Address	<p>Specifies the Auto-enrollment Service HTTPS URL for computers. This lets you configure computers to enroll through the Auto-enrollment Service. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollMachineURL Value Type: REG_SZ Value Data: <URL1>; <URL2></p> <p>Example of an Auto-enrollment Service URL:</p> <p>https://abc.xyz.com/AutoEnrollment/AutoEnroll</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>If you use the Auto-enrollment Service, you can optionally specify a certificate type and role for user auto-enrollment or recovery. This setting overrides the certificate type and role that you configure through the Auto-enrollment Service. For further information, see "Customizing the certificate type and role" on page 154 as well as the <i>Entrust Authority Administration Services Configuration Guide</i>.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollUserDigitalIDType Value Type: REG_SZ Value Data: <string from ae-default.xml file></p>

Table 39: Auto-enrollment settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>If you use the Auto-enrollment Service, you can optionally specify a certificate type and role for machine auto-enrollment or recovery. This setting overrides the certificate type and role that you configure through the Auto-enrollment Service. For further information, see “Customizing the certificate type and role” on page 154 as well as the <i>Entrust Authority Administration Services Configuration Guide</i>.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollMachineDigitalIDType Value Type: REG_SZ Value Data: <string from ae-default.xml file></p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Determines the number of auto-enrollment retries that should be attempted when the Auto-enrollment Service returns an error code to Security Provider for Windows. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollNumberOfRetries Value Type: REG_DWORD Value Data: <number_of_retries></p> <p>Example:</p> <p>Value Data: 10</p> <p>The default is 10.</p> <p>See “Resending auto-enrollment requests” on page 158 for more information.</p>

Table 39: Auto-enrollment settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>When the Auto-enrollment Service sends an error code in a response message to Security Provider for Windows, the <code>AutoEnrollRetryInterval</code> setting determines the number of seconds that should elapse between each auto-enrollment request retry.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollRetryInterval Value Type: REG_DWORD Value Data: <Number_of_seconds></p> <p>Example: Value Data: 30</p> <p>The default is 30 seconds.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Normally, Security Provider for Windows displays the security store icon in the task bar to alert users that they were enrolled for a digital ID or their ID needs to be recovered. Since users sometimes do not notice the icon, you can choose to alert users with a popup dialog instead of the icon.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: SkipAutoEnrollRecoverNotification Value Type: REG_DWORD Value Data: <0_or_1></p> <p>0 (default): Icon appears 1: Popup appears</p>

Table 39: Auto-enrollment settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>By default, if you are using Auto-enrollment Service, Security Provider detects when a user needs to be enrolled or recovered and either enrolls/recovers them silently, or adds a notification to the taskbar prompting them to enroll/recover. In both scenarios, users have no control over when the enrollment/recovery occurs.</p> <p>You can change the default behavior so that users can initiate and complete a digital ID enrollment or recovery themselves. This feature is particularly useful if users have forgotten their passwords, because it allows them to regenerate a digital ID with a new password without having to involve their PKI administrator.</p> <p>To manually create a digital ID, users click Next through the Enrollment/Recovery wizard until they come to the end at which point a digital ID is created. Note that the wizard does not prompt users for a reference number and authorization code.</p> <p>Warning: When this feature is enabled, users must not cancel the enrollment or recovery part way through. Doing so may leave their digital ID in the recovery state, preventing future management events from occurring.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: UseAutoEnrollForManualOperations Value Type: REG_DWORD Value Data: <0_or_1></p> <p>0 (default): Disable manual enrollment or recovery.</p> <p>1 = Enable manual enrollment or recovery with Auto-enrollment Service.</p> <p>Attention: If set to 1, the AllowAutoEnrollServerToRecoverIfActive setting must also be set to 1. For more on this setting, see page 366.</p>

Table 39: Auto-enrollment settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>If users cancel recovery part way through the process, it may leave their digital IDs in the recovery state, preventing future management events from occurring. Use this registry key to disable the cancel function on the Recovery wizards.</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: AutoEnrollDisableRecoveryWizardCancel Value Type: REG_DWORD Value Data: <0_or_1></p> <p>0 (default): Enable the cancel function.</p> <p>1 = Disable the cancel function. If users click Cancel, a dialog appears asking them to complete the recovery.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Determines if Security Provider performs a recovery if a user logs in to Windows and their certificate is not immediately available in the Personal certificate store. Security Provider uses the Auto-enrollment Service for recovery.</p> <p>Do not enable this feature for deployments that include smart cards or roaming security stores. For example, if you enable this setting and a roaming user logs in to many different computers, the digital ID will be recovered on each of those computers.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: AllowAutoEnrollServerToRecoverIfActive Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Do not automatically recover users.</p> <p>1 = Automatically recover users.</p> <p>Example: Value Data: 1</p>

CA-specific OCSP Responder settings

If you use the **Custom Installation** wizard, OCSP Responder settings are configurable through the **OCSP Responders** tab (Figure 35). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 40 describes the OCSP Responder setting.

The setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Note: Additional OCSP settings are available. For details, see [“OCSP Revocation Provider settings” on page 425](#) and [“HTTP connection and timeout settings” on page 476](#).

Figure 35: OCSP Responders tab

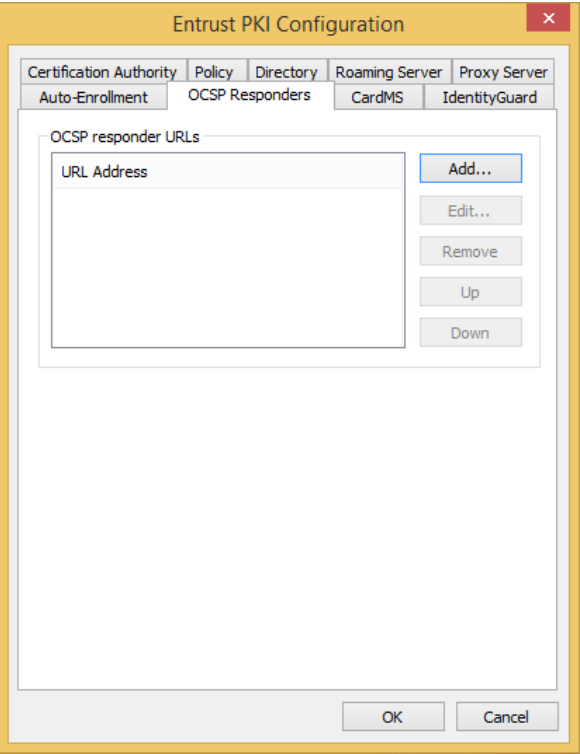


Table 40: CA-specific OCSP Responders settings

Setting name and location in Custom Installation wizard	Description and registry value
Specify PKI Information page > Add > OCSP Responders tab > OCSP Responder URLs Add > URL Address	<p>Specifies a list of OCSP Responder URLs in HTTP or HTTPS format. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: OCSPResponderURLs Value Type: REG_SZ Value Data: <URL1>; <URL2></p>

CardMS settings

If you use the **Custom Installation** wizard, CardMS settings are configurable through the **CardMS** tab (Figure 36). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 41 describes the CardMS settings.

Note: A CardMS logging setting also exists. It is detailed under [“Logging settings” on page 489](#).

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Attention: Integrating with a CardMS involves more than configuring registry settings. For step-by-step integration instructions, see [“Integrating Security Provider and a CardMS” on page 189](#).

Figure 36: CardMS tab

Entrust PKI Configuration

Certification Authority

Policy

Directory

Roaming Server

Proxy Server

Auto-Enrollment

OCSF Responders

CardMS

IdentityGuard

☐ Enable card management system integration (CardMS)

Name of CardMS client:

OK

Cancel

Table 41: CardMS settings

Setting name and location in Custom Installation wizard	Description and registry value
Specify PKI Information page > Add > CardMS tab > Enable Card Management System Integration Name of CardMS client	<p>Gives the CardMS name exactly as it appears under HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\ESP\CardMS\</p> <p>Note: In order for the name to appear, you must register the CardMS client .dll by typing regsvr32 <path_to_client_dll> at a command-line prompt.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: CardMSUpdatesPerformedBy Value Type: REG_SZ Value Data: <CardMS_name></p> <p><CardMS_name> is the name of the CardMS exactly as it appears under HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\ESP\CardMS\</p> <p>Example:</p> <p>Value Data: My Card MS</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Provides the name and path of the CardMS client .dll file.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\CardMS\<CardMS_name> Value Name: DLLPath Value Type: REG_SZ Value Data: <path_to_dll_on_user_computer></p> <p>Example:</p> <p>Value Data: C:\Program Files\Entrust\ESP\MyClient.dll</p>

Entrust IdentityGuard settings

If you use the **Custom Installation** wizard, The Entrust IdentityGuard setting is configurable through the **IdentityGuard** tab (Figure 36). To navigate to this tab, click **Add** on the **Specify PKI Information** page.

Table 42 describes the Entrust IdentityGuard settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#)

Figure 37: Entrust IdentityGuard Tab

Entrust PKI Configuration

Certification Authority

Policy

Directory

Roaming Server

Proxy Server

Auto-Enrollment

OCSP Responders

CardMS

IdentityGuard

Entrust IdentityGuard Self-Service Module Transaction Component

Hostname:

IDGServer.example.com

Port number:

8445

Check Connection

OK

Cancel

Table 42: Entrust IdentityGuard settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	This is the URL used by ESP to communicate with Entrust IdentityGuard for smart card management operations. If this is not in the installation package, it is filled in automatically when ESP and Entrust IdentityGuard first connect. Key: <ESP_registry_location>\CardMS\<CardMS_name> Value Name: IdentityGuardURL Value Type: String Value Data: <URL for IdentityGuard>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Security Provider generates a message asking a user to communicate with their Administrator when a PIV digital ID update is required. The message is configurable. Enter a custom message to have it displayed instead. This setting will accept a large number of characters. Check the custom message to be sure that it displays as you expected. Path: <ESP_registry_location> Name: PIVMessageForRequiredUpdatesWithNonConfiguredIDG Type: REG_STRING Value: Message string. Default: By default, the original message is used.

Entrust digital ID settings

Entrust digital ID settings include:

- [“Entrust digital ID for users options settings” on page 373](#)
- [“Entrust Entelligence Windows Service Digital ID settings” on page 389](#)
- [“Entrust computer digital ID settings” on page 392](#)
- [“Entrust security store settings” on page 396](#)

Note: See also [“Entrust security store settings” on page 396](#).

Entrust digital ID for users options settings

If you use the **Custom Installation** wizard, Entrust user digital ID settings are configurable through the **Entrust Digital ID for Users Options** page (Figure 38).

Table 43 describes the “Entrust digital IDs for users options” settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 38: Entrust digital ID for a user page

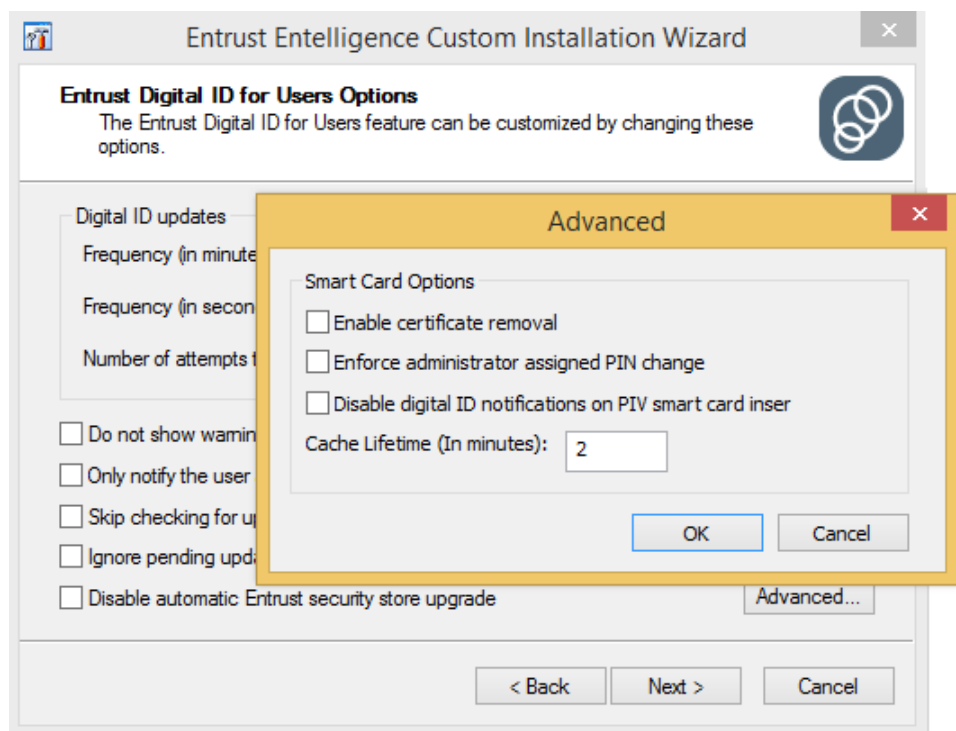


Table 43: Entrust digital ID for a user settings

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Frequency (in minutes) to check for updates	<p>Sets the interval at which Security Provider's Digital ID Monitor checks whether the certificates in the user's certificate store need to be updated. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: CertUpdateInterval Value Type: REG_DWORD Value Data: <0-n_minutes></p> <p>0 = Security Provider does not check for updates.</p> <p>Example:</p> <p>Value Data: 720</p> <p>The default is 720 minutes (12 hours).</p>
Entrust Digital ID for Users Options page > Frequency (in seconds) to wait before retrying if server is unavailable	<p>Sets the interval in seconds at which Security Provider's Digital ID Monitor retries managing a user's Entrust digital ID if it receives a Cannot Connect error code. This retry is particularly useful for VPN users who may log in to their security stores before creating their VPN connection. In this scenario, the first couple of management attempts may fail, but once the VPN connection is established, Security Provider can successfully check for updates.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: RetryManagementOfflineInterval Value Type: REG_DWORD Value Data: <0-n></p> <p>0 = Security Provider does not retry.</p> <p>Example:</p> <p>Value Data: 15</p> <p>The default is 30 seconds.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Number of attempts to retry if the server is unavailable	<p>Sets the number of times Security Provider's Digital ID Monitor attempts to retry managing a user's digital ID when the server is unavailable. This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: RetryManagementOfflineAttempts Value Type: REG_DWORD Value Data: <0-n></p> <p>0 = After the first attempt fails, Security Provider does not retry again.</p> <p>Example: Value Data: 10</p> <p>The default is 5.</p>
Entrust Digital ID for Users Options page > Do not show warning if digital ID is missing certificates	<p>Hides a dialog box that appears when the user's Entrust digital ID is missing certificates. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: SkipMissingCertsNag Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Show the dialog box. 1 = Hide the dialog box.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Disable automatic Entrust Security Store upgrade	<p>Disables the automatic migration of a user's v3 Entrust security stores to v4. This setting is optional. This setting is used when users migrate from Entrust Desktop Solutions to Security Provider.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DisableAutomaticEntrustSecurityStoreUpgrade Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Enable the automatic migration. 1 = Disable the automatic migration.</p> <p>Attention: Entrust recommends that this setting not be used. There are no known reasons why the migration from version 3 to version 4 should be prevented. The configuration setting is provided solely for customers that have a unique and specific need to prevent migration.</p> <p>Note: If you disable the automatic migration, when users start using Security Provider they will not have access to their old decryption keys. This becomes a problem when a user wants to decrypt an older message that can only be decrypted with the older key. To provide access to these older keys, the automatic upgrade must be enabled.</p>
Entrust Digital ID for Users Options page > Skip checking for updates after Entrust security store login	<p>By default, the action of a user logging in to an Entrust security store notifies the Digital ID Monitor to check this digital ID for a pending update. If this key is set to 1, it prevents the Digital ID Monitor from checking the logged-in ID immediately.</p> <p>Key: <ESP_registry_location> Value Name: SkipUpdateAfterEntrustSecurityStoreLogin Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = The Digital ID Monitor checks the digital ID for a pending update as soon as a user logs in. 1 = Do not check for an update immediately when a user logs in. Instead, the check is performed at the time interval set by CertUpdateInterval.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Ignore pending update during Entrust security store login	<p>By default, if multiple users with separate .epf files use the same Windows account, a notice appears when any of the .epf files needs an update. This can confuse users as they may think the notice applies to them when it does not. Set this key to prevent an update of an .epf file until the owner of that file logs in.</p> <p>Key: <ESP_registry_location> Value Name: IgnoreEntrustSecurityStoreUpdateUntilLogin Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Always display update notices. 1 = Do not display update notices for users who are not logged in.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard	<p>These two registry settings let you import additional CA certificates to users' desktop security stores (.epf files). Users can then take their .epf to another computer and use it successfully. (Without all the CA certificates present, it is less likely that the .epf can be used on another computer.)</p> <p>The registry settings are as follows:</p> <p>Key: HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\ESP (32 bit) or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Entrust\ESP (64 bit) Value name: ImportCACertChainForNonVerificationCertificates Type: DWORD Value Data: 0 or 1 (default)</p> <p>When 1, Security Provider imports the CA certificate chain for all of the user's current non-verification certificates (encryption certificates, for example). Any CA certificate that is not also part of the current verification certificate CA chain is placed in the 'Intermediate CA' section of the .epf file (including self-signed certificates).</p> <p>When 0, the behavior above is disabled.</p> <p>Key: HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\ESP (32 bit) or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Entrust\ESP (64 bit) Value name: ImportPreviousCACertificates Type: DWORD Value Data: 0 or 1 (default)</p> <p>When 1, Security Provider imports all the CA certificates from the user's old desktop security store (.epf file) into their current .epf file. Any CA certificate that is not part of the current verification certificate CA chain is placed in the 'Intermediate CA' section of the .epf file. Any CA certificate that is self-signed also goes in the 'Intermediate CA' section. The import occurs when the user logs in to their current desktop security store.</p> <p>When set to 0, the behavior above is disabled.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard	<p>The registry setting below allows administrators to disable the following notifications that Security Provider users receive when they login in to their Entrust Security Store:</p> <ul style="list-style-type: none">• notifications that are used to update Security Provider for Outlook settings• notifications that are used to update specific 3rd party applications such as Outlook and Cisco and Nortel VPN applications <p>Key: <ESP_registry_location> Value Name: DisableEPFLoginNotification Value Type: DWORD Value Data: <0_or_1></p> <p>0- (Default) Security Store login notifications are enabled. 1- Security Store login notifications are disabled.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard	<p>This setting enables Security Provider to save the Entrust Security Store immediately after performing a key management operation. This configuration setting is designed to save the Entrust Security Store for those users relying on a VPN connection, a Remote Desktop Service, or in Citrix environment.</p> <p>Key: <ESP_registry_location> Value Name: SaveEPFOnKeyManagement Value Type: DWORD Value Data: <0-1></p> <p>0 Don't attempt to save the EPF after a key management operation (default value). 1 Save EPF after a key management operation.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Only notify the user about update if the Entrust Security store is logged in	<p>When Security Provider for Windows detects that a digital ID requires an update, by default it automatically updates the Entrust digital ID when the user logs in. You can change this behavior so that the digital ID is not updated and an update icon appears instead.</p> <p>Key: <ESP_registry_location> Value Name: EffectOfLoginOnWaitingUpdate Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = If there is a pending Entrust digital ID update and the user is logging in to their digital ID, perform the update automatically, with no further action required.</p> <p>1= If there is a pending Entrust digital ID update and a user is logging in to their digital ID, do not update the ID automatically. Instead, display the Update Request icon in the taskbar notification area. The user must click this icon and select Update in order for the update to occur.</p> <p>Note: If the user is not logged in to their Entrust digital ID, then the Update Request icon appears in the taskbar regardless of whether you activated or deactivated the EffectOfLoginOnWaitingUpdate setting.</p>
You can specify this setting's registry value in Enable Certificate Removal on the Entrust Digital ID for Users > Advanced page of the Custom Installation wizard.	<p>By default, when the smart card is in use, certificates on the smart card are imported to the personal certificate store. The certificates are not removed by default when the smart card is removed.</p> <p>To enable certificate removal, leaving the certificates in the user's personal certificate store, add the following configuration setting to the registry:</p> <p>Key: <ESP_registry_location> Value Name: EnableSmartCardCertificateRemoval Value Type: REG_DWORD Value: 0 or 1</p> <p>0 (default) the certificates are not removed when the smart card is removed or 1, the certificates are removed from the personal certificate store.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>You can specify this setting's registry value in Enforce Administrator Assigned PIN change on the Entrust Digital ID for Users > Advanced page of the Custom Installation wizard.</p>	<p>When it is enabled, this setting forces users to change their administrator assigned PIN. Administrators configure the maximum number of successful authentications using the administrator-assigned PIN in Entrust IdentityGuard. If the user does not change the PIN before the maximum number of successful authentications, the smart card is blocked.</p> <p>Key: <ESP_registry_location> Value Name: PIVEnforceAdminAssignedPINChange Value Type: DWORD Value: 0 (user is not forced to change the administrator assigned PIN) or 1 (user must change the administrator assigned PIN)</p> <p>Each time the user enters the Administrator assigned PIN, users are presented with a message asking them to change their PIN (this happens whether or not this registry value is set). When the number of uses left approaches 0, users are given a warning message. When no uses are left, the smart card is blocked.</p> <p>Note: IdentityGuard Administrators should set the allowed number of PIN uses to a high number, as each login to a Windows account causes Windows to authenticate to the smart card multiple times.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Update digital ID silently</p>	<p>If this feature is enabled, the user's digital ID is updated silently without notifying the user when the digital ID monitor detects that an update is required.</p> <p>Note: The PKIX-CMP signing key must not be password protected for this feature to work properly. Be sure that Protect key storage for CSP is not selected in Security Manager's certificate definition policy settings.</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: UpdateDigitalIDSilently Value Type: REG_DWORD Value Data: <0 or 1></p> <p>0 (default) – The users are prompted with an Entrust Digital ID Update Request icon in their system tray when the digital ID monitor detects that an update is required.</p> <p>1 - The user's digital ID is updated silently without notifying the user when the digital ID monitor detects that an update is required.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>A client such as Security Provider can communicate with the Security Manager using an expired private signing key, provided the corresponding public verification certificate is still valid. This allows the Entrust digital ID to be updated (rather than recovered) after the private signing key has expired, and before the certificate has expired.</p> <p>You can control whether Security Provider will accept a certificate with an expired signing key.</p> <p>Key: <ESP_registry_location>\PKI\<CA_DN> Value Name: DoNotUseExpiredSignKeyInPkixCMP Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Allow certificate with expired signing key to communicate with the CA.</p> <p>1 = Do not allow certificate with expired signing key to communicate with the CA.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. Delay starting digital ID monitor	<p>The digital ID monitor can be configured to delay its startup. This can be used to prevent the digital ID monitor from detecting old certificates when using a smart card, since some smart card middleware takes a few seconds after login to propagate the smart card's current certificates in to the local certificate stores.</p> <p>Key: <ESP_registry_location> Value Name: MonitorStartingDelay Value Type: REG_DWORD Value Data: delay (in milliseconds) default value is 0</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Delay starting digital ID monitor</p>	<p>This setting allows administrators to configure the delay between the detection of the smart card and the start of the digital ID management cycle. By default, 15 seconds will pass between smart card detection and the triggering of the digital ID management cycle. Values from 0 to 300 seconds (inclusive) are allowed. The log messages "A new smart card was inserted: <smart card name>" and "Digital ID management triggered by smart card monitoring." track information about the time a particular smart card was detected and the start of the digital ID management cycle.</p> <p>Key: <ESP_registry_location> Value Name: MonitorSmartCardDelay Value Type: DWORD Value Data: <delay in seconds></p> <p>Default value data: 15</p> <p>Allowed values: 0 to 300</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Controls the number of times that the user can skip updating the certificate</p>	<p>Controls the number of times that a user can use the Remind me later option in the Entrust Digital ID Update Request dialog box to skip updating their digital ID.</p> <p>Key: <ESP_registry_location> Value Name: IgnoreUpdateAttempts Value Type: REG_DWORD Value Data: <0, 1, n> default value is 5</p> <p>Each time the user skips an update, the value in the certificate property EE_CERT_PROP_HAVE_IGNORED_UPDATE_ATTEMPTS is increased by one. The Remind me later option is disabled when the value equals or exceeds the value in IgnoreUpdateAttempts. The value of EE_CERT_PROP_HAVE_IGNORED_UPDATE_ATTEMPTS is reset to 0 when the certificate is updated. If a certificate is deleted the monitor checks the other certificates in the digital ID to get this property.</p> <p>Note: If the SkipUpdateNotification setting is set to 1, no notification occurs.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Specifies that the Digital ID Monitor open the update dialog rather than displaying an icon in the taskbar.</p>	<p>By default Digital ID Monitor checks security store users at a configurable time interval to see if a key update is required. If a key update is required, an icon appears in the user's task bar which they can click to open the Entrust Digital ID Update Request dialog box.</p> <p>This setting enables administrators to configure the monitor to skip the notification icon and open the update dialog directly.</p> <p>Key: <ESP_registry_location> Value Name: SkipUpdateNotification Value Type: REG_DWORD Value Data: <0, 1></p> <p>0 (default) - Show the digital ID update notification in task bar notification icon</p> <p>1 - Skip the digital ID update notification icon in the task bar and show the digital ID update required dialog.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>By default, the CSP retrieves all available certificates during the smart card login process. The registry setting, "PIVOptimizeWindowsLoginPerformances" makes this behavior configurable. If the value is set to 1, the CSP retrieves only 1 certificate, speeding up the Windows login process. The PIV application retrieves the other certificates and adds them to the user's personal store after the user is logged in.</p> <p>Key:<ESP_registry_location> Value Name: PIVOptimizeWindowsLoginPerformances Type: DWORD Default value data: 0</p> <p>Allowed values: 0 or 1</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>EDS Notification Plugin</p>	<p>When set to 1 (true), Entrust Desktop Solutions (EDS)-specific information is removed from the user's smart card when the user enrolls for a certificate, updates their certificate or renews their certificate. Further logins to EDS are not possible. This setting only takes effect if the user has their Entrust digital ID stored on a smart card.</p> <p>Typically, you would leave this setting at its default of 0 to enable switching back to EDS from Security Provider. If, at a later time, you decide to remove EDS from your environment, you may consider setting <code>RemoveEDSSupport</code> to 1 to prevent the use of EDS.</p> <p>Note: To enable switching between EDS and Security Provider, additional configurations are required. See "Using smart cards with Security Provider and EDS" on page 185 for details.</p> <p>Key: <ESP_registry_location>\Notify\EDSClient Value Name: RemoveEDSSupport Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Do not remove EDS support. Switching back to EDS from Security Provider is allowed.</p> <p>1 = Remove EDS support. Further logins to EDS are not possible.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>EDS notification plugin</p>	<p>This setting is used to specify the PKCS11 library path when using the EDS notification plugin. By default it is set to <code>dkck201.dll</code>.</p> <p>Key: <ESP_registry_location>\Notify\EDSClient Value Name: DllNamePKCS11 Value Type: REG_SZ Value Data: <name_of_dll></p> <p>Note: The library name may be different for newer client software. For example, starting with the SafeNet 5100 eToken the library name is <code>eTPKCS11.dll</code>.</p>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. EDS notification plugin	This data object is required to enable login. The plug-in configuration contains an entry ("EntrustProfilePath") for this object. Default Setting: %APPDATA%\Entrust Security Store Key: <ESP_registry_location>\Notify\EDSClient Value Name: EntrustProfilePath Value Type: REG_SZ Value Data: <profile_path>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. EDS notification plugin	Identifies if EDS profile full recoveries are enabled. If set to 1, full recoveries are enabled. If set to 0, full recoveries are disabled. Default is 1. Key: <ESP_registry_location>\Notify\EDSClient Value Name: EnableEDSProfileFullSync Value Type: dword Value Data: <0_or_1>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. EDS notification plugin	Identifies if the wizard is shown during synchronization. If set to '0', users will not see the wizard when synchronizing the profile. Default is 1. Key: <ESP_registry_location>\Notify\EDSClient Value Name: WizardVisibility Value Type: dword Value Data: <0_or_1>

Table 43: Entrust digital ID for a user settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Determines at what percentage of the key's lifetime Security Provider will update the key.</p>	<p>This setting allows the Administrator to configure Security Provider to update the verification certificate at a specific percentage of the key's lifetime. For example, if set to the default (70%) Security Provider initiates a key update at when 70% of the keys lifetime has passed.This setting is configured separately for each CA.</p> <p>If Update cert at % of lifetime is set for the certificate in Security Manager, this percentage is also used.</p> <p>If, for example, you have a verification certificate with a lifetime of 100 days and Update cert at % of lifetime is not set. When PrivateKeyUsagePeriodPercentage is set to 60 in the registry, Security Provider assumes the private key lifetime is 100* 60% = 60 days.</p> <p>However, if Update cert at % of lifetime is set to 80 in the certificate definition policy for this verification certificate, Security Provider will calculate that the certificate requires an update when the certificate reached 60*80%= 48 days.</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: PrivateKeyUsagePeriodPercentage Value Type: REG_DWORD Value Data: <1 to 100> default value is 70</p>

Entrust Intelligence Windows Service Digital ID settings

If you use the **Custom Installation** wizard, Windows Service digital ID settings are configurable through the **Entrust Intelligence Windows Service Digital ID Service** options.

Figure 39: Digital ID For Windows Services

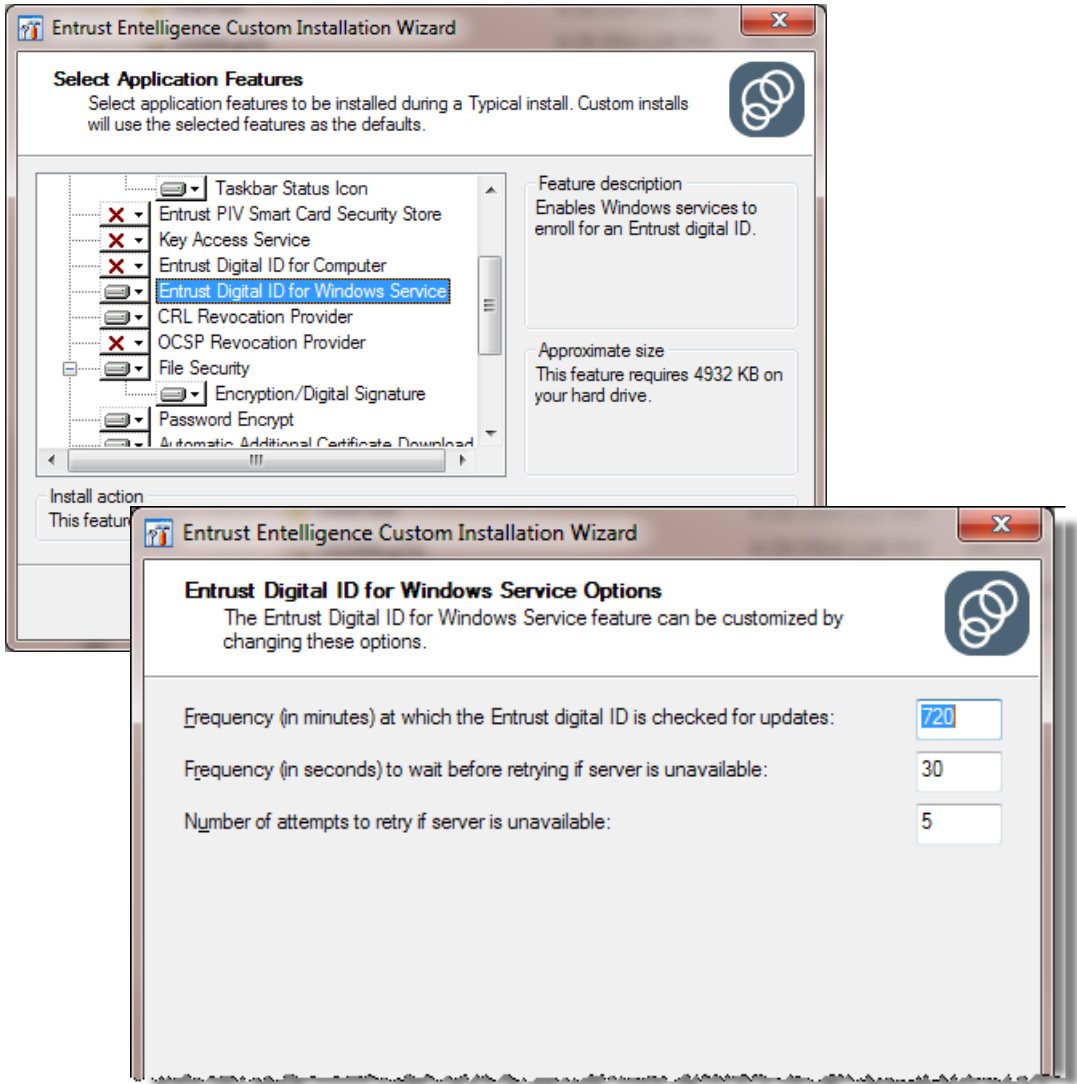


Table 44 describes the **Entrust Intelligence Windows Service Digital ID Service** settings.

The settings in the table refer to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#)

Table 44: Entrust digital ID for Windows Services settings

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Windows Service page> Frequency (in minutes) at which the Entrust digital ID is checked for updates	<p>Sets the interval at which the Entrust Entelligence Windows Service Digital ID Service checks whether the Windows Service certificates need to be updated. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: ServiceCertUpdateInterval Value Type: REG_DWORD Value Data: <0-n_minutes></p> <p>0 = Security Provider does not check for updates. Updates are only checked for if the administrator manually triggers an update from the MMC snap-in or if the service starts. Usually, the service only starts when the computer starts.</p> <p>Example: Value Data: 720</p> <p>The default is 720 minutes (12 hours).</p>
Entrust Digital ID for Windows Service page Frequency (in seconds) to wait before retrying if server is unavailable	<p>Sets the interval in seconds at which Entrust Entelligence Windows Service Digital ID Service retries managing a service's Entrust digital ID if it receives a Cannot Connect error code. This setting is optional.</p> <p>Note: The Windows service's digital ID must be in the local service certificate store not the current user certificate store. The DN of the issuer of the service's digital ID should be the same as the one specified in the registry under the PKI registry key (in <ESP_registry_location>\PKI\<DN_of_CA>).</p> <p>Key: <ESP_registry_location> Value Name: ServiceRetryManagementOfflineInterval Value Type: REG_DWORD Value Data: <0-n> seconds</p> <p>0 = Security Provider does not retry.</p> <p>Example: Value Data: 15</p> <p>The default is 30 seconds.</p>

Table 44: Entrust digital ID for Windows Services settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Windows Service page > Number of attempts to retry if the server is unavailable	<p>Sets the number of times the Entrust Entelligence Windows Service Digital ID Service attempts to retry managing a service's digital ID when the server is unavailable. If the value is 0, after the first attempt fails, the service does not retry again. This setting is optional.</p> <p>Key: <ESP_registry_location> Value Name: ServiceRetryManagementOfflineAttempts Value Type: REG_DWORD Value Data: <0-n></p> <p>0 = After the first attempt fails, Security Provider does not retry again.</p> <p>Example:</p> <p>Value Data: 10</p> <p>The default is 5.</p> <p>Note: The Windows service's digital ID must be in the local service certificate store not the current user certificate store. The DN of the issuer of the service's digital ID should be the same as the one specified in the registry under the PKI registry key (in <ESP_registry_location>\PKI\<DN_of_CA>).</p>

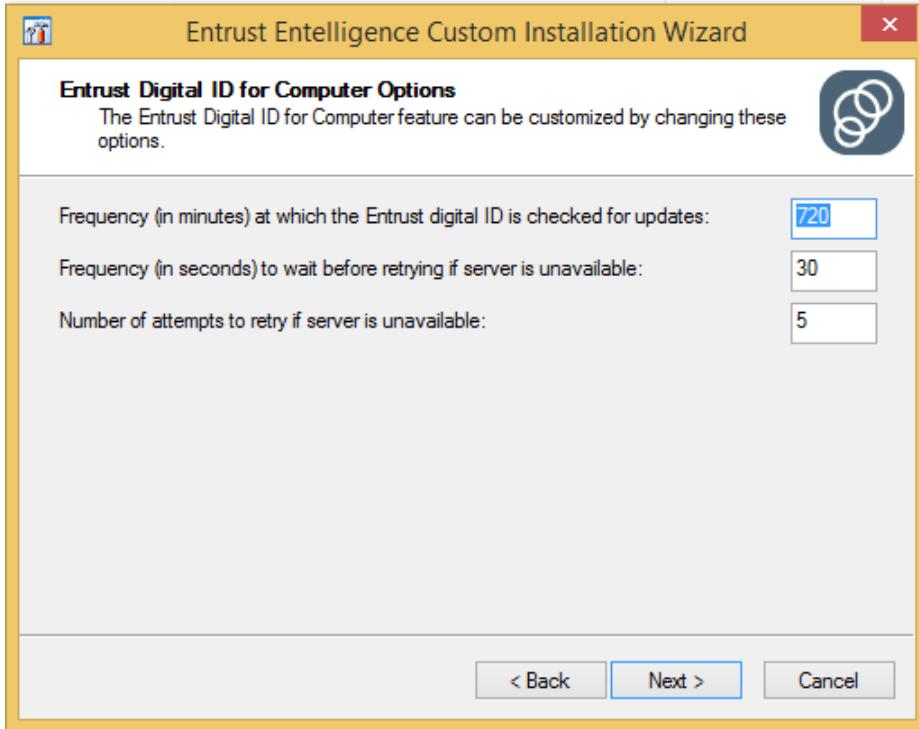
Entrust computer digital ID settings

If you use the **Custom Installation** wizard, Entrust computer digital ID settings are configurable through the **Entrust Digital ID for Computer Options** page (Figure 40).

Table 45 describes the “Entrust digital IDs for computer” settings.

The setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 40: Entrust digital ID for a computer page



The screenshot shows a window titled "Entrust Intelligence Custom Installation Wizard" with a close button in the top right corner. The main heading is "Entrust Digital ID for Computer Options". Below the heading is a descriptive text: "The Entrust Digital ID for Computer feature can be customized by changing these options." To the right of this text is a circular logo with three interlocking rings. The settings area contains three rows, each with a label and a text input field:

Setting	Value
Frequency (in minutes) at which the Entrust digital ID is checked for updates:	720
Frequency (in seconds) to wait before retrying if server is unavailable:	30
Number of attempts to retry if server is unavailable:	5

At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a blue border.

Table 45: Entrust digital ID for a computer settings

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Computer Options page > Frequency (in minutes) at which the Entrust digital ID is checked for updates	<p>Sets the interval at which Security Provider's Digital ID Monitor checks whether the computer certificates need to be updated. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: ComputerCertUpdateInterval Value Type: REG_DWORD Value Data: <0-n_minutes></p> <p>0 = Security Provider does not check for updates. Updates are only checked for if the administrator manually triggers an update from the MMC snap-in or if the service starts. Usually, the service only starts when the computer starts.</p> <p>Example:</p> <p>Value Data: 720</p> <p>The default is 720 minutes (12 hours).</p>

Table 45: Entrust digital ID for a computer settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Frequency (in seconds) to wait before retrying if server is unavailable	<p>Sets the interval in seconds at which Security Provider's Digital ID Monitor retries managing a computer's Entrust digital ID if it receives a Cannot Connect error code. This retry is particularly useful for VPN users who may log in to their security stores before creating their VPN connection. In this scenario, the first couple of management attempts may fail, but once the VPN connection is established, Security Provider can successfully check for updates.</p> <p>Note: The computer's digital ID must be in the local certificate store not the current user certificate store. The DN of the issuer of the computer's digital ID should be the same as the one specified in the registry under the PKI registry key (in <ESP_registry_location>\PKI\<DN_of_CA>).</p> <p>Key: <ESP_registry_location> Value Name: ComputerRetryManagementOfflineInterval Value Type: REG_DWORD Value Data: <0-n> seconds</p> <p>0 = Security Provider does not retry.</p> <p>Example: Value Data: 15</p> <p>The default is 30 seconds.</p>

Table 45: Entrust digital ID for a computer settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Digital ID for Users Options page > Number of attempts to retry if the server is unavailable	<p>Sets the number of times Security Provider's Digital ID Monitor attempts to retry managing a computer's digital ID when the server is unavailable. This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: ComputerRetryManagementOfflineAttempts Value Type: REG_DWORD Value Data: <0-n></p> <p>0 = After the first attempt fails, Security Provider does not retry again.</p> <p>Example:</p> <p>Value Data: 10</p> <p>The default is 5.</p> <p>Note: The computer's digital ID must be in the local certificate store not the current user certificate store. The DN of the issuer of the computer's digital ID should be the same as the one specified in the registry under the PKI registry key (in <ESP_registry_location>\PKI\<DN_of_CA>).</p>

Entrust security store settings

Entrust security store settings include:

- [“Entrust security store login settings” on page 396](#)
- [“Entrust security store creation settings” on page 405](#)
- [“Entrust security store startup and shutdown settings” on page 416](#)

Note: See also [“Entrust digital ID settings” on page 373](#).

Entrust security store login settings

If you use the **Custom Installation** wizard, login settings for Entrust security stores are configurable through the **Entrust Security Store Login Options** page (Figure 41).

Table 46 describes the login settings for Entrust security stores.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 41: Entrust Security Store Login Options page

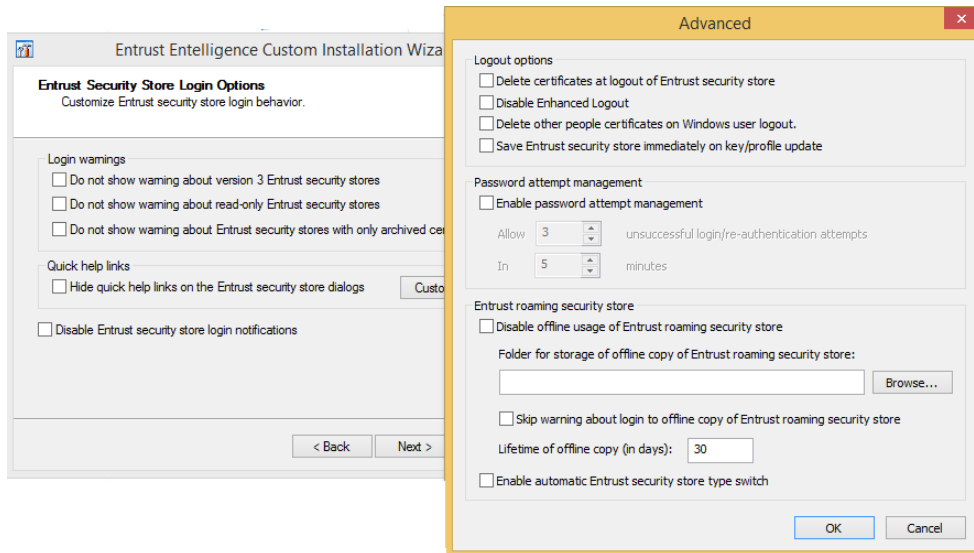


Table 46: Login settings specific to Entrust security stores

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Login Options page > Do not show warning about version 3 Entrust security stores	Hides the dialog box that appears after the user logs in to a v3 Entrust security store (.epf). This setting is optional. For details on v3 security stores, see “Entrust digital ID and security store versions and contents” on page 499 . This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: SkipNoCertHistoryNag Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Show the dialog box. 1 = Hide the dialog box.
Entrust Security Store Login Options page > Do not show warning about read-only Entrust security stores	Hides the dialog box that appears after the user logs in to a Entrust security store that is read-only. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: SkipReadOnlyEPFNag Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Show the dialog box. 1 = Hide the dialog box.
Entrust Security Store Login Options page > Do not show warning about Entrust security store with only archived certificates	Hides the dialog box that appears after the user logs in to a Entrust security store that only contains archived certificates. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: SkipArchivedCertsNag Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Show the dialog box. 1 = Hide the dialog box.

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Login Options page > Hide quick help links on the Entrust security store dialogs	<p>Hides the help links that appear on the left-hand side of Security Provider's Login, Unlock, and Authenticate dialog boxes.</p> <p>This setting is optional and maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: HideQuickLinks Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Show the help links. 1 = Hide the help links.</p>
Entrust Security Store Login Options page > Customize Links > Login, Unlock, ReAuthenticate tabs Entrust Authority Security Manager Entrust Authority Security Manager - Upgrade from Desktop Solutions Generic Certification Authority Custom	<p>Specifies which set of help links to show on the left-hand side of Security Provider's Login, Unlock, and Authenticate dialog boxes.</p> <p>The settings map to following registry values:</p> <p>Key: <ESP_registry_location>\EELS Value Name: LoginQuickLinks Value Type: REG_DWORD Value Data: <0-3></p> <p>Key: <ESP_registry_location>\EELS Value Name: UnlockQuickLinks Value Type: REG_DWORD Value Data: <0-3></p> <p>Key: <ESP_registry_location>\EELS Value Name: ReAuthQuickLinks Value Type: REG_DWORD Value Data: <0-3></p> <p>0 = Show custom links to your own help set. How to specify your links is described in the following row in this table.</p> <p>1 (default) = Show the Entrust Authority Security Manager link set. Use this if you deploy Entrust digital IDs.</p> <p>2 = Show the Entrust Authority Security Manager - Upgrade from Desktop Solutions link set. Use this if your users used Entrust Desktop Solutions in the past.</p> <p>3 = Show the Generic Certification Authority link set. Use this if you are importing third-party generated keys and certificates into an Entrust security store.</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Login Options page > Customize Links > Login tab > Custom > Add > Text Target	<p>Specifies a custom link text and link target for help links that appear on the left-hand side of Security Provider's Login, Unlock, and Authenticate dialog boxes. These settings take effect when you enable the custom link set, described in the previous table row.</p> <p>The settings in the Custom Installation wizard map to the following registry values:</p> <p>Key: <ESP_registry_location>\EELS Value Name: <Login_Unlock_ReAuth>QuickLink<n>Title Value Type: REG_SZ Value Data: <link_text></p> <p>Key: <ESP_registry_location>\EELS Value Name: <Login_Unlock_ReAuth>QuickLink<n>Target Value Type: REG_SZ Value Data: <link_target></p> <p><Login_Unlock_ReAuth> is replaced with the dialog box to which the link applies—either Login, Unlock, or ReAuth.</p> <p><n> is replaced with a number from 1 to 6. The numbers in the title and target for a particular link must match. Numbers are specified in sequence starting at 1, without skipping numbers.</p> <p><link_text> is the underlined link text.</p> <p><link_target> is any file that is executable by the Windows shell.</p> <p>The following is an example of how to set a custom help link on the Authenticate dialog box that reads “How to log in”:</p> <p>Key: <ESP_registry_location>\EELS Value Name: ReAuthQuickLink1Title Value Type: REG_SZ Value Data: How to log in</p> <p>Key: <ESP_registry_location>\EELS Value Name: ReAuthQuickLink1Target Value Type: REG_SZ Value Data: c:\program files\common files\entrust\esp\eelogin.exe</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>When this registry value is enabled (set to 1) enhanced logout is disabled. Enhanced logout support provides an automatic, orderly logout (or the login sequence is discontinued) if the Entrust security store detects the following:</p> <ul style="list-style-type: none">• a screen saver is activated• users lock their computer• users cancel a login sequence before completion (no error message is displayed) <p>Key: <ESP_registry_location>\EELS Value Name: DisableEnhancedLogout Registry Values: 0 or 1</p> <p>By default, this registry setting is not available.</p> <p>When this registry setting is unavailable or when its value is equal to 0, ESP enhanced logout is enabled.</p> <p>When this registry setting is set to 1, ESP enhanced logout is disabled.</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>These settings allow the administrator to replace the default help links that appear on the left side of the smart card login, authenticate and unblock pages a set of with custom links.</p> <p>The PIVCustomQuickLinkEnabled setting toggles between the custom and default links. For example, setting PIVCustomQuickLinkEnabled to 1 uses the custom links for all of the pages.</p> <p>Key: <ESP_registry_location> Value name: PIVCustomQuickLinkEnabled Type: DWORD Value: 0 uses the default links. 1 uses the custom links.</p> <p>The PIVCustomQuickLink<n>Title and PIVCustomQuickLink<n>Target are used together to create the custom link. Replace the <n> in the value with the number the reflects the order of the title on the page. For example, PIVCustomQuickLink1Title is the first link in the column. Numbers 1-6 are accepted. The numbering must be consecutive.</p> <p>To set the target for that link, replace the <n> with the same number in the PIVCustomQuickLink<n>Target registry setting. For example, the corresponding setting to PIVCustomQuickLink1Title is PIVCustomQuickLink1Target. The target can be any file that is executable by the Windows shell.</p> <p>Key: <ESP_registry_location> Value name: PIVCustomQuickLink<n>Title Type: string Value: <wording_of_the_link></p> <p>For example: Corporate password policy</p> <p>Key: <ESP_registry_location> Value name: PIVCustomQuickLink<n>Target Type: string Value: <any_file_that_is_executable_by_the_Windows_shell></p> <p>For example: c:\program files\common files\example\security_provider\pwpolicy.exe</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Login Options page > Advanced > Delete certificates at logout of Entrust security store	<p>Deletes all users' certificates in the Personal certificate store when users log out of their Entrust security stores (.epf).</p> <p>Note: EFS certificates are kept. The EFS certificate is left in the store to prevent the possibility of the EFS generating a self-signed certificate at the next login.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DeleteCertsAtLogout Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = keep user's certificates. 1 = delete user's certificates.</p> <p>Example: Value Data: 0</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting allows you to hide PIV smart card readers so that they do not appear in the Select Entrust Smart Card list.</p> <p>Key: <ESP_registry_location> Value Name: PIVHiddenReaders Value Type: REG_MULTI_SZ Value: the full name of the reader (with spaces) as it appears in the list</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Login Options page > Advanced > Enable password attempts management Allow <n> unsuccessful login or reauthentication attempts In <n> minutes	<p>Sets the number of bad login attempts to allow until the user successfully logs in to their Entrust security store for the first time.</p> <p>Note: If you use Security Manager, once the user logs in for the first time, the Managing bad login attempts and Login attempt window user policy settings configured in Security Manager are used.</p> <p>The setting maps to the following registry value:</p> <p>Key: HKEY_LOCAL_MACHINE\SOFTWARE\Entrust\ESP\EELS\PAM Value Name: Default Value Type: REG_BINARY Value Data: <numberofattempts_numberofminutes></p> <p>Example:</p> <p>Value Data: 03 00 00 00 3C 00 00 00</p> <p>The above value data indicates to allow 3 consecutive bad login attempts within 60 minutes.</p> <p>When set, the default is to allow 3 bad login attempts in 5 minutes.</p> <p>See “Managing login attempts” on page 252 and “Configuring password expiry times” on page 254 for information on configuring the user policy settings in Security Manager.</p>
Entrust Security Store Login Options page > Advanced > Disable offline usage of Entrust roaming security store	<p>Disables offline roaming for users with Entrust roaming security stores. If you activated offline roaming in Security Manager, the DisableOfflineRoaming setting takes effect. Otherwise, the DisableOfflineRoaming setting is ignored.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DisableOfflineRoaming Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Enable offline roaming. 1 = Disable offline roaming.</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Login Options page > Advanced > Folder for storage of offline copy of Entrust roaming security store	<p>Specifies a default folder for storing a user's offline Entrust roaming security store, if different from the <code>DefaultFolder</code> setting. The setting can contain environment strings in the form of <code>%XXX%</code> and they are expanded. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <code><ESP_registry_location></code> Value Name: <code>OfflineRoamingFolder</code> Value Type: <code>REG_SZ</code> Value Data: <code><path_of_offline_roaming_folder></code></p> <p>Example:</p> <p>Value Data: <code>%USERPROFILE%\EPF</code></p>
Entrust Security Store Login Options page > Advanced > Skip warning about login to offline copy of Entrust roaming security store	<p>Hides the dialog box that appears after the user logs in to the offline Entrust roaming security store. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <code><ESP_registry_location></code> Value Name: <code>SkipOfflineRoamingNag</code> Value Type: <code>REG_DWORD</code> Value Data: <code><0-1></code></p> <p>0 (default) = Show the dialog box. 1 = Hide the dialog box.</p>
Entrust Security Store Login Options page > Advanced > Lifetime of offline copy (in days)	<p>Specifies the length of time in days that the offline Entrust roaming security store is valid for. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <code><ESP_registry_location></code> Value Name: <code>OfflineRoamingLifetime</code> Value Type: <code>REG_DWORD</code> Value Data: <code><number_of_days></code></p> <p>Example:</p> <p>Value Data: 7</p> <p>The default is 30 days.</p>

Table 46: Login settings specific to Entrust security stores (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>When this key is set to 1, users can log in to a read-only Entrust security store (.epf) even after the password expires.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: AllowLoginToReadOnlyExpiredEPF Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Users logging in to a read-only Entrust security store with an expired password are prompted to change their password. That action is not possible in this case.</p> <p>1 = Users logging in to a read-only Entrust security store with an expired password are allowed access and not prompted to change their password.</p> <p>Example: Value Data: 1</p>

Entrust security store creation settings

If you use the **Custom Installation** wizard, settings related to Entrust security store creation are configurable through the **Entrust Security Store Creation Options** page (Figure 42).

Table 47 describes the settings related to Entrust security store creation.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 42: Entrust Security Store Creation Options page

The image shows the 'Entrust Security Store Creation Options' window with the 'Advanced' dialog box open. The main window has a title bar 'Entrust Intelligence Custom Install' and a subtitle 'Entrust Security Store Creation Options'. It contains several sections: 'Entrust security store folder' with a 'Default folder:' text box and a checkbox 'Force users to use default Entrust security store folder'; 'Entrust security store name' with a checkbox 'Force users to use default Entrust security store name' and a label 'Read the Entrust security store name from DN attribute:'; and 'Default Entrust security store timeout (in minutes):'. The 'Advanced' dialog box has a title bar 'Advanced' and a close button. It contains a section 'CA certificates to import' with two checkboxes: 'Import previous CA certificates' (checked) and 'Import CA certificates from non-verification certificate'. Below this is a warning icon and text: 'The below policies for an Entrust security store only apply if Entrust Authority Security Manager is not being used.' The 'Password Policy' section includes 'Minimum number of characters:' (8), 'Maximum number of characters:' (0), three checkboxes for 'Must contain uppercase character', 'Must contain lowercase character', and 'Must contain digit' (all checked), 'Must contain non-alphanumeric character' (unchecked), 'Password lifetime (in weeks):' (0), and 'Number of previous passwords to be checked:' (0). The 'Timeout Policy' section has 'Maximum timeout (in minutes):' (15). The 'Protection Policy' section has 'Encryption algorithm:' set to 'CAST-128'. At the bottom are 'OK' and 'Cancel' buttons.

Entrust Intelligence Custom Install

Entrust Security Store Creation Options
Customize options for new Entrust security stores.

Entrust security store folder
Default folder:
☐ Force users to use default Entrust security store folder

Entrust security store name
☐ Force users to use default Entrust security store name
Read the Entrust security store name from DN attribute:
Default Entrust security store timeout (in minutes):

< Back

Advanced

CA certificates to import
☒ Import previous CA certificates
☐ Import CA certificates from non-verification certificate

The below policies for an Entrust security store only apply if Entrust Authority Security Manager is not being used.

Password Policy
Minimum number of characters:
Maximum number of characters:
☒ Must contain uppercase character
☒ Must contain lowercase character
☐ Must contain non-alphanumeric character
☒ Must contain digit
Password lifetime (in weeks):
Number of previous passwords to be checked:

Timeout Policy
Maximum timeout (in minutes):

Protection Policy
Encryption algorithm:

OK Cancel

Table 47: Entrust security store creation settings

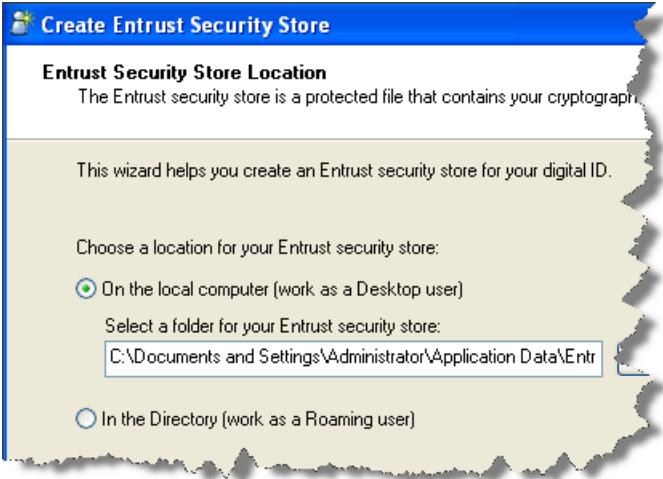
Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Configures the type of Entrust security store (roaming or desktop) selected by default when users recover or enroll for an Entrust security store.</p> <div></div> <p>This setting only applies if your End User Policy permits both roaming and desktop security stores. If your End User Policy only permits one type of security store, then Security Provider will create that security store type without prompting the user to choose.</p> <p>This setting maps to the following registry value:</p> <p>Key:<ESP_registry_location> Value Name:DefaultEntrustSecurityStoreType Value Type: REG_DWORD Value Data:<0-1></p> <p>0 (default) = Entrust desktop security store is selected by default. 1 = Entrust roaming security store is selected by default.</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Default folder	<p>Specifies the name and path of a default folder for storing Entrust desktop security stores (.epf files). The setting can contain environment strings in the form of %XXX% and they are expanded. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DefaultFolder Value Type: REG_SZ Value Data: <path_of_default_folder></p> <p>Example:</p> <p>Value Data: %USERPROFILE%\EPF</p>
Entrust Security Store Creation Options page > Force users to use default Entrust security store folder	<p>Locks the value of the DefaultFolder setting, so users cannot choose the location for their Entrust security store (.epf file). The path is grayed out in the GUI. If a user switches from roaming to a desktop user, the Entrust security store is created in this location. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FolderLocked Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Folder path is configurable through a Browse button. 1 = Folder path is locked and grayed out in the GUI.</p> <p>Example:</p> <p>Value Data: 1</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Force users to use default Entrust security store name	<p>Locks the Entrust security store name to either the Windows user name or the user's DN attribute (if you specify to read the name from a DN attribute). The name is locked on the enroll and recover wizards so that users cannot change it.</p> <p>This setting locks the name of all Entrust security stores, regardless of the CA they are associated with. See also the <code>EPFNameLocked</code> setting (described in the following table row), which allows you to lock names on a per-CA basis. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: NameLocked Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = The default Windows user name appears in an editable field.</p> <p>1 = The default Windows user name is grayed out.</p> <p>Desktop Entrust security store names cannot contain the following characters: \ / : * ? " < > ' . Roaming Entrust security store names cannot contain the following characters: \ / : * ? " < > ' { } [] ^ ~ ' .</p>
Entrust Security Store Creation Options page > You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>When a user is presented with a suggested name for their Entrust security store during the enrollment or recovery process, you can have a preset value automatically appended to the name. You can configure this string for each CA so that a different appended name appears for each CA for a user. The resulting name has this syntax: <username>_<appended-name>.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>PKI\<DN_of_CA> Value Name: AppendToEPFName Value Type: REG_SZ Value Data: <appended_name></p> <p>Example:</p> <p>Value Data: _US</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Read the Entrust security store name from DN attribute	<p>Instead of using the Windows user name as the default Entrust security store name in the enroll and recover wizards, you can use a value read from a DN attribute that you specify instead. For example, you can read the name from the <code>cn</code> attribute. This setting is optional, and must be specified as an OID.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: EPFNameFromDNAttribute Value Type: REG_SZ Value Data: <OID_for_user_RDN_attribute></p> <p>Examples:</p> <p>Value Data: 2.5.4.3 (for <code>cn</code>) Value Data: 2.5.4.45 (for <code>UID</code>)</p> <p>Note: If you want to have complete control over which name is presented, you can write your own DLL to set the name, and then have Security Provider for Windows read in the name from this DLL. For more information, see the <i>Entrust Entelligence Security Provider 9.2 for Windows - Customizing the Entrust security Store Login Service White Paper</i>.</p>
Entrust Security Store Creation Options page > Default Entrust security store timeout (in minutes)	<p>Specifies the default timeout for Entrust security stores after which users must log in again. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DefaultEntrustSecurityStoreTimeout Value Type: REG_DWORD Value Data: <timeout_in_minutes></p> <p>The default is 5 minutes.</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Advanced > Minimum number of characters	<p>Specifies the minimum number of characters allowed in the user's Entrust security store password.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordMinLength Value Type: REG_DWORD Value Data: <number></p> <p>The default is 6.</p>
Entrust Security Store Creation Options page > Advanced > Maximum number of characters	<p>Specifies the maximum number of characters allowed in the user's Entrust security store password.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordMaxLength Value Type: REG_DWORD Value Data: <number></p> <p>The default is to allow any length.</p>
Entrust Security Store Creation Options page > Advanced > Must contain upper character	<p>Specifies whether an uppercase character is required in the user's Entrust security store password.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordMustContainUpper Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = Do not require an uppercase character. 1 (default) = Requires an uppercase character.</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Advanced > Must contain lower character	<p>Specifies whether a lowercase character is required in the user's Entrust security store password.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordMustContainLower Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = Do not require a lowercase character. 1 (default) = Requires a lowercase character.</p>
Entrust Security Store Creation Options page > Advanced > Must contain non alphanumeric character	<p>Specifies whether an non-alphanumeric character (not A,a–Z,z,0–9) is required in the user's Entrust security store password.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordMustContainNonAlphanumeric Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = Do not require a nonalphanumeric character. 1 (default) = Requires a nonalphanumeric character.</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Advanced > Must contain digit	<p>Specifies whether a digit (0–9) is required in the user’s Entrust security store password.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager’s user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordMustContainDigit Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = Do not require a digit. 1 (default) = Requires a digit.</p>
Entrust Security Store Creation Options page > Advanced > Password lifetime (in weeks)	<p>Specifies a number of weeks after which the user’s Entrust security store password expires.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager’s user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: PasswordLifetime Value Type: REG_DWORD Value Data: <number_of_weeks></p> <p>The default is 0 (never expires).</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Advanced > Number of previous passwords to be checked	<p>Specifies a number of old passwords that the current Entrust security store password must not match. For example, if you specify 2, then the password being set cannot match the one being replaced or the password before that; however, it can match a three-times-removed password.</p> <p>If the Data Value is set to 0, no password history is enforced.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: NumOfPreviousPasswordsToBeChecked Value Type: REG_DWORD Value Data: <number></p> <p>The default is 5. The maximum is 8.</p>
Entrust Security Store Creation Options page > Advanced > Maximum timeout (in minutes)	<p>Specifies the timeout (in minutes) for the Entrust security store, regardless of when the digital ID was last used.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the password policy is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: MaxEntrustSecurityStoreTimeout Value Type: REG_DWORD Value Data: <number_of_minutes></p> <p>The default is 15.</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Creation Options page > Advanced > Encryption algorithm	<p>Specifies the algorithm to use to encrypt the Entrust security store. The algorithm can be either CAST-128 or Triple DES.</p> <p>Note: This setting applies to non-Entrust digital IDs stored in an Entrust security store. If you deploy Entrust digital IDs, the encryption algorithm is set through Security Manager's user policy, and this setting is ignored.</p> <p>Key: <ESP_registry_location> Value Name: EPFEncryptionAlgorithm Value Type: REG_SZ Value Data: <CAST_or_TRIPLE-DES></p> <p>Acceptable values:</p> <ul style="list-style-type: none"> • CAST (default) • TRIPLE-DES <p>Example: Value Data:TRIPLE-DES</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Locks the Entrust security store name to either the Windows user name or the user's DN attribute (if you specify to read the name from a DN attribute).</p> <p>This setting locks the name of an Entrust security store that is specific to a particular CA. Any Entrust security stores that are not associated with that particular CA are not affected by this setting.</p> <p>This setting is optional and maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: EPFNameLocked Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = The default Windows user name appears in an editable field. Users belonging to the CA specified in <ESP_registry_location>\PKI\<DN_of_CA> can change the name.</p> <p>1 = The default Windows user name is grayed-out. Users belonging to the CA specified in <ESP_registry_location>\PKI\<DN_of_CA> cannot change the name.</p> <p>Desktop Entrust security store names cannot contain the following characters: \ / : * ? " < > ' . Roaming Entrust security store names cannot contain the following characters: \ / : * ? " < > ' { } [] ^ ~ ' .</p>

Table 47: Entrust security store creation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Determines where to place intermediate CA certificates in the Entrust Security Store (.epf file). The default is to place intermediate certificates in two locations: in the [Subordinate CA Certificates] section and the [Intermediate CA Certificates] section. This dual locality is necessary to enable backwards compatibility with pre-9.1 versions of Security Provider. If backwards compatibility is not a concern, then you can have intermediate CA certificates placed in the [Intermediate CA Certificates] section only. Having the certificate in a single location makes the .epf file smaller. Other than a smaller file size, there are no other benefits to changing this setting from its default.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DisableEPFSubCACertsCompatibility Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Enables backwards compatibility. Intermediate CA certificates are written to the [Subordinate CA Certificates] and [Intermediate CA Certificates] sections of the Entrust security store.</p> <p>1 = Disables backwards compatibility. Intermediate CA certificates are written to the [Intermediate CA Certificates] section only.</p> <p>Example: Value Data: 1</p>

Entrust security store startup and shutdown settings

If you use the **Custom Installation** wizard, startup and shutdown settings for Entrust security stores are configurable through the **Entrust Security Store Startup/Shutdown Options** page (Figure 43).

Table 48 describes the startup and shutdown settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 43: Entrust security store startup and shutdown options page

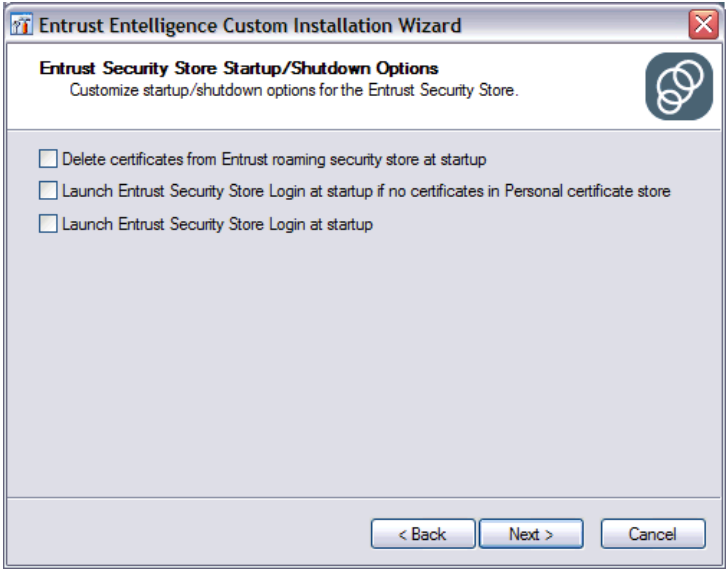


Table 48: Entrust security store startup and shutdown settings

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Startup/Shutdown Options page > Delete certificates from Entrust roaming security store at startup	<p>Deletes all the user's Entrust roaming security store certificates that are in the Personal certificate store when the user logs in to the Windows operating system. This setting is optional.</p> <p>Note: The taskbar status icon subfeature must be installed for this feature to work. See "Taskbar status icon" on page 55 for more information.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DeleteRoamCertsAtStartup Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Keep roaming certificates. 1 = Delete roaming certificates.</p>

Table 48: Entrust security store startup and shutdown settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust Security Store Startup/Shutdown Options page > Launch Entrust security store login at startup if no certificates in Personal certificate store	<p>Displays the Entrust security store login dialog box immediately after a Windows login if no certificates exist in their Personal certificate store. For example, when roaming users log out of their Entrust security stores and then try to start up a new session, their Entrust security stores are deleted from the Microsoft certificate store at startup. With this setting activated, these users are then prompted to log in with their Entrust security store located in the directory. This setting is optional.</p> <p>Note: The taskbar status icon subfeature must be installed for this feature to work. See “Taskbar status icon” on page 55 for more information.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: PromptIfNoCertificatesAtStartup Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = No prompt. 1 = Prompt.</p>
Entrust Security Store Startup/Shutdown Options page > Launch Entrust security store login at startup	<p>Displays the Entrust security store login dialog box immediately after a Windows login. This setting is optional.</p> <p>Note: In order to display the login dialog box, Security Provider's taskbar status icon must be activated.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: PromptForSecurityStoreLoginAtStartup Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Do not display the login dialog box. 1 = Display the login dialog box.</p>

CRL Revocation Provider settings

If you use the **Custom Installation** wizard, most CRL Revocation Provider settings are configurable through the **CRL Revocation Provider Options** page (Figure 44).

Table 49 describes the CRL Revocation Provider settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?”](#) on page 329.

Figure 44: CRL Revocation Provider Options page

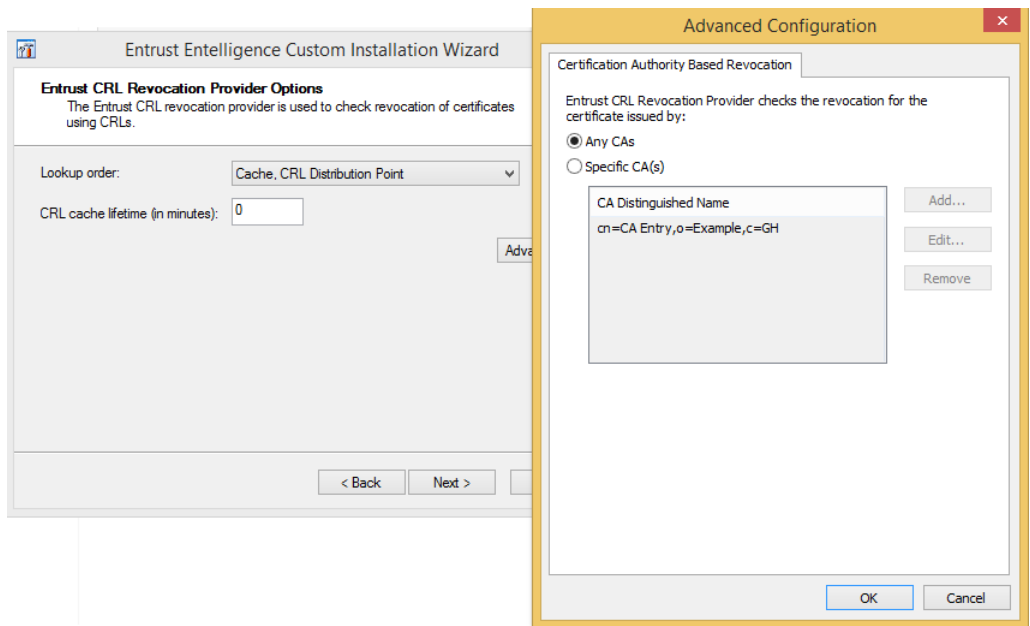


Table 49: CRL Revocation Provider settings

Setting name and location in Custom Installation wizard	Description and registry value
CRL Revocation Provider page > Advanced > Certification Authority Based Revocation	<p>The registry setting can specify different options for multiple entries. This allows administrators to configure a specific option for each CA in the event of cross certification, or with respect to the root and any implicit trusts (cross certificate, link certificate, intermediate certificate). So, for example there may be different CRL revocation options for the root and intermediate certificates.</p> <p>Key: <ESP_registry_location>\Revocation Value Name: <CA's Distinguished Name> Value Type: REG_DWORD Value Data: <0, 1, 2></p> <p>0 - (Default) The certificate issued by this CA's DN will be checked for revocation using the ESP CRL Revocation Provider.</p> <p>1 - The certificate issued by this CA's DN will be checked for revocation using the ESP OCSP Revocation Provider.</p> <p>2 - The certificate issued by this CA's DN will be checked for revocation using both revocation providers.</p> <p>When you install both revocation providers, the OCSP revocation provider is always used to check for revocation first. If the OCSP Revocation Provider fails, revocation checking passes to the CRL Revocation Provider.</p>

Table 49: CRL Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
CRL Revocation Provider page > Lookup Order	<p>Enables checking of the local Certificate Revocation List (CRL) in the CRL store. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: EnableCRLCache Value Type: REG_DWORD Value Data: <0-2></p> <p>0 = CRL Distribution Point Only. Always fetch the CRL from the CRL Distribution Point (CDP); never use locally cached information, even if offline.</p> <p>1 (default) = Cache, CRL Distribution Point. Check the local cache for previous revocation information before fetching the CRL from the CDP. This option results in quick revocation checks.</p> <p>2 = CRL Distribution Point, Cache. Fetch the CRL from the CDP but use the local cache if offline.</p> <p>Example:</p> <p>Value Data: 1</p>
CRL Revocation Provider page > CRL Cache Lifetime (in minutes)	<p>Specifies the validity period (in minutes) of the cached CRL after which it expires. Works in conjunction with the EnableCRLCache setting if a cache is used.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: CRLCacheLifetime Value Type: REG_DWORD Value Data: <number_of_minutes></p> <p>Example:</p> <p>Value Data: 60</p> <p>0 (zero) indicates that the cached copy is good for the lifetime specified in the CRL.</p>

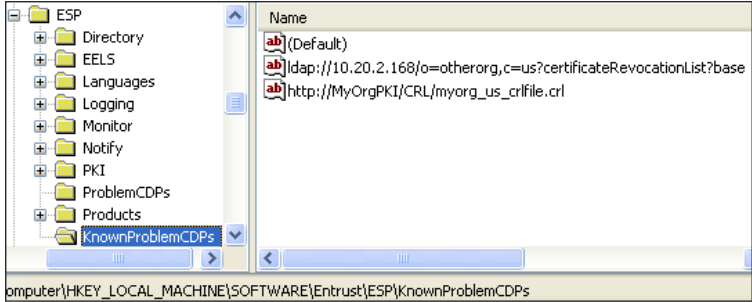
Table 49: CRL Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>You can direct the CRL Revocation Provider to skip CDP entries that use the directory name format if another format is available. Such CDP entries point to partitioned CRLs instead of the larger combined CRL. Skipping partitioned CRLs might better fit the needs of a high-volume application doing revocation checks. The setting applies on a per-CA basis.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\PKI\<DN_of_CA> Value Name: SkipDirectoryNameInCDP Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Do not skip CDP entries. 1 = Skip CDP entries that use the directory name format when applicable.</p> <p>Example: Value Data: 1</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Sets a timeout value for FTP connection requests. If a connection request takes longer than this timeout value, (for example, the computer is offline) the request is canceled. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FTPConnectTimeLimit Value Type: REG_DWORD Value Data: <time-out_in_seconds></p> <p>The default is 5 seconds.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Sets a timeout value for file-based repository connection requests. If a connection request takes longer than this timeout value, the request is canceled. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FileConnectTimeLimit Value Type: REG_DWORD Value Data: <time-out_in_seconds></p> <p>The default is 5 seconds.</p>

Table 49: CRL Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Sets the interval the CRL Revocation Provider waits to download a new CRL when the previous CRL download fails. When Security Provider detects a problem with a downloaded CRL, it rejects it. The CRL Revocation Provider downloads the CRL again after a set period. The default is 5 minutes. Set the time interval in <code>ProblemCDPCacheLifetime</code> to wait before another download attempt. In the interval, Security Provider uses the last cached CRL.</p> <p>You can set a maximum value of 4294967296 minutes. The default is 5 minutes.</p> <p>Take care not to make the period too short. If a retrieval problem occurs and persists, it can lead to repeated, closely-timed attempts to download a good CRL. This can cause performance problems for users, such as long waits to open encrypted email.</p> <p>This registry value interacts with a second key described below:</p> <p>Key: <code><ESP_registry_location></code> Value Name: <code>ProblemCDPCacheLifetime</code> Value Type: <code>REG_DWORD</code> Value Data: <code><number_of_minutes></code></p> <p>When the CRL Revocation Provider fails to download a valid CRL, it writes the time and reason at the following registry key:</p> <p>Key: <code>HKEY_CURRENT_USER\SOFTWARE\Entrust\ESP\ProblemCDPs</code> Value Name: <code><location to put failure information></code> Value Type: <code>REG_SZ</code> Value Data: <code><failure_details></code></p> <p>Example:</p> <p>Value Data: <code>Offline\20081009175742Z</code></p> <p>Reasons for failure include the following:</p> <ul style="list-style-type: none">OfflineUntrustedUnsupported CRL FormatDelta CRLUnrecognized CRL ExtensionAll Reason Codes Not CoveredNot FoundReceive FailureSend Request Failure

Table 49: CRL Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Specifies CRL Distribution Points (CDPs) that you want Security Provider for Windows to ignore. Security Provider never attempts connections to these CDPs.</p> <p>Use this registry key to specify problematic CDPs, for example, ones that include CRL URLs that do not work.</p> <p>This setting maps to the following registry key:</p> <p>Key: <ESP_registry_location>\KnownProblemCDPs Value Name: <CDP_URL> Value Type: REG_SZ Value Data: <none></p> <p>Create one registry entry per CDP. For example, when you specify two problem CDPs, your registry looks similar to this:</p> 

OCSP Revocation Provider settings

If you use the **Custom Installation** wizard, OCSP Revocation Provider settings are configurable through the **OCSP Revocation Provider Options** page (Figure 45).

Table 50 describes the OCSP settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?”](#) on page 329.

- Note: Other OCSP settings are available. For details, see:
 - [“CA-specific OCSP Responder settings”](#) on page 367
 - [“HTTP connection and timeout settings”](#) on page 476
 - [“Logging settings”](#) on page 489

Figure 45: OCSP Revocation Provider Options page

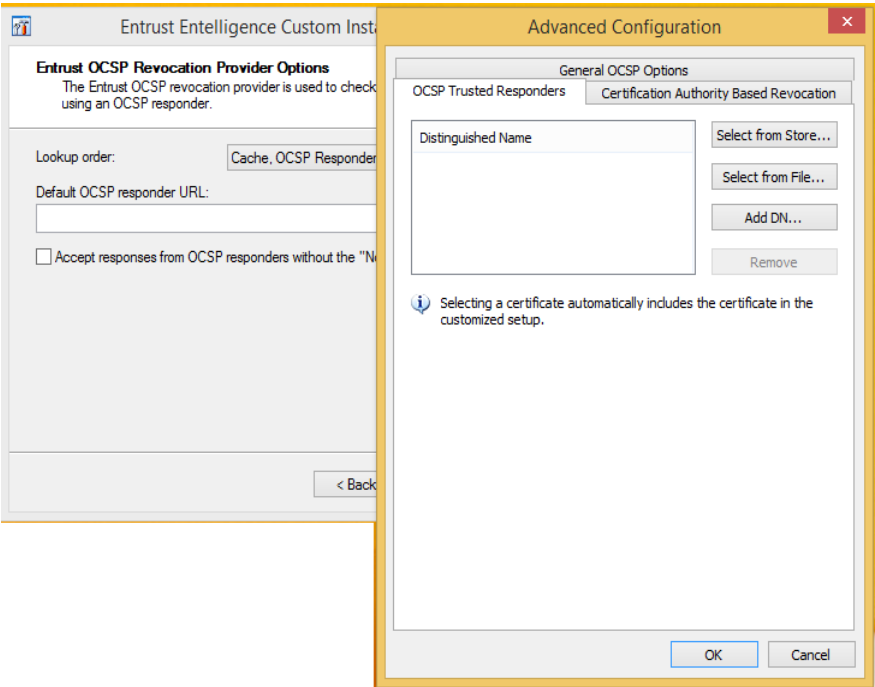


Table 50: OCSP Revocation Provider settings

Setting name and location in Custom Installation wizard	Description and registry value
OCSP Revocation Provider page > Advanced > Certification Authority Based Revocation	<p>The registry setting can specify different options for multiple entries. This allows administrators to configure a specific option for each CA in the event of cross certification, or with respect to the root and any implicit trusts (cross certificate, link certificate, intermediate certificate). So, for example there may be different CRL revocation options for the root and intermediate certificates.</p> <p>Key: <ESP_registry_location>\Revocation Value Name: <CA's Distinguished Name> Value Type: REG_DWORD Value Data: <0, 1, 2></p> <p>0 - (Default) The certificate issued by this CA's DN will be checked for revocation using the ESP CRL Revocation Provider.</p> <p>1 - The certificate issued by this CA's DN will be checked for revocation using the ESP OCSP Revocation Provider.</p> <p>2 - The certificate issued by this CA's DN will be checked for revocation using both revocation providers.</p> <p>When you install both revocation providers, the OCSP revocation provider is always used to check for revocation first. If the OCSP Revocation Provider fails, revocation checking passes to the CRL Revocation Provider.</p>

Table 50: OCSP Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
OCSP Revocation Provider page > Lookup Order	<p>You can configure the OCSP Revocation Provider to either</p> <ul style="list-style-type: none">• contact the OCSP responder to get a response or• use a cached response <p>This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: EnableOCSPCache Value Type: REG_DWORD Value Data: <0-2></p> <p>0 = OCSP Responder Only. The OCSP Revocation Provider directly contacts the OCSP responder to get a response every time the client requests the status of the certificate.</p> <p>1 (default) = Cache, OCSP Responder. The OCSP Revocation Provider uses the cached OCSP response until it expires. When the cached response expires, the OCSP Revocation Provider contacts the OCSP responder to get a response, validates it, and then caches a successfully validated response.</p> <p>2 = OCSP Responder, Cache. The OCSP Revocation Provider directly contacts the OCSP responder to get a response first. If the server is offline or it cannot retrieve the response from the server, the cached response is used if it is valid.</p>
OCSP Revocation Provider page > Default OCSP Responder URL	<p>Sets the URL for the default OCSP Responder in HTTP or HTTPS format. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DefaultOCSPResponderURL Value Type: REG_SZ Value Data: <URL_of_Responder></p>

Table 50: OCSP Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
OCSP Revocation Provider page > Accept responses from OCSP responders without the NoCheck extension	Forces the OCSP Revocation Provider to accept a response even if the responder's certificate is missing the NoCheck extension. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: OCSPAcceptMissingNoCheckExtension Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Reject the response if responder's certificate is missing the NoCheck extension. 1 = Accept the response.
OCSP Revocation Provider page > Advanced Configuration > General OCSP Options tab > Enable nonce support in OCSP requests	Causes the OCSP Revocation Provider to place a nonce consisting of a random sequence of 20 bytes in its requests. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: OCSPEnableNonce Value Type: REG_DWORD Value Data: <0-n> 0 (default) = The nonce is not included. 1 or greater = The OCSP Revocation Provider always generates a nonce and places it in the OCSP request.
OCSP Revocation Provider page > Advanced Configuration > General OCSP Options tab > OCSP cache store interval	Determines the interval at which the OCSP cache stores are checked for updates. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: OCSPCacheStoreUpdateInterval Value Type: REG_DWORD Value Data: <interval_in_minutes> Example: Value Data: 1440 The default is 1440 minutes (24 hours).

Table 50: OCSP Revocation Provider settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
OCSP Revocation Provider page > Advanced Configuration > OCSP Trusted Responders tab > Distinguished Name	Lists the DNs belonging to trusted OCSP Responders. The DNs are listed in each responder's certificate. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: OCSPTrustedResponders Value Type: REG_SZ Value Data: <Responder_1_DN>; <Responder_2_DN>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Determines the validity period of the OCSP response if the nextUpdate field is not present in the OCSP basic response. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: OCSPAllowableInterval Value Type: REG_DWORD Value Data: <minutes> Example: Value Data: 1440 The default is 1440 minutes (24 hours).

Entrust File Security settings

If you use the **Custom Installation** wizard, File Security settings are configurable through the **Entrust File Security Options** page (Figure 46).

Table 51 describes the file security settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Figure 46: Entrust File Security Options page

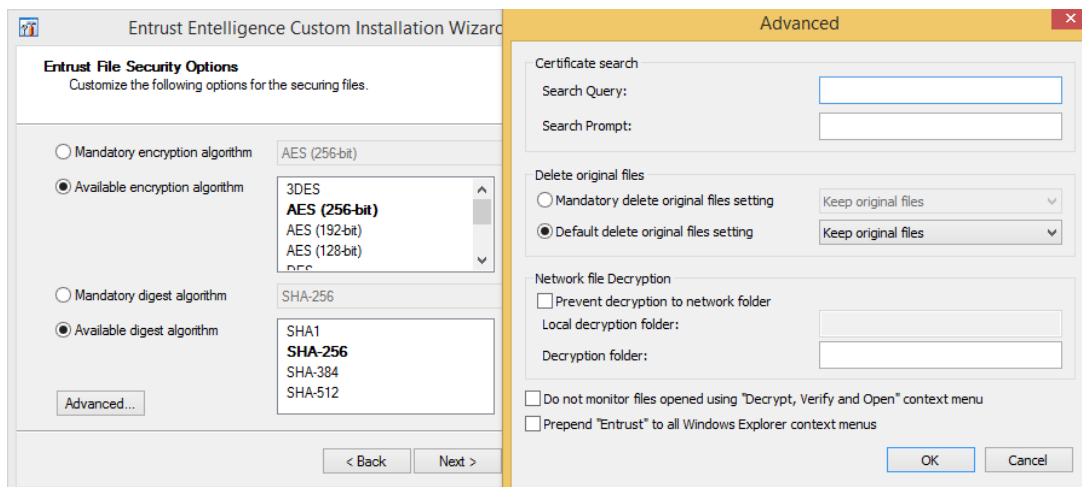


Table 51: Entrust File Security settings

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Mandatory encryption algorithm	<p>Specifies an encryption algorithm and grays it out in the wizards so that the user cannot change it. If you do not specify this setting, Security Provider uses the default encryption algorithm (FileEncryptionAlgorithmDefault) setting instead.</p> <p>This setting maps to two registry values:</p> <p>Key: <ESP_registry_location> Value Name: FileEncryptionAlgorithm Value Type: REG_DWORD Value Data: <string></p> <p>Acceptable values are:</p> <p>6603 (3DES) 6601 (DES) 6602 (RC2)* 6606 (CAST)* 6605 (IDEA)* 6611 (AES)*</p> <p>Example:</p> <p>Value Data:6603 Base: Hexadecimal</p> <p>*These algorithms have a corresponding length governed by FileEncryptionAlgorithmLength. The hexadecimal number set in the registry is the value for the combination of algorithm and key length and therefore may not be the value listed here (for example, AES is 6611 and AES256 is 6610).</p> <p>Key: <ESP_registry_location> Value Name: FileEncryptionAlgorithmLength Value Type: REG_DWORD Value Data: <Length_specific_to_algorithm></p> <p>256, 192, 128 (AES) 128, 80, 64, 40 (CAST) 128, 64, 56, 40 (RC2) 128 (IDEA)</p> <p>Example:</p> <p>Value Data: 256</p> <p>The key length value is displayed in the registry in the format <hexadecimal_value_of_length> (<value_in_decimal_notation>)</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Available encryption algorithm>	<p>Sets which encryption algorithms appear in a list of algorithms available to users. Use this setting to reduce the default list of algorithms. Users can select any algorithm in the list. The list is available only when Mandatory encryption algorithm (FileEncryptionAlgorithm) is not set.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name:AllowedFileEncryptionAlgorithms Value Type: REG_SZ Value Data: <string></p> <p>Acceptable values are:</p> <p>6603 (3DES) 6601 (DES) 6602 (RC2) 6606 (CAST) 6605 (IDEA) 6611 (AES)</p> <p>List the values separated by semicolons. Where applicable, the hexadecimal values can include a bit size value preceded by a colon.</p> <p>Example:</p> <p>Value Data: 6603; 6611:256</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Available encryption algorithm (set as the default using the Default button)	<p>Sets which encryption algorithm appears first in the list of available algorithms in the wizards. Users can then change the algorithm to any available on their system. To prevent users from changing the default algorithm, instead use the Mandatory encryption algorithm (FileEncryptionAlgorithm) setting. To limit users to a subset of algorithms available on their system, use Available encryption algorithm (AllowedFileEncryptionAlgorithms) instead.</p> <p>This setting maps to two registry values:</p> <p>Key: <ESP_registry_location> Value Name: FileEncryptionAlgorithmDefault Value Type: REG_DWORD Value Data: <string></p> <p>Acceptable values are:</p> <p>6603 (3DES) (Default) 6601 (DES) 6602 (RC2)* 6606 (CAST)* 6605 (IDEA)* 6611 (AES)*</p> <p>Example:</p> <p>Value Data: 6603 Base: Hexadecimal</p> <p>**These algorithms have a corresponding default length set by FileEncryptionAlgorithmLengthDefault.</p> <p>Key: <ESP_registry_location> Value Name: FileEncryptionAlgorithmLengthDefault Value Type: REG_DWORD Value Data: <String></p> <p>Acceptable values are:</p> <p>256, 192, 128 (AES) 128, 80, 64, 40 (CAST) 128, 64, 56, 40 (RC2) 128 (IDEA)</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Mandatory digest algorithm	<p>Specifies a hashing algorithm (used for signing) and grays it out in the wizards so that users cannot change it.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FileHashAlgorithm Value Type: REG_DWORD Value Data: <string></p> <p>Acceptable values are:</p> <p>8004 (SHA1) 800C (SHA 256) (default) 800D (SHA 384) 800E (SHA 512)</p> <p>Example:</p> <p>Value Data: 800C Base: Hexadecimal</p>
Entrust File Security Options page > Available digest algorithm	<p>Sets which hashing algorithms appear in a list of algorithms available to users. Use this setting to reduce the default list of algorithms. Users can select any algorithm in the list. The list is available only when Mandatory digest algorithm (FileHashAlgorithm) is not set.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: AllowedFileHashAlgorithms Value Type: REG_SZ Value Data: <string></p> <p>Acceptable values are:</p> <p>8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512)</p> <p>List the values separated by semicolons.</p> <p>Example:</p> <p>Value Data: 800C; 800D</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Advanced > Search Query	<p>Sets the LDAP search filter used when searching directories for certificates. For a complete description of the search filter format, see RFC 2254 available from the IETF Web site.</p> <p>The attributes set here appear when users use the Search for People dialog box in the Entrust Certificate Explorer (and various wizards). This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FileEncryptionSearchQuery Value Type: REG_SZ Value Data: " (<attribute>=%1!s!*) "</p> <p>The default is: " (& ((cn=%1!s!*) (mail=%1!s!*)) ((userCertificate=*) (userCertificate;binary=*))) "</p> <p>where:</p> <ul style="list-style-type: none"> • %1!s! is a placeholder for the user-entered text • & indicates AND logic • indicates OR logic • asterisks (*) allow users to perform wildcard searches with or without typing in the asterisk (if the user enters *, it is redundant and not used) <p>Be careful when using asterisks (*), especially at the beginning of a search string, as this can cause excessive returns due to substring matches and slowness from the directory.</p> <p>Attributes can be any defined in the directory. Examples include:</p> <ul style="list-style-type: none"> • cn (common name) • sn (surname) • userCertificate (all the user's certificate details - this can be several KB in size) • mail (email) <p>Note: Both userCertificate and userCertificate;binary are used by default to cover the format of various directories.</p> <p>Examples:</p> <p>"& ((cn=%1!s!*) (sn=%1!s!*) (mail=%1!s!*) " searches on common name, surname, and email address</p> <p>"& ((mail=%1!s!*) " searches on email address only</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Advanced > Mandatory delete original files setting	<p>Forces the deletion or preservation of the original plaintext files after an encryption operation. If you do not specify a value for this setting, Security Provider uses the Default delete original files setting (FileDeletePlainTextDefault) setting instead.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FileDeletePlainText Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Disables and grays out the Delete the original files on finish check box and forces the preservation of plaintext files.</p> <p>1 = Enables and grays out the Delete the original files on finish check box and forces the deletion of plaintext files.</p>
Entrust File Security Options page > Advanced > Default delete original files setting	<p>Sets whether the Delete the original files on finish check box is activated or deactivated by default on the completion page of the encryption wizards. Users can then change the setting, if desired. If you prevent users from changing the setting, set the Mandatory delete original files setting (FileDeletePlainText) instead.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FileDeletePlainTextDefault Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Disable the check box.</p> <p>1 = Enable the check box.</p>
Entrust File Security Options page > Advanced > Do not monitor files opened using “Decrypt, Verify and Open” context menu	<p>Disables monitoring of opened encrypted files. The monitoring feature ensures that plaintext files are not left on the system without the user’s knowledge.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: SkipFileOpenWatch Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Monitor.</p> <p>1 = Do not monitor.</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
Entrust File Security Options page > Advanced > Prepend “Entrust” to all Windows Explorer context menus	<p>Places the word Entrust at the beginning of the File Security right-click context menu options. For example, the Digitally Sign File menu option becomes Entrust Digitally Sign File.</p> <p>Enable this setting to avoid duplication between Entrust context menu options and EFS context menu options.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FilePrefixExplorerMenus Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Do not add the prefix. 1 = Add the prefix.</p>
Entrust File Security Options page > Advanced > Prevent decryption of file to a network folder	<p>When Security Provider decrypts a file that resides in a network folder, the default action is to create the plaintext version of the file in the same network folder. You can use this registry setting to prevent creation of the plaintext version on the network. When this key is set, the user is prompted for a local folder to hold the decrypted version. See the description of the registry setting <code>LocalDecryptionFolder</code> for information about setting a default local folder.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: PreventNetworkFileDecrypt Value Type: REG_DWORD Value Data: <0-n></p> <p>0 (default) = Allows decryption to a network folder. 1 or other value = Prompts the user for a local folder and prevents decryption to a network folder.</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting.</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Identify a default local folder to use if network file decryption is prevented</p>	<p>This setting allows you to specify the default local decryption folder to be used when file decryption to a folder on the network is prevented. See the description of the registry setting <code>PreventNetworkFileDecrypt</code> for additional information about restricting network file decryption.</p> <p>Add the following configuration setting to the registry:</p> <p>Key:<ESP_registry_location> Value Name: LocalDecryptionFolder Value Type: REG_SZ Value: Folder path</p>
<p>No wizard setting.</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>This setting allows you specify a default destination folder for users decrypting files. This setting only works if <code>PreventNetworkFileDecrypt</code> is disabled (set to 0) and decrypting over the network is allowed. See the description of the registry setting <code>PreventNetworkFileDecrypt</code> for additional information about restricting network file decryption.</p> <p>Add the following configuration setting to the registry:</p> <p>Key:<ESP_registry_location> Value Name: DecryptionFolder Value Type: REG_SZ Value: Folder path</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Adds the EFS encryption menu item to the context menu that appears when users right-click files. This option may require a reboot on some systems.</p> <p>This setting maps to the following registry value:</p> <p>Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced Value Name: EncryptionContextMenu Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Do not display EFS encryption menu item. 1 = Display EFS encryption menu item.</p> <p>The <code>EncryptionContextMenu</code> value is only supported by the <code>HKEY_LOCAL_MACHINE</code> registry subtree.</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>This key controls an optional column on the Certificate Explorer's results table that shows the certificate's trust status.</p> <p>Key: <ESP_registry_location> Value Name: EnableCertificateStatusColumn Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = hide the column and do not allow users to add it</p> <p>1 (default) = hide column but allow users to add it (right-click table header)</p> <p>For 1, the status is collected in the background even if the column is not selected.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>The Encrypt Files wizard can now compress the encrypted files. By default this option is hidden. Use this key to make it available to users.</p> <p>Key: <ESP_registry_location> Value Name: FileAllowSMIMECompression Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = compression check box hidden</p> <p>1 = compression check box visible</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>The Encrypt Files wizard includes a check box labeled "Encrypt the files for other people in addition to myself." By default, the option is not selected. Use this key to have the option enabled by default. The user can still clear the selection. Also see <code>FileEncryptForOthers</code>.</p> <p>Key: <ESP_registry_location> Value Name: FileEncryptForOthersDefault Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = not checked (disabled)</p> <p>1 = selected (enabled)</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>The Encrypt Files wizard includes a check box labeled "Encrypt the files for other people in addition to myself." Use this key to have the option enabled or disabled, and prevent the user from changing the setting. Also see <code>FileEncryptForOthersDefault</code>.</p> <p>Key: <ESP_registry_location> Value Name: <code>FileEncryptForOthers</code> Value Type: <code>REG_DWORD</code> Value Data: <0-1></p> <p>0 (default) = not checked (disabled) 1 = selected (enabled)</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting allows you to switch to from Security Provider's default method of opening a secure file, to a method using the Windows UI.</p> <p>By default Security Provider's asks the user to confirm "open" and then opens the file calling the <code>ShellExecute</code> command. This does not match the Windows UI that appears when opening a downloaded file from the Web or an attachment in Outlook.</p> <p>Windows provides the <code>IAttachmentExecute</code> interface for this purpose. In addition to having the Windows UI, <code>IAttachmentExecute</code> allows Administrators to apply additional policy such as preventing executables from ever being opened.</p> <p>Key: <ESP_registry_location> Value Name: <code>FileOpenWithAttachmentManager</code> Value Type: <code>REG_DWORD</code> Value Data: 0 (default) or 1 (use <code>IAttachmentExecute</code>)</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Allows you to hide the file security options that appear in the right-click menu.</p>	<p>These registry settings are used to hide or reveal the encrypt, sign, or encrypt and sign capability of Security Provider from the user. If the setting has a value of 0 (the default) that capability appears in the Microsoft Explorer menu when the user right clicks on the file. If the value of the setting is 1 the capability is hidden from the user even though the user may have the correct key pair to perform the action.</p> <p>To hide or reveal the encrypt menu option:</p> <p>Key: <ESP_registry_location> Value Name: FileHideEncryptExplorerMenu Value Type: REG_DWORD Value Data: 0 (default) or 1 (hide menu item)</p> <p>To hide or reveal the sign menu option:</p> <p>Key: <ESP_registry_location> Value Name: FileHideSignExplorerMenu Value Type: REG_DWORD Value Data: 0 (default) or 1 (hide menu item)</p> <p>To hide or reveal the encrypt and sign menu option:</p> <p>Key: <ESP_registry_location> Value Name: FileHideEncryptSignExplorerMenu Value Type: REG_DWORD Value Data: 0 (default) or 1 (hide menu item)</p>

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Use this key to specify the hash algorithms your organization considers weak when decrypting signed files. When Security Provider verifies files signed with these algorithms, a warning appears. This applies to both S/MIME and Entrust format files. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: WeakFileHashAlgorithms Value Type: REG_SZ Value Data: <string> Acceptable values are: 8003 (MD5) 8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512) List the values separated by semicolons. For example, to set SHA1 as weak enter 8004
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	By default, the File Security application cannot secure files using certificates that have the Secure Email Extended Key Usage (EKU) OID 1.3.6.1.5.5.7.3.4. To enable the File Security application to use these certificates, set the registry setting below. Key: <ESP_registry_location> Value Name: FileAllowEmailProtectionEKU Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Disable the use of certificates with the Secure Email EKU. 1 = Enable the use of certificates with the Secure Email EKU.

Table 51: Entrust File Security settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Use this key to specify the hash algorithms your organization considers insecure when decrypting signed files. When Security Provider verifies files signed with these algorithms, a warning appears that the signature is not trusted. This applies to both S/MIME and Entrust format files.</p> <p>This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: InsecureFileHashAlgorithms Value Type: REG_SZ Value Data: <string></p> <p>Acceptable values are:</p> <p>8003 (MD5) 8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512)</p> <p>List the values separated by semicolons.</p> <p>For example, to set MD5 as insecure enter 8003</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>By default, when a user encrypts or decrypts a file, the action changes the file's modified date. Security Provider saves the file's original creation, last modified, last accessed times within a secure file. When set to 1, this key causes Security Provider to restore those time/date values.</p> <p>Key: <ESP_registry_location> Value Name: FileRestoreFileTimes Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = do not restore date/time values</p> <p>1 = restore date/time values</p>

Timestamp server settings

If you use the **Custom Installation** wizard, timestamp server settings are configurable through the **Timestamp Server Options** page (Figure 47).

Table 52 describes the timestamp settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Timestamp Server Configuration dialog b

Figure 47: Timestamp Server Configuration dialog box

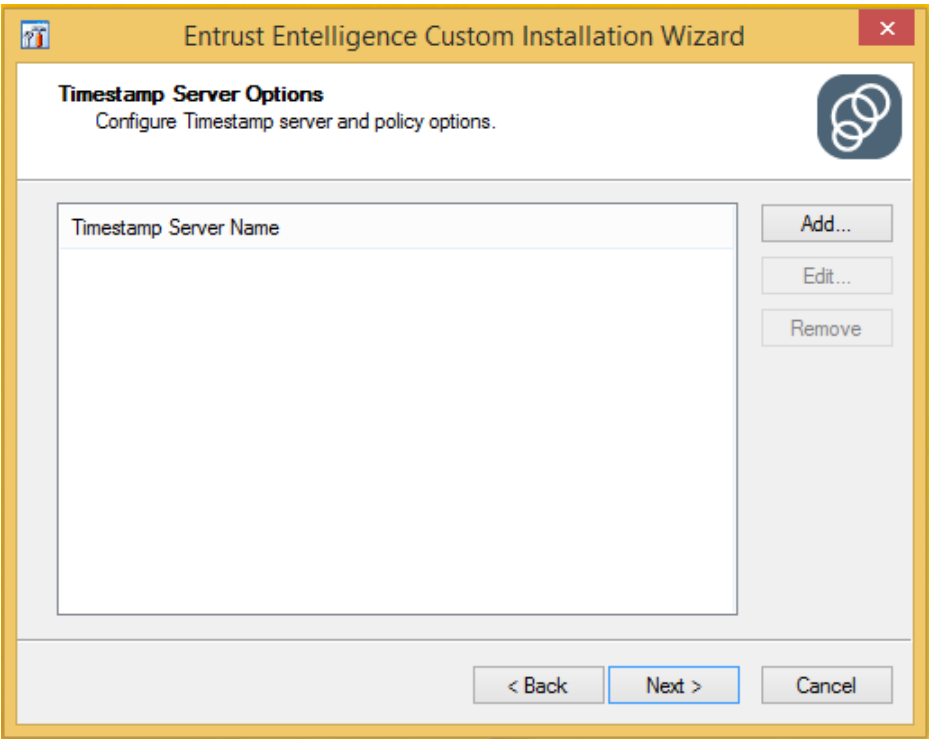


Table 52: Entrust timestamp server settings

Setting name and location in Custom Installation wizard	Description and Value Name
Timestamp Server Options page > Add > Server name	<p>Specifies the name of the Timestamp server you want to use. You can use any name that identifies the server.</p> <p>When you specify a Server name in the Custom Installation wizard, a registry key is created, called <ESP_registry_location>\Timestamp\<server_name>, where <server_name> is your server's name.</p> <p>If you want to specify this setting by hand or through Group Policy, you must create a registry key with your server's name under <ESP_registry_location>\Timestamp.</p>
Timestamp Server Configuration page > Add > Friendly name	<p>Specifies a friendly name for the Timestamp server. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Timestamp\<server_name> Value Name: Name Value Type: REG_SZ Value Data: <friendly_name></p> <p>where <friendly_name> is replaced with a friendly name for your Timestamp server.</p> <p>Example: Value Data: Timestamp 1</p>

Table 52: Entrust timestamp server settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Timestamp Server Configuration page > Add > Friendly name	<p>This is the hash algorithm that Security Provider uses by default for this timestamp server. A different algorithm (or multiple algorithms) may be may defined as policies.</p> <p>Key: <ESP_registry_location>\Timestamp\<server_name> Value Name:DefaultImprintHashAlgorithm Value Type: REG_DWORD Value Data: <Hash Algorithm ID></p> <p>where <Hash Algorithm ID> is the hash algorithm to be used.</p> <p>Acceptable values are:</p> <p>8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512)</p>
Timestamp Server Configuration page > Add > Add (next to URL list) > URL Address	<p>Specifies the URL of your Timestamp server. If you specify multiple URLs for a particular server, Security Provider for Windows attempts to get a timestamp from the first URL, and if that fails, from the second URL, and so on until a valid timestamp is received.</p> <p>Note: Entrust offers timestamping through its Entrust Verification Server product.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location>\Timestamp\<server_name> Value Name: Server Value Type: REG_SZ Value Data: <URL></p> <p>where <URL> is the URL for your Timestamp server. To specify multiple URLs, separate each URL with a pipe (). The Timestamp server must support RFC 3161.</p> <p>Example:</p> <p>Value Data: http://tserver.company.com:1234/verificationserver/rfc3161timestamp</p>

Table 52: Entrust timestamp server settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Timestamp Server Configuration page > Add > Add (next to Policy list) > OID	<p>Specifies a timestamp policy object identifier (OID). This OID is sent to the timestamp server whenever a timestamp request is submitted, and must be acceptable to the timestamp server. Sending a timestamp policy OID to the timestamp server is optional.</p> <p>The default policy OID acceptable to Verification Server (a timestamp server available from Entrust) is 1.2.840.113533.7.75.0.</p> <p>You can specify one or more policy OIDs in the Custom Installation wizard, or you can specify them by hand or through Group Policy. To specify OIDs manually or through Group Policy, you must do one of the following:</p> <ul style="list-style-type: none">• If you want to specify multiple OIDs:<ol style="list-style-type: none">1. Create one registry key per OID under <ESP_registry_location>\Timestamp\<server_name>. For example <ESP_registry_location>\Timestamp\<server_name>\1.234.456.where 1.234.456 is the OID number.<ol style="list-style-type: none">2. Set the <code>DefaultPolicy</code> setting, as described on page 449.3. Set the OID's <code>FriendlyName</code>, as described on page 449.The result is that users see a drop-down list asking them to pick a policy when they timestamp a file.• If you want to specify a single OID:<p>Set the <code>DefaultPolicy</code> setting, as described on page 449. The result is that this OID is sent along with the timestamp request.</p>

Table 52: Entrust timestamp server settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Timestamp Server Configuration page > Add > Policy group > Default button	<p>Specifies the default policy OID. If only one OID is specified, this setting specifies that OID. If multiple OIDs are specified, this setting specifies which policy OID is selected by default in the drop-down menu presented to users when they digitally sign a file. This setting maps to the following registry key:</p> <p>Key: <ESP_registry_location>\Timestamp\<server_name> Value Name:DefaultPolicy Value Type: REG_SZ Value Data: <OID></p> <p>where <OID> is replaced with the policy OID that you want to send to your Timestamp server. You can only send one OID per timestamp request.</p> <p>Example: Value Data: 1.2.840.113533.7.75.0</p> <p>Note: The specific OIDs accepted by the timestamp server.</p>
Timestamp Server Configuration page > Add > Add (next to Policy list) > Friendly Name	<p>Specifies the friendly name of a policy. This name appears in the drop-down list presented to users when they digitally sign a file. If you have specified a single policy, you can ignore this setting because your users never see the drop-down list.</p> <p>This setting maps to the following registry key:</p> <p>Key: <ESP_registry_location>\Timestamp\<server_name>\<OID> Value Name: Name Value Type: REG_SZ Value Data: <friendly_name></p> <p>where <friendly_name> is replaced with a friendly name that appears in the drop-down list presented to users when they digitally sign a file.</p> <p>Example: Value Data: Top Secret Policy</p>

Table 52: Entrust timestamp server settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Timestamp Server Configuration page > Add > Friendly name	<p>This is the hash algorithm that Security Provider uses for a particular policy for a timestamp server. If the policy is selected by the user it is used instead of the default algorithm.</p> <p>Key: <ESP_registry_location>\Timestamp\<server_name> Value Name:ImprintHashAlgorithm Value Type: REG_DWORD Value Data: <Hash Algorithm ID></p> <p>where <Hash Algorithm ID> is the hash algorithm to be used.</p> <p>Acceptable values are:</p> <p>8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512)</p>

Password Encrypt settings

If you use the **Custom Installation** wizard, Password Encrypt settings are configurable through the **Password Encrypt Options** page (Figure 48).

Table 53 describes the password encrypt settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?”](#) on page 329.

Figure 48: Password Encrypt Options page

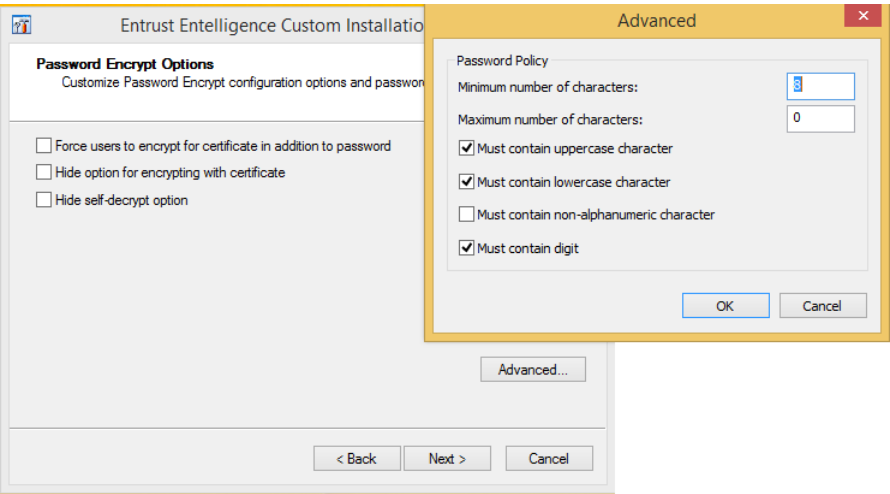


Table 53: Password encrypt settings

Setting name and location in Custom Installation wizard	Description and Value Name
Password Encrypt Options > Force users to encrypt for certificate in addition to password	<p>Specifies whether the Encrypt the files for my encryption certificate in addition to the password check box is selected in the password encrypt wizard. When this check box is enabled, the file is encrypted with a password and the user's certificate (if they have one).</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: EncryptPasswordFilesForCert Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = Check box is deselected. 1 (default) = Check box is selected.</p>
Password Encrypt Options > Hide option for encrypting with certificate	<p>Specifies whether the Encrypt the files for my encryption certificate in addition to the password check box and related controls are visible in the password encrypt wizard.</p> <p>Key: <ESP_registry_location> Value Name: HideEncryptPasswordFilesForCert Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Show the check box and controls. 1 = Hide the check box and controls.</p>
Password Encrypt Options > Hide self-decrypt option	<p>Specifies whether the Generate self-decrypting output file check box is visible in the Password Encrypt wizard. For details on self-decrypt, see "Password Encrypt functionality" on page 222.</p> <p>Key: <ESP_registry_location> Value Name: HideSelfDecrypt Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Show the Generate self-decrypting output file check box. The check box is shown, deselected. 1 = Deselect and hide the Generate self-decrypting output file check box. (This setting effectively disables the self-decrypt feature.)</p>

Table 53: Password encrypt settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Password Encrypt Options > Advanced > Password Policy	<p>Several settings allow you to specify password rules.</p> <p>In the Custom Installation wizard, these settings are:</p> <p>Minimum number of characters Maximum number of characters Must contain uppercase character Must contain lowercase character Must contain non-alphanumeric character Must contain digit</p> <p>The above settings map to the following registry settings:</p> <p>Key: <ESP_registry_location> Value Names: EncryptPasswordMinLength (default: 8) EncryptPasswordMaxLength (default: 0, meaning no max.) EncryptPasswordMustContainUpper (default: 1 (true)) EncryptPasswordMustContainLower (default: 1 (true)) EncryptPasswordMustContainNonAlphanumeric (default: 0 (false)) EncryptPasswordMustContainDigit (default: 1 (true)) Value Type: REG_DWORD Value Data: <0-n></p>
Entrust File Security Options page > Advanced > Mandatory delete original files setting	<p>Forces the deletion or preservation of the original plaintext files after an encryption operation. If you do not specify a value for this setting, Security Provider uses the Default delete original files setting (PEFileDeletePlainTextDefault) setting instead.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: PEFileDeletePlainText Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Disables and grays out the Delete the original files on finish check box and forces the preservation of plaintext files.</p> <p>1 = Enables and grays out the Delete the original files on finish check box and forces the deletion of plaintext files.</p>

Table 53: Password encrypt settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
Entrust File Security Options page > Advanced > Default delete original files setting	<p>Sets whether the Delete the original files on finish check box is activated or deactivated by default on the completion page of the encryption wizards. Users can then change the setting, if desired. If you prevent users from changing the setting, set the Mandatory delete original files setting (PEFileDeletePlainText) instead.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: PEFileDeletePlainTextDefault Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Disable the check box. 1 = Enable the check box.</p>

TrueDelete settings

If you use the **Custom Installation** wizard, most TrueDelete settings are configurable through the **TrueDelete Filter Configuration Options** page (Figure 49). To navigate to this page, click **Add** on the **TrueDelete Configuration Options** page.

Table 54 describes the TrueDelete settings. Each setting in the table refers to the `<ESP_registry_location>` variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Note: If you add the TrueDelete filter rules in the registry settings, manually (rather than through the Customization wizard), you must restart the TrueDelete service to enable the new registry settings.

Figure 49: TrueDelete Configuration Options page

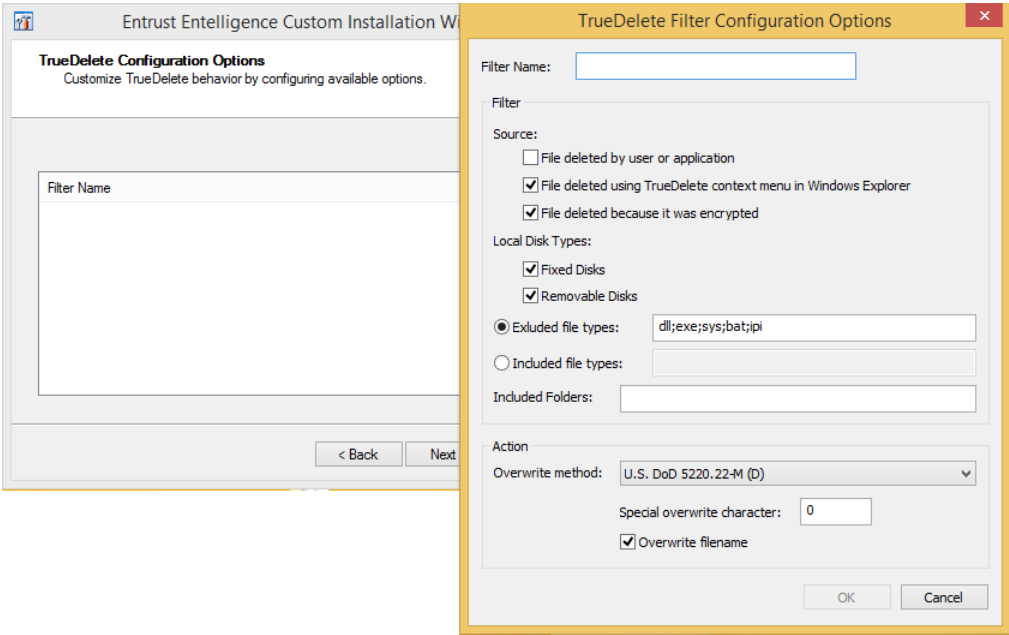


Table 54: TrueDelete settings

Setting name and location in Custom Installation wizard	Description and Value Name
TrueDelete Configuration Options page > Add > Filter Name	<p>The name of a filter. A filter associates a TrueDelete trigger with an action. For example, if a user presses Shift+Delete (trigger), then overwrite method 1 is invoked (action). You might name this filter ShiftDeleteFilter.</p> <p>When you specify a Filter Name in the Custom Installation wizard, a registry key is created, called <ESP_registry_location>\TrueDelete\Filter\<filter_name>, where <filter_name> is your filter's name.</p>
TrueDelete Configuration Options page > Up and Down buttons	<p>Specifies the order in which the filters are checked. TrueDelete checks each filter, one-by-one, in order, until a filter is matched. If no filter is matched, then TrueDelete is not triggered.</p> <p>The Up and Down buttons map to the following registry value:</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\ Value Name: FilterOrder Value Type: REG_SZ Value Data: <filter_names></p> <p>where <filter_names> is replaced with a list of filter names that you have defined, separated by a semi-colon (;).</p> <p>Example: Value Data: My filter; My 2nd filter; My 3rd filter</p>

Table 54: TrueDelete settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
TrueDelete Configuration Options page > Add > Source	<p>Specifies the action that triggers TrueDelete to securely delete files. In the Custom Installation wizard, you are presented with these check boxes:</p> <ul style="list-style-type: none">• File deleted by user or application—when this is selected, TrueDelete is triggered when a user or application deletes a file• File deleted using TrueDelete context menu in Windows Explorer—when this is selected, TrueDelete is triggered when a user right-clicks a file and selects Securely Delete File.• File deleted because it was encrypted—when this is selected, TrueDelete is triggered when a user or application encrypts a file (the original unencrypted file is overwritten by TrueDelete) <p>The above options map to the following registry value.</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: Source Value Type: REG_DWORD Value Data: <1_2_4_or_combination></p> <p>1 = TrueDelete is triggered when a user deletes a file using the Shift+Delete key combination (Delete by itself does not trigger TrueDelete), or when an application deletes a file.</p> <p>2 (default) = TrueDelete is triggered when a user right-clicks a file or folder and selects Securely Delete.</p> <p>4 = TrueDelete is triggered when a user or application encrypts a file (the original unencrypted file is overwritten by TrueDelete)</p> <p>To use the triggers in combination, add them together. For example, if you want to enable triggers 1 and 4, enter 5 into the value data, or if you want to use triggers 1, 2 and 4, enter 7.</p>

Table 54: TrueDelete settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
TrueDelete Configuration Options page > Add > Local Disk Types	<p>Specifies the disks for which TrueDelete is enabled. In the Custom Installation wizard, you are presented with these check boxes:</p> <ul style="list-style-type: none"> • Fixed Disks—when this is selected, TrueDelete is enabled for files that reside on non-removable disks such as a fixed hard drive. This includes solid state drives (SSD). • Removable Disks—when this is selected, TrueDelete is enabled for files that reside on a removable media such as an external hard drive. <p>The above options map to the following registry value.</p> <p>Key:<ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: DriveTypes</p> <p>Value Type: REG_DWORD</p> <p>Value Data: <1_2_or_3></p> <p>1 = TrueDelete is enabled for files that reside on non-removable disks such as a fixed hard drive.</p> <p>2 = TrueDelete is enabled for files that reside on a removable media such as an external hard drive.</p> <p>3 (default) = TrueDelete is triggered regardless of whether a file resides on a fixed or removable disk.</p>
TrueDelete Configuration Options page > Add > Excluded file types	<p>Specifies the file types for which TrueDelete is disabled.</p> <p>The Excluded file types options maps to the following registry value.</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: ExcludedFileTypes</p> <p>Value Type: REG_SZ</p> <p>Value Data: <extension1;extension2;extension_n></p> <p>where <extension1;extension2;extension_n> is a list of file extensions separated by semi-colons (;).</p> <p>The default is dll;exe;sys;bat;ipi.</p>

Table 54: TrueDelete settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
TrueDelete Configuration Options page > Add > Included file types	<p>Specifies the file types for which TrueDelete is enabled.</p> <p>The Included file types option maps to the following registry value.</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: IncludedFileTypes Value Type: REG_SZ Value Data: <extension1;extension2;extension_n></p> <p>where <extension1;extension2;extension_n> is a list of file extensions separated by semi-colons (;).</p> <p>By default, this setting is not present, meaning TrueDelete is enabled for all file types except those specified in the Excluded file types option.</p>

Table 54: TrueDelete settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. IncludedFolders	<p>Specifies folders or drives for which TrueDelete is enabled.</p> <p>The Included folders option maps to the following registry value.</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: IncludedFolders Value Type: REG_MULTI_SZ Value Data: <folderordrive_1> <folderordrive_n></p> <p>where <folderordrive1> <folderordrive_n> is a list of folders or drives, each on a separate line. The value supports system environment variables. (User environment variables are not supported.)</p> <p>Example:</p> <p>Value Data: D: C:\Documents and Settings\%PROTECTED_FOLDER%</p> <p>Note: Use the wildcard character to enable TrueDelete to delete subfolders when a user deletes a folder.</p> <p>For example: C:\Documents and Settings\%PROTECTED_FOLDER%*</p> <p>By default, this setting is not present, meaning TrueDelete is enabled for all folders and drives.</p>

Table 54: TrueDelete settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
TrueDelete Configuration Options page > Add > Overwrite method	<p>Specifies the overwriting method that TrueDelete uses to securely delete files. For details, see “About overwriting methods” on page 231.</p> <p>The Overwrite method option maps to the following registry value.</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: OverwritingMethod Value Type: REG_DWORD Value Data: <0-12></p> <p>0 = The file is deleted as normal. TrueDelete does nothing. 1 = One Pass Zeroes overwriting method. 2 = One Pass Random overwriting method. 3 = U.S. DoD 5220.22-M (C) overwriting method. 4 (default) = U.S. DoD 5220.22-M (D) overwriting method. 5 = U.S. DoD 5220.22-M (E) overwriting method. 6 = U.S. DoD 5220.22-M (EV) overwriting method. 7 = US Army AR380-19 overwriting method. 8 = Canadian RCMP TSSIT OPS-II overwriting method. 9 = German VSITR overwriting method. 10 = Russian GOST P50739-95 overwriting method. 11 = British HMG IS5 Baseline overwriting method. 12 = British HMG IS5 Enhanced overwriting method. 13 = U.S. DOE-NNSA overwriting method</p>

Table 54: TrueDelete settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
TrueDelete Configuration Options page > Add > Special overwrite character	<p>A user-defined character that the overwriting method uses. User-defined characters are only supported for overwriting methods 3 - 7 and 9. For details, see “About overwriting methods” on page 231.</p> <p>The Special overwrite character maps to the following registry value:</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: UserDefinedCharacter Value Type: REG_SZ Value Data: <any_character></p> <p>where <any_character> can be any letter, number, or special character.</p> <p>The default is 0.</p>
TrueDelete Configuration Options page > Add > Overwrite filename	<p>Specifies whether a file name is overwritten after overwriting a file's contents.</p> <p>The Special overwrite character maps to the following registry value:</p> <p>Key: <ESP_registry_location>\TrueDelete\Filter\<filter_name></p> <p>Value Name: OverwriteFilename Value Type: REG_DWORD Value Data: <0_or_1></p> <p>0 = do not overwrite the file name</p> <p>1 (default) = overwrite the file name. TrueDelete renames the file 26 times, each time replacing the file's name with a Globally Unique Identifier (GUID).</p>

Entrust Certificate Explorer settings

Table 55 describes the Entrust Certificate Explorer settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Note: The **Search for People** dialog box available in the Entrust Certificate Explorer has a setting described in [“Entrust File Security settings” on page 430](#). Additionally, there is a setting to hide the Entrust Certificate Explorer menu item, described in [“GUI customization settings” on page 478](#).

Table 55: Entrust Certificate Explorer settings

Setting name and location in Custom Installation wizard	Description and Value Name
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Specifies whether to display the Personal folder in the tree view when users open the Entrust Certificate Explorer for the first time.</p> <p>If you specify this setting under the HKEY_CURRENT_USER root, you are setting a default that users can override. If you specify this setting under the HKEY_LOCAL_MACHINE root, you are setting an enforced value that users cannot modify.</p> <p>For example, if you set ShowPersonalCertificates=0 under HKEY_CURRENT_USER, personal certificates are hidden by default; however, users can opt to display them by selecting View > Show Personal Certificates. If you set ShowPersonalCertificates=0 under HKEY_LOCAL_MACHINE, personal certificates are hidden permanently, and users cannot opt to display them. (The View > Show Personal Certificates menu option is grayed out.)</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: ShowPersonalCertificates Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Hide the certificates. 1 = Display the certificates.</p>

Table 55: Entrust Certificate Explorer settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Specifies whether to display the Intermediate Certification Authorities and the Trusted Root Certification Authorities folders (Figure 20 on page 234) when users open the Entrust Certificate Explorer for the first time.</p> <p>If you specify this setting under the HKEY_CURRENT_USER root, you are setting a default that users can override. If you specify this setting under the HKEY_LOCAL_MACHINE root, you are setting an enforced value that users cannot modify.</p> <p>For example, if you set ShowCACertificates=0 under HKEY_CURRENT_USER, CA certificates are hidden by default; however, users can opt to display them by selecting View > Show CA Certificates. If you set ShowCACertificates=0 under HKEY_LOCAL_MACHINE, CA certificates are hidden permanently, and users cannot opt to display them. (The View > Show CA Certificates menu option is grayed out.)</p> <p>Key: <ESP_registry_location> Value Name: ShowCACertificates Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Hide the certificates. 1 = Display the certificates.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Allows you to customize the location of the file, <code>pegroups.dat</code>, used to store personal encryption groups.</p> <p>Key: <ESP_registry_location> Value Name: AppDataFolder Value Type: REG_SZ Value Data: <path-to-folder></p> <p>Specify a path to the root folder for the file. Security Provider automatically creates an <code>\Entrust\ESP</code> subfolder. The specified path can contain environment variables. They are expanded before the folder is used.</p> <p>Note: If a <code>pegroups.dat</code> file exists in original default folder, it is not copied to the new location and this setting is ignored.</p>

Table 55: Entrust Certificate Explorer settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Determines if the Certificate Explorer menu option to import a personal address book (PAB), Import Entrust Address Book, is visible or not. See "About manual address book migration" on page 102 for feature information.</p> <p>Key: <ESP_registry_location> Value Name: EnableEntrustPABImport Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Hide the menu option. 1 = Show the menu option.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Determines where certificates from a personal address book (PAB) are stored when a user imports a PAB using the Certificate Explorer. See "Address book (PAB)" on page 101 for feature information. This also sets the location used by automatic PAB migration, such as when a user logs in to an .epf file.</p> <p>Key: <ESP_registry_location> Value Name: ExportPABToOtherPeopleStore Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Import certificates to the Trusted People store. 1 = Import certificates to the Other People store.</p> <p>The Certificate Explorer menu option related to importing a PAB is not visible if EnableEntrustPABImport is set to 0.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Controls whether the Certificate Explorer includes a menu option to import an Entrust .key file. (See "Importing certificates from an Entrust key file" on page 105 for feature information.)</p> <p>Key: <ESP_registry_location> Value Name: EnableEntrustKeyImport Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Hide the menu option. 1 = Show the menu option.</p>

Table 55: Entrust Certificate Explorer settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Controls whether the Certificate Explorer includes a menu option to export an Entrust key file. (See “Exporting a certificate to an Entrust key file” on page 105 for feature information.)</p> <p>Key: <ESP_registry_location> Value Name: EnableEntrustKeyExport Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Hide the menu option. 1 = Show the menu option.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Specifies whether to display the archived certificates by default in Certificate Explorer.</p> <p>If you set ShowArchivedCertificates to 0, archived certificates are hidden by default; however, users can display them by selecting View > Show Archived Certificates in the right-click menu. If you set ShowArchivedCertificates to 1, archived certificates are displayed by default.</p> <p>Key: <ESP_registry_location> Value Name: ShowArchivedCertificates Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Hide the certificates by default. 1 = Display the certificates by default.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Specifies whether to display the Personal Encryption Groups link in the tree view of the Entrust Certificate Explorer. (See “About the manual recipient list migration” on page 103 for feature information.)</p> <p>Key: <ESP_registry_location> Value Name: ShowPersonalEncryptionGroups Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = Hide the link. 1 (default) = Display the link.</p>

Table 55: Entrust Certificate Explorer settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Specifies whether the associated private key is deleted from the CSP when the certificate is deleted. Key: <ESP_registry_location> Value Name: DeleteKeyWhenDeleteCertificate Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Do not delete the private key. 1 = Delete the private key.
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. Preferred status	By selecting Group By from the right click menu in the Certificate explorer list, a user can display the entries in the list by Issuer, Directory, or OU (see "Grouping certificates in a list" on page 239). Certificate Explorer displays these groups in alphabetical order by default. This order can be altered by defining a priority for specific Issuers, Directories (with or without Search Base), and Organizational Units. For example, you can prioritize the list so entries with specific organizational units will appear first, second, third by defining them as Group1, Group2, or Group3. For the Issuer list: Key: <ESP_registry_location>\GroupByIssuerOrder Value Name: Group1 (or Group2 or Group3 and so on) Value Type: REG_SZ Value Data: Display value of Issuer, this is usually the CN from the issuer's DN. For the Organization list: Key: <ESP_registry_location>\GroupByOUOrder Value Name: Group1 (or Group2 or Group3 and so on) Value Type: REG_SZ Value Data: Value of the OU, from the issuer's DN. For the Directory list: Key: <ESP_registry_location>\GroupBySearchDirectoryOrder Value Name: Group1 (or Group2 or Group3 and so on) Value Type: REG_SZ Value Data: Directory name

Table 55: Entrust Certificate Explorer settings (continued)

Setting name and location in Custom Installation wizard	Description and Value Name
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard. Display mode	Certificate Explorer is a very powerful tool for looking at digital IDs and is useful for troubleshooting problems. To deliver the right level of information to the user, it can be configured for three modes. In the default mode the user sees the level of information suitable for the average user; Advanced mode displays additional information, and Debug mode displays the largest amount of information. See "Setting up advanced user and debug modes" on page 242 . Key: <ESP_registry_location> Value Name: CertificateExplorerMode Value Type: REG_DWORD Value Data: 1 for Advanced mode, 2 for Debug mode. Default is 0.

Entrust Ready identity device setting

Table 56 describes the Entrust Ready identity device setting.

The setting refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Table 56: Entrust Ready identity device settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Specifies the full path to the DLL file of an Entrust Ready identity device. For example, you could use this with an Entrust-ready biometric device, such as a fingerprint scanner. This setting is optional.</p> <p>This feature is only available when users enroll for Entrust security stores using the Entrust Enhanced Cryptographic Provider.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: IdentityLibrary Value Type: REG_SZ Value Data: <full_path_to_identity_library_dll></p>

Certificate path discovery, validation, download, and extensions settings

Table 57 describes the settings for the following features:

- Automatic Additional Certificate Download
- Certificate Path Discovery
- Certificate Path Validation
- Certificate Path Critical Extension Policy Provider

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Table 57: Certificate path discovery and validation settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Automatic Additional Certificate Download feature only.</p> <p>Sets the interval used when retrieving extra certificates, such as cross-certificates and link certificates, from LDAP directories. This setting is optional.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: RetrieveExtraCertsInterval Value Type: REG_DWORD Value Data: <interval_in_minutes></p> <p>0 = No extra certificates are retrieved. This has the effect of disabling retrieval of cross-certificates and link certificates by the Digital ID Monitor, Windows service Digital ID, and Computer Digital ID Service. Certificates are still retrieved when the user logs in at the end of an enrollment or recovery operation.</p> <p>The default is 360 minutes.</p>

Table 57: Certificate path discovery and validation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Certificate Path Discovery feature only.</p> <p>Sets the lifetime of the CA certificate cache (eespcacertcache.sst). When the lifetime expires, Security Provider returns to the default directory to retrieve and cache a new set of CA certificates and cross-certificates.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: CASearchResultLifetime Value Type: REG_DWORD Value Data: <time_in_minutes></p> <p>The default is 720 minutes.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Certificate Path Validation feature only.</p> <p>Specifies a list of policy identifiers corresponding to policies that are acceptable to the user. Consult RFC 3280bis-02 for more details on this setting.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: UserInitialPolicySet Value Type: REG_SZ Value Data: <policy_OID1;policy_OID2;policy_OIDn></p> <p>The default is any-policy.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Certificate Path Validation feature only.</p> <p>Specifies whether the anyPolicy OID must be processed if it is included in the certificate. Consult RFC 3280bis-02 for more details on this setting.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: InitialAnyPolicyInhibit Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = The anyPolicy OID does not need to be processed. 1 = The anyPolicy OID must be processed.</p>

Table 57: Certificate path discovery and validation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Certificate Path Validation feature.</p> <p>Specifies whether policy mapping is allowed in the certification path. Consult RFC 3280bis-02 for more details on this setting.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: InitialPolicyMappingInhibit Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Allow policy mapping in the certification path. 1 = Prohibit policy mapping in the certification path.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Certificate Path Validation feature.</p> <p>Specifies whether the path must be valid for at least one of the certificate policies in the UserInitialPolicySet. Consult RFC 3280b for more details on this setting.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: InitialExplicitPolicy Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = No requirement for at least one valid certificate policy path. 1 = At least one certificate policy must have a valid path.</p>

Table 57: Certificate path discovery and validation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting pertains to the Certificate Path Critical Extension Policy Provider and applies to private extensions only.</p> <p>Specifies the acceptable critical extensions for your environment. Each acceptable critical extension is added as a separate value name. Once a private critical extension is defined in the registry, it is no longer considered an unknown extension.</p> <p>By default, the Certificate Path Critical Extension Policy Provider accepts the following extensions, when they are critical:</p> <p>2.5.29.10—basicConstraints (old) 2.5.29.19—basicConstraints 2.5.29.15—keyUsage 2.5.29.30—id-ce-nameConstraints 2.5.29.36—id-ce-policyConstraints 2.5.29.33—id-ce-policyMappings 2.5.29.37—id-ce-extKeyUsage 2.5.29.54—id-ce-inhibitAnyPolicy 2.5.29.17—id-ce-subjectAltName 2.5.29.32—id-ce-certificatePolicies</p> <p>Note: The above-mentioned extensions do not have to be added in the registry. They are added by default.</p> <p>To specify the name of the critical extension, use the following registry value:</p> <p>Key: <ESP_registry_location>\Critical Extensions Value Name: <Extension_OID> (for example, 1.2.3.4.5) Value Type: REG_SZ Value Data: <extension_name></p> <p>Example:</p> <p>Value Data: MyExtension</p>

Table 57: Certificate path discovery and validation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Identifies a hash algorithm as Insecure</p>	<p>Security Provider's Policy Base Provider validates that a certificate chain is not using a hash algorithm that is specified in this setting and is therefore insecure. When one of the certificates in the chain uses an insecure hash algorithm, the certificate chain is not valid.</p> <p>Key: <ESP_registry_location> Value Name: InsecureCertHashAlgorithms Value Type: REG_SZ Value Data: <string></p> <p>Acceptable values are:</p> <p>8003 (MD5) 8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512)</p> <p>List the values separated by semicolons.</p> <p>For example, to set MD5 as insecure set the value data to 8003.</p> <p>When one of the certificates in the chain uses an insecure hash algorithm, the certificate chain is considered not to be valid.</p>

Table 57: Certificate path discovery and validation settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Identifies a hash algorithm as Weak</p>	<p>Security Provider's Policy Base Provider validates that a certificate chain is not using a hash algorithm that is specified here. When the certificate uses a weak hash algorithm, Security Provider's Policy Base Provider sets an information status code in the trust status of the certificate.</p> <p>Key: <ESP_registry_location> Value Name: WeakCertHashAlgorithms Value Type: REG_SZ Value Data: <string>;<string></p> <p>Acceptable values are:</p> <p>8003 (MD5) 8004 (SHA1) 800C (SHA 256) 800D (SHA 384) 800E (SHA 512)</p> <p>List the values separated by semicolons.</p> <p>For example, to set SHA1 as weak set the value data to 8004.</p> <p>When the certificate uses a weak hash algorithm, Security Provider's Policy Base Provider sets an information status code in the trust status of the certificate.</p>

HTTP connection and timeout settings

Internet connection timeout settings take effect when Security Provider connects to a server (for example, the Security Manager Proxy, Auto-enrollment Service, and OCSP server) over HTTP or HTTPS.

Table 58 describes the Internet connection and timeout settings.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Table 58: Internet connection and timeout settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Add this value to set the timeout in seconds for Internet connection requests. If a connection request takes longer than this timeout value, the request is canceled. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: HTTPConnectTimeLimit Value Type: REG_DWORD Value Data: <timeout_in_seconds>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Add this value to set the timeout in seconds for receiving an response to an Internet request. If the response takes longer than the timeout value, the request is canceled. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: HTTPReceiveTimeLimit Value Type: REG_DWORD Value Data: <timeout_in_seconds>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Add this value to set the timeout in seconds for sending Internet requests. If sending the request takes longer than the timeout value, it is canceled. This setting is optional. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: HTTPSendTimeLimit Value Type: REG_DWORD Value Data: <timeout_in_seconds>

Table 58: Internet connection and timeout settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>You can specify a custom user-agent header when using HTTP or HTTPS protocols. These protocols are used for CRL retrieval, OCSP protocol, auto-enrollment protocol, and proxy access through the Entrust Authority Proxy server.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: HTTPUserAgent Value Type: REG_SZ Value Data: <user-agent-header></p> <p>The default is Entrust Entelligence Security Provider.</p>

GUI customization settings

Table 59 describes the settings that hide elements of the Security Provider GUI. Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Note: Other settings are available to change the help links on various dialog boxes, and the text in the **Search** dialog box. See [“Entrust security store login settings” on page 396](#) and [“Entrust File Security settings” on page 430](#) for details.

Table 59: GUI customization settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Hides the Options menu item when right-clicking the taskbar. This setting is optional. Note: This setting requires a computer reboot. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: HideOptionsInTrayMenu Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Show the Options menu item. 1 = Hide the Options menu item.

Table 59: GUI customization settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Hides the Enroll for Entrust Digital ID menu item when right-clicking the taskbar. The option remains visible from the Start menu. This setting is optional. This setting requires a computer reboot. Another way to hide the enroll option in both the taskbar and the Start menu is to disable the Entrust digital ID feature through the Custom Installation wizard. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: HideEnrollInTrayMenu Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Show the Enroll for Entrust Digital ID menu item. 1 = Hide the Enroll for Entrust Digital ID menu item.
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Hides the Recover Entrust Digital ID menu item when right-clicking the taskbar. The option remains visible from the Start menu. This setting is optional. This setting requires a computer reboot. Another way to hide the recover option in both the taskbar and the Start menu is to disable the Entrust digital ID feature through the Custom Installation wizard. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: HideRecoverInTrayMenu Value Type: REG_DWORD Value Data: <0-1> 0 (default) = Show the Recover Entrust Digital ID menu item. 1 = Hide the Recover Entrust Digital ID menu item.

Table 59: GUI customization settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Hides the Help menu item when right-clicking the taskbar status icon in the taskbar notification area. This setting is optional.</p> <p>Note: This setting requires a computer reboot.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: HideHelpInTrayMenu Value Type: REG_DWORD</p> <p>0 (default) = Show the Help menu item. 1 = Hide the Help menu item.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Hides the Entrust Certificate Explorer menu item when right-clicking the taskbar status icon in the taskbar notification area. The item remains visible through the Start menu. If you do not want users to access the Entrust Certificate Explorer at all, disable the feature in the Custom Installation wizard. This setting is optional.</p> <p>Note: This setting requires a computer reboot.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: HideCertExplorerInTrayMenu Value Type: REG_DWORD</p> <p>0 (default) = Show the Entrust Certificate Explorer menu item. 1 = Hide the Entrust Certificate Explorer menu item.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>This setting changes the default display of DNs in the Select Certificate dialog from the simplified display name to the full DN. For example, if the setting is disabled, the UI shows Alice Gray in the Issued to column. If the setting is enabled, it shows Alice Gray (cn= Alice Gray, o=Example, c=CA). The setting maps to:</p> <p>Key: <ESP_registry_location> Value Name: IncludeFullDNInName Value Type: REG_DWORD</p> <p>0 (default) = Show the display name. 1 = Show full DN.</p>

Table 59: GUI customization settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This registry setting is used to change the graphic in the heading of the login dialog, PIV smart card authentication dialog, and system tray from Entrust® Securing Digital Identities & Information to a custom heading of your choice.</p> <p>Additionally, this feature requires:</p> <ul style="list-style-type: none">• the Security Provider branding dll (eebrnd.dll)• a custom dynamic link library created by the Administrator• a graphic displaying the new heading <p>Key: <HKLM or HKCU>\Software\Entrust\ESP\PKI\<CA DN> Value Name: EPFNamingDllName Value Type: REG_SZ Value Data: <Full_path_to_the_naming_dynamic_link_library></p> <p>The <i>Customizing the Entrust Security Store Login Service White Paper</i> contains instructions about using this feature.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This registry setting hides the login option in the user's system tray (see PIVInsertRetiresSystemTrayOptions). It will no longer appear to these smart card users.</p> <p>Key: <ESP_registry_location> Value Name: HideLoginInTrayMenu Value Type: DWORD Values: <1 or 0> Default: 0</p> <p>0: Login option in system tray menu is shown. 1: Login option in system tray menu is hidden.</p>

Table 59: GUI customization settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>If users have the system tray component of Security Provider, this registry setting disables the user's system tray (see <code>PIVInsertRetiresSystemTrayOptions</code>). The system tray will no longer appear to these users.</p> <p>Key: <ESP_registry_location> Value Name: <code>DisableSystemTray</code> Value Type: <code>DWORD</code> Values: <1 or 0> Default: 0</p> <p>0: System tray is enabled. 1: System tray is disabled.</p> <p>Note: The <code>DisableSystemTray</code> registry option is used internally by Security Provider to disable the system tray. If administrators do not want the system tray option to appear to users under ordinary circumstances they should not include that component in their installation.</p>

Table 59: GUI customization settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting disables the Options, Enroll, Recover, and Login options in the system tray or the entire Security Provider system tray, depending on the value selected. If a different option is selected in the registry settings listed below, it will be used instead of this setting.</p> <ul style="list-style-type: none">• HideOptionsInTrayMenu• HideLoginInTrayMenu• HideEnrollInTrayMenu• HideRecoverInTrayMenu• DisableSystemTray <p>Note: Only the current Windows user account is affected.</p> <p>Key: <HKLM>\SOFTWARE\Wow6432Node\Entrust\ESP Value Name: PIVInsertRetiresSystemTrayOptions Value Type: DWORD Value Data: 0, 1, or 2 Default value: 0</p> <p>0 - No retirement operation are performed on the first smart card insert.</p> <p>1 - ESP Hides the following system tray options on the first smart card insert: Options, Enroll, Recover, and Login</p> <p>2 - ESP Disables the Entrust system tray</p> <p>Note: The changes and are valid only for the current Windows user account.</p> <p>Also, if an administrator sets a different value in HKEY_LOCAL_MACHINE for any of the 5 registry automatically set by ESP on the smart card insert, the HKEY_LOCAL_MACHINE value will be used.</p>

Miscellaneous settings

Table 60 describes the settings for Entrust TruePass, CSPs, KAS, enrollment stations, and encoding.

Each setting in the table refers to the <ESP_registry_location> variable. To determine this location, see [“What is the ESP registry location?” on page 329](#).

Table 60: Miscellaneous settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>This setting changes the way that the intermediate CA certificates are saved into an Entrust security store. Entrust Entelligence Security Provider and Entrust Authority Toolkit for the Java Platform have implemented this differently in the past. For backwards compatibility and compatibility with the Java Toolkit the default value of this setting uses both. However, you can alter this setting for compatibility only with the Java Toolkit, if backward compatibility with previous versions of Security Provider are not required.</p> <p>Key: <ESP_registry_location> Value Name: DisableEPFSubCACertsCompatibility Value Type: REG_DWORD Value Data: <0 or 1></p> <p>If 1, intermediate CA certificates will not be written into the sections used by older versions of Security Provider. Default is 0.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>If this value is set to 1, Security Provider's CSP will accept an RSA public key with a weak public key exponent length for public key operations (usually an older CA key). If the value is set to 0 (the default), public keys with weak exponent lengths are not accepted.</p> <p>Note: Do not disable this check if FIPS 140-2 compliance is required.</p> <p>Key: <ESP_registry_location> Value name: CSPDoNotEnforceRSAPublicKeyExponentLength Value Type: DWORD Default value data: 0</p> <p>Allowed values: 0 or 1</p>

Table 60: Miscellaneous settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>When this setting is enabled, Security Provider removes all entries and certificates from the Other People certificate store.</p> <p>Key: <ESP_registry_location> Data Name: DeleteOtherPeopleCertsAtLogout Data Type: DWORD Values: 0 or 1</p> <p>0 - Don't delete certificates from the Other People certificate store on Windows logout.</p> <p>1 - Delete certificates from the Other People certificate store on Windows Logout.</p> <p>The Enhanced Logout feature must be enabled for this feature to work (<code>DisableEnhancedLogout</code>) should not be set to 0.</p> <p>Note: By default, Enhanced Logout is enabled.</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>By default, users with large keys larger than those specified in FIPS guidelines, (RSA4096, for example), are accepted by Security Provider's CSP. To conform to FIPS 140-2 guidelines Security Provider's CSP can be configured to accept only key lengths of 1024, 2048, or 3072 bits. Setting this value to 1 disallows the use of larger key lengths. If this value is set to 0 (the default), the larger key lengths are accepted.</p> <p>Key: <ESP_registry_location> Value Name: CSPEnforceRSAKeyPairLength Data Type: DWORD Default value data: 0</p> <p>Allowed values: 0 or 1</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Prevents Security Provider from managing certificates created with Entrust TruePass 6.0. This setting is optional and is intended for backwards compatibility only.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: DisableTruePassManagement Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Enable management.</p> <p>1 = Disable management.</p>

Table 60: Miscellaneous settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Enables an enrollment station. When users enroll or recover, their certificates are never saved to the local Personal certificate store. Users can enroll using the Entrust Enhanced Cryptographic Provider or a smart card vendor's CSP. This setting is optional. See "Configuring an enrollment station" on page 106 for more information.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: EnrollmentStation Value Type: REG_DWORD Value Data: <0-1></p> <p>0 (default) = Disable enrollment station: certificates are not copied to the local Personal certificate store.</p> <p>1 = Enable enrollment station: certificates are copied to the local Personal certificate store.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Determines if file names that include non-ASCII characters will be UTF-8 encoded in the MIME layer of an S/MIME-encoded file. Set this to 1 if you transfer or share files between countries or users where some computers may not be configured to support non-ASCII characters in file names.</p> <p>This setting maps to the following registry value:</p> <p>Key: <ESP_registry_location> Value Name: FileUTF8FilenameEncoding Value Type: REG_DWORD Value Data: <0 or 1></p> <p>0 (default) = Disable UTF-8 encoding of file names.</p> <p>1 = Enable UTF-8 encoding of file names.</p>

Table 60: Miscellaneous settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	Sets how long the internal certificate cache files used by the KAS application are valid. When the cache lifetime expires, the KAS application deletes to cache files and generates new ones. This setting maps to the following registry value: Key: <ESP_registry_location> Value Name: KASCacheLifetime Value Type: REG_DWORD Value Data: <n> n = the number of hours before the cache expires. The default is 720 hours (30 days). A value of 0 specifies the cache does not expire.
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	This setting prevents Security Provider from automatically selecting the native smart card CSP. This is useful, for example, if you are using a non-Entrust smart card and you want to use "Any SC" in Entrust Authority Security Manager Administration's "CSP to manage keys" setting. Key: <ESP_registry_location> Value Name: PreventSmartCardNativeSelectReaderUI Value Type: REG_DWORD Value Data: <1_or_0> Default is 0 A value of 1 enables the setting.

Table 60: Miscellaneous settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p> <p>Allows you to identify known problem CA certificates.</p>	<p>Security Provider has the concept of a known problem Certification Authority (CA) certificate. A known problem CA certificate may cause certificate chain development issues or some other issue within your environment. Once a CA certificate has been configured as a known problem, Security Provider will skip it when importing certificates to the Intermediate Certification Authorities and Trust Root Certification Authorities certificate stores. Security Provider can also be configured to remove known problem CA certificates from these stores when doing normal management operations.</p> <p>To specify a CA certificate as a known problem CA certificate, add the following configuration setting to the registry:</p> <p>Key: <ESP_registry_location>\KnownProblemCACertificates</p> <p>Value Name: <any description of the certificate desired></p> <p>Value Type: REG_SZ</p> <p>Value: HEX encoded SHA-1 hash of the certificate</p> <p>To specify that Security Provider should remove any specified known problem CA certificates, add the following configuration setting to the registry:</p> <p>Key: <ESP_registry_location></p> <p>Value Name: RemoveKnownProblemCACertificates</p> <p>Value Type: REG_DWORD</p> <p>Value: If set to 0, known problem CA certificates are not removed. If set to 1 (the default if not specified), known problem CA certificates are removed if they exist during the Security Provider digital ID management operations.</p>

Logging settings

You configure the logging settings using Microsoft Group Policy, the **Custom Installation** wizard, or through the Windows registry editor.

Note: For the logging settings, <ESP_registry_location> is not configured under the current user registry location. The logging service runs under system account.

Table 61 describes the logging settings. These settings are further explained in [“Troubleshooting” on page 313](#).

Table 61: Logging settings

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Specifies the full path and name of the log file. The log file contains information on the feature that logged the message, an event identifier, as well as other information. See “Security Provider for Windows logs” on page 314 for more information.</p> <p>Add the following registry value:</p> <p>Key: <ESP_registry_location>\Logging Value Name: LogFile Value Type: REG_EXPAND_SZ Value Data: <path_and_name_of_log_file_xml></p> <p>The default is: \Program Files\Common Files\Entrust\ESP\Logging\logfile.xml (32-bit machines)</p> <p>or</p> <p>\Program Files (x86)\Common Files\Entrust\ESP\Logging\logfile.xml (64-bit machines)</p>

Table 61: Logging settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Specifies the logging level for the log file. There are five logging levels. When changing the logging level, you do not need to perform a reboot.</p> <p>To configure the log level, set the following registry value:</p> <p>Key: <ESP_registry_location>\Logging Value Name: LogLevel Value Type: REG_DWORD Value Data: <0-4></p> <p>0 — Log level off 1 — Error log level 2 (default) — Warning log level 3 — Information log level 4 — Detailed log level</p>
No wizard setting You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.	<p>Specifies the maximum size of the log file in kilobytes. The maximum size must be greater than 100 KB.</p> <p>Add the following registry value:</p> <p>Key: <ESP_registry_location>\Logging Value Name: MaxLogSize Value Type: REG_DWORD Value Data: <number_of_kilobytes></p> <p>The default is 512.</p>

Table 61: Logging settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Specifies the overwrite behavior for the log file.</p> <p>Add the following registry value:</p> <p>Key: <ESP_registry_location>\Logging Value Name: OverwriteLog Value Type: REG_DWORD Value Data: <0-1></p> <p>0 = If the XML log file reaches its maximum size (as specified in the MaxLogSize entry), the following two checks take place:</p> <ul style="list-style-type: none"> • Can a new backup log file be added? If yes, a new XML file is created with an index number not exceeding the number of backup log files allowed in the MaxBackupLogFiles setting. • Has the maximum number of log files been reached? If yes, remove 5% of the oldest event logs and write all new events to the log file. <p>1 (default) = When the log file is full, 5% of the oldest event logs are removed and all new events are written to the log.</p>
<p>No wizard setting</p> <p>You can specify this setting's registry value on the Specify Additional Registry Values page of the Custom Installation wizard.</p>	<p>Maximum number of backup log files allowed.</p> <p>Add the following registry value:</p> <p>Key: <ESP_registry_location>\Logging Value Name: MaxBackupLogFiles Value Type: REG_DWORD Value Data: <number_of_log_files></p> <p>The default is 15.</p>
<p>No wizard setting</p> <p>Manually add this registry setting to the computer experiencing problems. To open the registry, type regedit at a command line.</p>	<p>Specifies the folder in which to create the PKIX-CMP dump files. Security Provider for Windows creates the folder if it does not exist. See "PKIX-CMP messages" on page 320 for more information.</p> <p>Add the following value to the registry:</p> <p>Key: <ESP_registry_location>\Logging Value Name: PKIXCMPDumpLocation Value Type: REG_SZ Value Data: C:\PKIXCMPDumpLocation</p> <p>Example:</p> <p>Value Data: C:\PKIXCMPDumpLocation</p>

Table 61: Logging settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
No wizard setting Manually add this registry setting to the computer experiencing problems. To open the registry, type <code>regedit</code> at a command line.	<p>Specifies the folder in which to create the policy certificate dump files. Security Provider for Windows creates the folder if it does not exist. See “Policy certificate messages” on page 318 for more information.</p> <p>Adds the following value to the registry:</p> <p>Key: <ESP_registry_location>\Logging Value Name: PolicyCertDumpLocation Value Type: REG_SZ Value Data: C:\PolicyCertDumpLocation</p> <p>Example:</p> <p>Value Data: C:\PolicyCertDumpLocation</p>
No wizard setting Manually add this registry setting to the computer experiencing problems. To open the registry, type <code>regedit</code> at a command line.	<p>Specifies the folder in which to create the auto-enrollment dump files. These files contain all auto-enrollment requests and responses, and are used to troubleshoot auto-enrollment problems. The dump files are in XML format and are named <code>Auto_Enroll_Request.txt</code> and <code>Auto_Enroll_Response.txt</code>. If a file by the same name already exists in the folder, Security Provider overwrites it.</p> <p>Attention: To minimize the risk of exposing this secure information, enable the log files only for troubleshooting purposes and disabled the key as soon as possible.</p> <p>Add the following value to the registry:</p> <p>Key: <ESP_registry_location>\Logging Value Name: AutoEnrollMessageDumpLocation Value Type: REG_SZ Value Data: <Path_to_dump_folder></p> <p>Example:</p> <p>Value Data: c:\temp</p>

Table 61: Logging settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>Manually add this registry setting to the computer experiencing problems. To open the registry, type <code>regedit</code> at a command line.</p>	<p>Specifies the folder in which to create the CardMS dump file. This file contains all CardMS messages, and is used to troubleshoot CardMS problems. The dump file is called <code>CardMS_Updater_Request.der</code>. If a file by the same name already exists in the folder, Security Provider overwrites it.</p> <p>To read this file, you must decode the <code>.der</code> files with a DER decoder. DER decoders are available online.</p> <p>Attention: To minimize the risk of exposing this secure information, enable the log files only for troubleshooting purposes and disabled the key as soon as possible.</p> <p>Add the following registry value:</p> <p>Key: <code><ESP_registry_location>\Logging</code> Value Name: <code>CardMSUpdaterMessageDumpLocation</code> Value Type: <code>REG_SZ</code> Value Data: <code><Path_to_dump_folder></code></p> <p>Example:</p> <p>Value Data: <code>c:\temp</code></p>
<p>No wizard setting</p> <p>Manually add this registry setting to the computer experiencing problems. To open the registry, type <code>regedit</code> at a command line.</p>	<p>Specifies the folder in which to create the OCSP dump files for troubleshooting purposes. Two dump files are created:</p> <ul style="list-style-type: none"> <code><serial#_of_cert_being_checked_for_revocation>_request.der</code> <code><serial#_of_certificate_being_checked_for_revocation>_response.der</code> <p>To read these files, you must decode the <code>.der</code> files with a DER decoder. DER decoders are available online.</p> <p>If a file by the same name already exists in the folder, Security Provider overwrites it.</p> <p>Specify the following registry value:</p> <p>Key: <code><ESP_registry_location>\Logging</code> Value Name: <code>OCSPDumpLocation</code> Value Type: <code>REG_SZ</code> Value Data: <code><Path_to_dump_folder></code></p> <p>Example:</p> <p>Value Data: <code>c:\temp</code></p>

Table 61: Logging settings (continued)

Setting name and location in Custom Installation wizard	Description and registry value
<p>No wizard setting</p> <p>Manually add this registry setting to the computer experiencing problems. To open the registry, type regedit at a command line.</p>	<p>When this setting is used (set to 1) a standard set of details about the certificate context, certificate chain context, or CRL context is sent to a file that is stored in the user's local data folders. The context is dumped to the file and the file is zipped to save disk space. The filename and path are written to the log entry.</p> <p>Key: <ESP_registry_location>\Logging Value Name: LogBinaryDetails Value Type: REG_DWORD Value Date: <0, 1></p> <p>0 (default) - Log certificate, certificate chain and CRL context information only.</p> <p>1 - Save certificate, certificate chain and CRL context to the file and log their information.</p> <p>An example of certificate entry details using 1 is:</p> <p>The pIssuerCert member in the CERT_REVOCATION_PARA structure is specified. Certificate context information: The certificate is saved to C:\Documents and Settings\Administrator\Local Settings\Application Data\Entrust\ESP\LogBinaryDetails\eecertificate_WCL1F3.zip. Serial Number: 4287 2D4C (1116155212) Issuer: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), O=Entrust.net, C=US Valid From: 2007-01-05T15:20:39.000+05:00 Valid To: 2017-01-05T15:50:39.000+05:00 Subject: CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc. ", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc. ", C=US</p> <p>An example of certificate chain details using 1 is:</p> <p>Start the base chain policy verification checks... Certificate chain context information: The certificate chain context is saved to C:\Documents and Settings\Administrator\Local Settings\Application Data\Entrust\ESP\LogBinaryDetails\eechain_WCC1F8.zip. The number of simple chain is 1. The number of lower quality chain context is 0. Combined trust error of the simple chains: No error found for this certificate or chain. (0x0) Combined trust information of the simple chains: The certificate or chain has a preferred issuer. This status code applies to certificates and chains. (0x100)</p>

Entrust email certificate exchange settings

The settings in Table 62 allow you to configure some aspects of the behavior of the automatic email exchange feature. These settings can also be used with Entrust Solo.

For <ESP_registry_location> use the registry key that applies to your installation:

- HKEY_CURRENT_USER > SOFTWARE > ENTRUST > ESP
Use this registry key if you want the settings to apply only to the currently-logged in user.
- HKEY_CURRENT_USER > SOFTWARE > POLICIES > ENTRUST > ESP
Use this registry key if you want the settings to apply only to the currently-logged in user and you are using Group Policy to push out the settings.
- HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP
Use this registry key if you want the settings to apply to all users of the computer and you are using a 32-bit operating system.
- HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432Node > ENTRUST > ESP
Use this registry key if you want the settings to apply to all users of the computer and you are using a 64-bit operating system.
- HKEY_LOCAL_MACHINE > SOFTWARE > POLICIES > ENTRUST > ESP
Use this registry key if you want the settings to apply to all users of the computer, and you are using Group Policy to push out the settings, and you are using a 32-bit operating system.
- HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432Node > POLICIES > ENTRUST > ESP
Use this registry key if you want the settings to apply to all users of the computer, and you are using Group Policy to push out the settings, and you are using a 64-bit operating system.

Table 62: Email exchange settings

DigitalIDEmailMessage	<p>Use this setting to customize the email message used when you are exchanging certificates. Enter your customized message in a text file and enter the full path and the name of the file as the value. If Security Provider cannot find the file it will use the default message.</p> <p>Key: <ESP_registry_location> Type: REG_SZ Value: <String> Default = Default email message</p> <p>Where <String> is the complete path and filename of the text file.</p>
DigitalIDEmailAttachmentZipped	<p>Use this setting to specify that attached certificates should be zipped.</p> <p>When zipping certificates, a randomly generated password is created to protect the content. The user emailing certificates must provide the password to the other recipient. The email message is changed to provide information about importing these certificates.</p> <p>Key: <ESP_registry_location> Type: REG_DWORD Value: <1_or_0> Default = 0</p> <p>0 = Do not zip certificates 1 = Zip certificates and attach to email</p>
DigitalIDEmailAttachCertificates	<p>Use this setting to attach certificates in CER format.</p> <p>Note: Some email applications regard CER files as potentially dangerous and strip them out of email. If you get a warning indicating that the CER file is regarded as a threat, you can attach the certificates as a ZIP bundle.</p> <p>Key: <ESP_registry_location> Type: REG_DWORD Value: <1_or_0> Default = 0</p> <p>0 = Do not attach in CER format 1 = Attach in CER format</p>

Table 62: Email exchange settings (continued)

DigitalIDEmailAttachP7CFile	Use this setting to attach certificates in P7C format. Key: <ESP_registry_location> Type: REG_DWORD Value: <1_or_0> Default = 1 0 = Do not attach P7C file 1 = Attach P7C file

Entrust digital ID and security store versions and contents

Entrust digital IDs have two versions: V1 and V2. Similarly, Entrust security stores have two versions: v3 and v4. The version (V1/V2, and v3/v4) determines the contents of the digital ID and security store.

Note: Third-party security stores are outside the scope of this appendix.

Table 63 and Table 64 indicate which Entrust security store and Entrust digital ID versions your users may have, and what their contents may be.

Table 63: Entrust security store version and contents

If this application created the Entrust security store...	Against...	Then the Entrust security store version is...	And the Entrust security store contains...
Entrust TruePass 8.1	Security Manager 8.x	v4	A full certificate history
Security Provider/Security Toolkit for the Java Platform 7.x or 8.x	Security Manager 7.x or 8.x	v4	A full certificate history

Table 64: Entrust digital ID version and contents

If this application created the Entrust digital ID...	Against...	Then the Entrust digital ID version is...	And the Entrust digital ID can contain...
Entrust TruePass	Security Manager 8.x	V2	any number of key pairs
Security Provider/Security Toolkit for the Java Platform8.x	Security Manager 8.x	V2	any number of key pairs

How Security Provider upgrades V1 digital IDs and V3 Entrust security stores

This section outlines when and how these upgrades are done.

- When Security Provider does a management check, Security Manager will convert V1 digital IDs to V2.
- When a user logs into their v3 Entrust security store and the registry setting `DisableAutomaticEntrustSecurityStoreUpgrade` is set to 0 (the default, enabling automatic migration) ESP downloads the certificate history from Security Manager and upgrades the security store to v4.
- If a key in the Entrust security store is updated, v3 is updated to v4 but the certificate history is not downloaded.

1-key pair	single key pair that consists of a public key, used for both encryption and verification, and a private key, used for both decryption and signing, to allow interoperability with third-party S/MIME products - formerly called single key pair
2-key pair	set of two-key pairs; one encryption, which allows users to encrypt data in order to keep the data private, and one signing, which allows users to digitally sign data to provide authentication (guarantees who signed the data), data integrity (recipients of signed data are alerted if the data was tampered with), and nonrepudiation (a user cannot deny having signed the data) - formerly called dual-key pair
3-key pair	set of three key pairs; the 2-key pairs defined in 2-key pair in addition to one of either a nonrepudiation signing key pair or a Microsoft EFS encryption key pair
4-key pair	set of four key pairs; the 2-key pairs defined in 2-key pair, in addition to one nonrepudiation signing key pair and a Microsoft EFS encryption key pair
API	see application program interface (API)
activation codes	reference number and authorization code that are generated when an Entrust Administrator adds or recovers a user using Entrust Authority Security Manager Administration, or when users add or recover themselves using Entrust Authority Administration Services.
administrator	persons who configure and manage Security Provider for Windows or other Entrust products that need specific configuration for Security Provider for Windows to work
AIA (Authority Info Access)	a certificate extension

application program interface (API)	set of common building blocks in the form of routines, protocols, and tools provided for programmers to write applications consistent with the operating environment
authorization code	alphanumeric code (for example, CMTJ-8VOR-VFNS) generated when an administrator creates a new user or recovers an existing user, required along with its corresponding reference number
CA	see Certification Authority (CA)
CDP	see CRL distribution points
CRL	see certificate revocation
CRL distribution points (CDP)	points uniquely distributed throughout a directory containing multiple CRLs, enabling user's certificates to contain a pointer to the appropriate distribution point in order for Entrust client software, such as Security Provider for Windows, to find the corresponding CRL for a given certificate
CSP	see Cryptographic Service Provider
certificate	a collection of information in a standard format that is digitally signed by a Certification Authority (CA)
Certification Authority (CA)	part of Security Manager that ensures the trustworthiness of electronic identities; it issues electronic identities in the form of public key certificates, policy certificates, cross-certificates, certificate revocation lists, and authority revocation lists, and signs the certificates with its signing key thereby ensuring the integrity of the electronic identity
certificate revocation list (CRL)	signed and timestamped certificate containing the serial numbers of public key certificates that were revoked, and a reason for each revocation
certificate store	contains user and machine certificates, and keeps track of the CSP associated with each certificate
certificate type	is defined using certificate definitions and determines how Security Manager customizes certificates issued for a particular type
computer	machine used to enroll an Entrust digital ID for computer
CryptoAPI	Microsoft Windows API that provides PKI client capabilities to the desktop operating system, allowing applications to take advantage of desktop cryptographic functionality built in by Microsoft
Cryptographic Service Provider (CSP)	acts as an interface between Microsoft CryptoAPI and private key stores , and performs all cryptographic operations for Microsoft applications and any third-party applications that are properly built on the Windows security framework, such as encrypting and decrypting data, verifying signatures, signing data, and verifying certificates

DN	see distinguished name
directory	LDAP-compliant directory service containing the name of all Entrust Authority Security Manager users, acts as repository for users' encryption public key certificates
decryption private key	decrypts data that was encrypted with its corresponding encryption public key ; for example, Bob is the only user who has access to his decryption private key, which he uses to decrypt information that was encrypted for him by other users with his encryption public key
desktop user	a user whose Entrust digital ID is stored in an Entrust desktop security store, located in an <code>.epf</code> file
digital ID	set of cryptographic data that defines an entity, consisting of a public portion (user's public key certificates) and a private portion (user's private keys), and can verify one's identity
distinguished name (DN)	complete name of directory entry that uniquely identifies a person or entity; DNs of all Entrust Authority Security Manager users are stored in the directory
EFS decryption private key	decrypts EFS data that was encrypted with its corresponding EFS encryption public key
EFS encryption key pair	contains an EFS encryption public key and associated EFS decryption private key
EFS encryption public key	encrypts data specifically to support the EFS format that can be decrypted with the corresponding EFS decryption private key
encryption key pair	contains an encryption public key and associated decryption private key
encryption public key	encrypts data that can be decrypted with the corresponding decryption private key
end user	a user who has successfully enrolled for an Entrust digital ID using Security Provider for Windows
Entrust desktop security store	see <code>.epf</code>
Entrust digital ID	digital ID that is created, protected, and managed by Entrust; stored in one of more of the following: Entrust security store and third-party security store
Entrust digital ID for computer	digital ID that is created, protected, and managed by Entrust; stored in a Microsoft certificate store which is not password-protected; used to identify the computer itself

Entrust digital ID for Windows Services	digital ID that is created, protected, and managed by Entrust; stored in a Microsoft certificate store which is not password-protected; used to identify the Windows service
Entrust roaming security store	password protected Entrust security store file, located in a directory; stored and accessed only when a user's computer is connected to Entrust Authority Roaming Server
Entrust security store	password protected file, acting as a storage medium for a user's Entrust digital IDs when created with an Entrust CSP
.epf file	password protected Entrust security store file, located on user's desktop computer; sometimes referred to as an Entrust desktop security store
extended enterprise environment	configuration in which network communication takes place beyond the context of an internal organization, typically across one or more firewalls (defined as such for the purpose of this document)
IDP (Issuing Distribution Point)	an extension in the CRL
key	special number that an encryption algorithm uses to change data, making it secure
key history	collection of decryption private keys belonging to a user, stored by Entrust Authority Security Manager
key lifetime	length of time a key is valid; all keys have specific lifetimes except the decryption private key which never expires
key pairs	asymmetric keys come in pairs; Security Provider for Windows uses asymmetric keys in both encryption and digital signature operations
key recovery	process of generating new activation codes for a user who has lost their security store or has forgotten their password
key store	also called a security store, it holds private keys for users and machines and makes them accessible to the CSP that manages it
key update	replaces old key pairs with new ones and new public key certificates are created; new keys and certificates have no relation to the old keys and certificates; users receive new keys and certificates securely
Microsoft certificate store	see certificate store
.msi file	installer database (Windows installer package) containing the instructions and data required to install an application; can include one or more transform files (.mst files)
.mst file	collection of changes called a transform file that can be applied to a Windows Installer package (.msi file)
nonce	arbitrary number that is generated for security purposes.

nonrepudiation	irrefutable evidence that makes it impossible to reject the validity of one's signature on a file or transaction; an Entrust digital signature provides nonrepudiation
nonrepudiation signing key pair	used for users in high-assurance positions who require separate digital signature and nonrepudiation keys and contains a nonrepudiation signing private key and a nonrepudiation verification public key
nonrepudiation signing private key	encrypts a hash value that is decrypted with the corresponding nonrepudiation verification public key
nonrepudiation verification public key	public key portion of a nonrepudiation signing key pair used to verify data that was signed by the corresponding nonrepudiation signing private key
personal encryption group (PEG)	A PEG is a self-defined group of individuals for which you can encrypt files. Personal Encryption Groups are useful if you regularly encrypt information for the same group of people. For example, if there is a sales team to which you regularly encrypt documents, you can create a PEG called 'sales team' and specify the sales team PEG when you encrypt the documents as opposed to specifying each individual.
policy certificate	defines privileges for users according to their roles; used to set user policies
PKIX-CMP protocol	secure communications protocol used to handle requests between Security Provider for Windows and the Security Manager CA
private key	portion of a key pair that is kept secret by the owner of the key pair
recovery	operation performed on users who lose or corrupt their security store; the operation generates new signing key pair, retrieves current encryption public key certificate, decryption private key history, verification public key certificate, and CA verification public key certificate
reference number	number (for example, 91480165) generated when an administrator creates a new user or recovers an existing user, required along with its corresponding authorization code
roaming user	when user's Entrust digital ID is stored in an Entrust roaming security store, located in the directory, and user's computer is connected to Entrust Authority Roaming Server
root certificate store	storage medium for the CA certificate when Microsoft Active Directory is not being used
security store	storage medium for users' Entrust digital ID; see Entrust security store and third-party security store
single-key pair	see 1-key pair
signing-key pair	contains a signing private key and a verification public key

signing private key	encrypts a hash value that is decrypted with the corresponding verification public key ; for example, Alice is the only user who has access to her signing private key, which she uses to encrypt the hash value of a file she is signing, and users verify the signature by successfully decrypting the hash value using Alice's verification public key
standard enterprise environment	configuration in which network communication takes place internally within the context of an organization (defined as such for the purpose of this document)
third-party security store	storage medium for a user's Entrust digital ID that is commonly password protected, owned by a third-party vendor, and managed by Entrust
thumbprint	A thumbprint is a string of letters and numbers that is generated by Entrust Entelligence Security Provider to be used as a test that the certificates have not been tampered with during the email exchange. If the certificates that are received have been tampered with, the thumbprint produced on the receiving end will not match the thumbprint recorded by the sender.
transform file	see .mst file
V1, V2, v3, v4	a version-1, version-2, version-3, or version-4 certificate
V1-key-pair	key pair that has only client settings policy attached to the certificate; is created using a pre-7.x version of Security Manager and encompasses 1-key-pair and 2-key-pair
V2-key-pair	key pair that has Certificate Definition Policy attached to the certificate; is created using Security Manager 8.x and encompasses 1-key-pair , 2-key-pair , 3-key-pair , and 4-key-pair
verification public key	public key portion of a signing key pair used to verify data that was signed by the corresponding signing private key and is stored in the verification public key certificate
verification public key certificate	verifies that the verification public key within it is the authentic public key of the identified user through its digital signature, which is signed by the CA

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

3DES algorithm 133, 134

A

About

- dialog box 324
- Entrust Entelligence Security Provider 25
- Microsoft® Windows® security framework 35

Activation codes 148

- definition 501
- during enrollment 66
- during manual user enrollment 71

Active Directory

- overview 32
- specifying 335

Address Book, see PAB

Administration Services 33, 148

administrative install 297, 299

AES algorithms

- supported 130, 131, 132, 133, 134

AES0170 error code 159

AIA 140

algorithms

- for encryption .epf 415
- for key pair setting 262
- registry setting 356, 415, 432, 433, 434, 435, 443, 444
- supported 130, 131, 132, 133, 134

Allow unsuccessful login/reauthentication attempts 403

AllowAutoEnrollServerToRecoverIfActive setting 366

Any SC 183, 260

anyExtendedKeyUsage EKU 206

AppendToEPFName setting 409

application program interface (API)

- definition 502

application-initiated login process 92

App-V 199

architecture 31

archived keys

- checking 55
- show 466
- storing by original CSP 80

ASCII 486

authenticate

- how users 52
- with nonrepudiation key 53

Authority setting 349

Authorization code 148

- definition 502
- during enroll/recover 71
- during enrollment 66

Auto-associating certificates in Microsoft Outlook 255

auto-enrollment

- retry behavior 159
- settings 361

Auto-enrollment Service 33

Auto-enrollment settings

- AllowAutoEnrollServerToRecoverIfActive 366
- AutoEnrollDisableRecoveryWizardCancel 366
- AutoEnrollMachineDigitalIDType setting 363
- AutoEnrollMachineURL 362
- AutoEnrollNumberOfRetries 363
- AutoEnrollRetryInterval 364
- AutoEnrollUserDigitalIDType 362
- AutoEnrollUserURL 362
- SkipAutoEnrollRecoverNotification 364
- UseAutoEnrollServerForManualOperations 365

automatic

- additional certificate download 100
- enrollment/recovery 65
- move user feature 83

Available digest algorithm 435

Available encryption algorithm 433

- default 434

B

backup

- certificate 55
- key 67, 82
- private key 263

base chain policy check 141

C

CA

- certificates downloading 100
- definition 502
- Display order 350
- DN during enroll/recover 66
- Friendly Name 351
- friendly name 349
- hide this CA during enrollment and recovery 350
- hiding 75, 78
- host name or IP address 349
- no display in wizard 75, 78
- overview 32
- port number 349
- settings 348, 352

cache

- clearing 249
- internal 89

CardMS

- DLLPath setting 370
- Name of CardMS client setting 370
- settings 368

CardMS settings

- CardMSUpdatesPerformedBy 370

CA-specific directory setting

- DirectoryName 354

CA-specific OCSP Responder settings

- OCSPResponderURLs 368

CAST algorithms

- supported 130, 131, 132, 133, 134

CDP, see CRL Distribution Point

Cert update date 261

certificate

- archived 67
- caching 249
- created on enroll 67
- definition 502
- deleting 235
- discovery settings 470
- editing properties of 235
- extension checking 141
- extension settings 470
- history 83
- importing/exporting 235
- path discovery 141
- path discovery, customizing 144
- path or chain 92
- path validation 141

- path validation, customizing 145
- policy validation 54
- prevent copying to store 106
- processing 54
- root CA certificate 141
- validation settings 470
- viewing content of 235
- viewing from remote computer 107, 114

certificate definition

- implications of adding/removing 83

certificate definition policy 93

- and Security Manager 8.x 259

certificate encryption 452

Certificate Explorer

- about 234
- hiding 480
- PAB import 102
- settings 463

certificate history

- in Personal certificate store 55
- see also key history 55

Certificate Path Critical Extension Policy Provider 143

Certificate path settings

- CASearchResultLifetime 471
- InitialAnyPolicyInhibit 471
- InitialExplicitPolicy 472
- InitialPolicyMappingInhibit 472
- InsecureCertHashAlgorithms 474
- OID for critical extension 473
- RetrieveExtraCertsInterval 470
- UserInitialPolicySet 471
- WeakCertHashAlgorithms 475

certificate revocation list (CRL) 136

- definition 502

certificate store

- and CryptoAPI 37
- definition 502

certificate type

- 1 key pair 96
- 2-key-pair 96
- and Security Manager 8.x 92
- changing 83
- choosing 98
- definition 502
- EFS (two key pair) 97
- nonrepudiation 98
- nonrepudiation and EFS 98
- Smart Card Logon 98

■ 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 ■

- certificate, self-signed 160
- certificates
 - checking with OCSP 139
 - downloading intermediate CA 142
- Certification Authority (CA)
 - definition 502
 - see also CA
- chain
 - see certificate path validation
- Cisco VPN Client 43, 82
- clearing the cache 249
- Client definition settings policy certificate
 - key usage policy setting 93
- Client settings policy
 - definition 92
- cn OID 410
- command
 - dumpall 248
- communication
 - protocol setting 336
 - with the CA 92
- computer digital ID 50
 - enrollment/recovery 107, 114
 - updates 86, 87
- Computer Digital ID Service
 - and management 86, 87
 - disabling 470
- Computer Digital ID Snap-in 107
- Connection time limit (in seconds) 336
- context menus
 - add extra text to 438
- critical extensions 141, 146
 - checking 137
 - customizing checks of 146
 - OID 473
 - OID setting 472
- CRL
 - and multiple CAs 137
 - cache lifetime 421
 - checking critical extensions 137
 - checking serial numbers 137
 - definition 502
 - Distribution Point 136
 - definition 502
 - download problems 423
 - how they are checked 137
 - Revocation Provider 136, 423
 - Revocation Provider settings 419

- CRL caching 249
- CRL Revocation Provider
 - settings 419
- CRL Revocation Provider settings
 - 420, 423, 424
 - CRLCacheLifetime 421
 - EnableCRLCache 421
 - FileConnectTimeLimit 422
 - FTPConnectTimeLimit 422
 - ProblemCDPCacheLifetime 423
 - SkipDirectoryNameInCDP 422
- cross certificates
 - downloading 100
- CryptoAPI 37
 - and Microsoft Outlook 43
 - applications 42
 - components in 36
 - definition 502
 - how it works 37
 - overview 36
 - private key store 38
 - see also Microsoft Windows
 - standards 37
- CSP 38, 50, 129
 - definition 502
 - Entrust Elliptic Curve CSP 28, 132
 - Entrust Enhanced 129
 - Entrust Enhanced Cryptographic Provider 38
 - Entrust Key Access Service 131
 - Entrust Symmetric 130
 - generating within smart card 183
 - KAS 89
 - Microsoft Base Cryptographic Provider 38
 - Microsoft Base Cryptographic Provider v1.0 50
 - Microsoft Enhanced Cryptographic Provider 50
 - Microsoft RSA SChannel Cryptographic Provider 50
 - Microsoft Strong Cryptographic Provider 50
 - smart card 183, 186
 - that create computer IDs 50
- Custom Installation Wizard
 - configuration 290
 - Default button 346
- Customer support 21
- customer support utility 248

D

- Data Recovery Agent 42

- Deactivating a user 277
- Decryption private key
 - definition 503
- Default
 - button in custom install wizard 346
 - encryption algorithm 434
 - Entrust Security Store timeout (in minutes) 410
- Default directory setting
 - Default 346
- default policy setting for Timestamp 448
- delete
 - plaintext 437
- deployment
 - architecture 31
 - worksheet 282
- DES algorithm 130, 132, 133, 134
- Desktop
 - permissions 255
 - user 503
- dialog box
 - About 324
 - hide 376, 397, 404
- Diffie-Hellman 132
- digest algorithm
 - mandatory 435
- digital ID
 - compare Entrust and non-Entrust 47
 - CSPs for computer IDs 50
 - defined 45
 - definition 503
 - exact locations 49
 - for computer 48
 - for computer enrollment/recovery 107, 114
 - for computers 47
 - for users 47
 - management 82
 - settings 373, 389, 392
 - silent update 86, 87
 - storage locations 48
 - types 46
- Digital ID Monitor
 - disabling 470
- Digital ID settings 389
- Directory 32
 - Authentication Method 337
 - connection settings 332
 - default settings 344
 - definition 503
 - Friendly Name 333
 - host name, port 333
 - overview 32
 - placing CA certs in 100
 - Proxy Order 339
 - search settings 341
 - tab for 354
- Directory connection settings
 - ActiveDirectory 335
 - ADDDiscoveryInterval 335
 - AuthenticationMethod 337
 - CertPropFriendlyNameFormat 340
 - DirectoryConnectTimeLimit 336
 - LDAPBindAnonymousFirst 340
 - LDAPVersion 336
 - name setting 333
 - ProxyOrder 339
 - server and port 334
- Directory search settings
 - DirectoryOperationSizeLimit 343
 - DirectoryOperationTimeLimit 343
 - IgnoreDNsForCAsSearch 344
 - SearchBaseOrder 342
- DirectoryName setting 354
- DisableOfflineRoaming 174
- Display
 - order 350
 - personal folder 463
 - this CA during enrollment and recovery 350
 - version information 324
- Distinguished name
 - changes 276
 - definition 503
- DllNamePKCS11 setting 386
- DLLPath setting 370
- DN
 - during enroll/recover 66
- Do not show warning about Entrust security store with only archived certificates 397
- Do not show warning about read-only Entrust security stores 397
- Do not show warning about version 3 Entrust security stores 397
- downloading
 - CA certificates 100
- dump file 248
 - location 249
 - password 249

■ 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 ■

- dump files 318
 - certificate management 318
 - enrollment/recovery 318
 - location of 319
 - PKIX CMP 321
 - reading 318
 - see also logging
- DUMPALL command 248

E

- ECC algorithms
 - supported 133
- ECDH 132
- ECDSA 132
- EFS 54
 - and EKUs 205
 - and nonrepudiation 98
 - certificate processing 54
 - decryption private key 503
 - encrypted folders 42
 - encryption key pair 503
 - encryption menu 42
 - encryption public key 503
 - two key pair 97
 - user 97
- EKU
 - anyExtendedKeyUsage 206
- elliptic curve 28
- Email certificate exchange settings
 - DigitalIDEmailAttachCertificates 496
 - DigitalIDEmailAttachmentZipped 496
 - DigitalIDEmailAttachP7CFile 497
 - DigitalIDEmailMessage 496
- Email EKU 443
- enable
 - Entrust Authority Proxy Server 359
 - password attempt management 403
 - suspended store 253
- encrypting
 - files 42, 202
 - folders 42
- Encrypting File System 42, 82
 - see also EFS
- encryption algorithm
 - default 434
 - for .epf 415
- Encryption key pair

- definition 503
- Encryption public key
 - definition 503
- EncryptPasswordFilesForCert 452
- End user
 - activation 271
 - definition 503
- Enhanced key usage certificate extension
 - definition 93
- enroll
 - a computer digital ID 107, 114
 - for Entrust Digital ID wizard 69
 - procedure 69
 - processes 69
- enrollment
 - automatic 65
 - details for Security Manager 66
 - dump files 318
 - manual 65
 - of smart cards 180
 - overview 64
 - station 106
 - Web 65
- enrollment station
 - settings 486
- ent file 204
- Entrust Authority
 - Auto-enrollment Service 149
 - complementary Entrust Authority applications 33
 - Roaming Server description 33
 - Security Manager overview 32
 - Security Manager Proxy 178
 - Security Manager Proxy description 33
- Entrust CA
 - overview 32
 - see also Entrust Authority
 - see also Security Manager
- Entrust Certificate Explorer 234
 - see also Certificate Explorer
- Entrust Certificate Explorer settings
 - AppDataFolder 464
 - CertificateExplorerMode 468
 - DeleteKeyWhenDeleteCertificate 467
 - EnableEntrustKeyExport 466
 - EnableEntrustKeyImport 465
 - EnableEntrustPABImport 465
 - ExportPABToOtherPeopleStore 465
 - group by issuer order GroupN 467

- group by OU GroupN 467
- group by search Dir order GroupN 467
- ShowArchivedCertificates 466
- ShowCACertificates 464
- ShowPersonalCertificates setting 463
- ShowPersonalEncryptionGroups 466
- Entrust computer digital ID settings
 - ComputerRetryManagementOfflineAttempts 395
 - ComputerRetryManagementOfflineInterval 394
- Entrust desktop security store
 - definition 503
- Entrust Desktop Solutions
 - migration 101
- Entrust digital ID 47, 82
 - definition 503
 - Disable automatic Entrust Security Store upgrade 377
 - Do not show warning if digital ID is missing
 - certificates 376
 - for computer, definition 503, 504
 - Frequency (in minutes) at which the Entrust digital ID is
 - checked for updates 390, 393
 - Frequency (in minutes) to check for updates 375
 - Frequency (in seconds) to wait before retrying if server
 - is unavailable 375, 390, 394
 - Number of attempts to retry if server is
 - unavailable 376, 391, 395
 - see also digital ID
 - Update Request 85
 - versions 499
- Entrust Elliptic Curve CSP 28, 132
- Entrust Enhanced CSP 129
- Entrust Enhanced Key Storage Provider 134
- Entrust File Security settings
 - AllowedFileEncryptionAlgorithms 433
 - AllowedFileHashAlgorithms 435
 - DecryptionFolder 439
 - EnableCertificateStatusColumn 440
 - EncryptionContextMenu 439
 - FileAllowEmailProtectionEKU 443
 - FileAllowSMIMECompression 440
 - FileDeletePlainText 437
 - FileDeletePlainTextDefault 437
 - FileEncryptForOthers 441
 - FileEncryptForOthersDefault 440
 - FileEncryptionAlgorithm setting 432
 - FileEncryptionAlgorithmDefault 434
 - FileEncryptionAlgorithmLength 432
 - FileEncryptionAlgorithmLengthDefault 434
 - FileEncryptionSearchQuery 436
 - FileHashAlgorithm 435
 - FileHideEncryptExplorerMenu 442
 - FileHideEncryptSignExplorerMenu 442
 - FileHideSignExplorerMenu 442
 - FileOpenWithAttachmentManager 441
 - FilePrefixExplorerMenus 438
 - FileRestoreFileTimes 444
 - InsecureFileHashAlgorithms 444
 - LocalDecryptionFolder 439
 - PreventNetworkFileDecrypt 438
 - SkipFileOpenWatch 437
 - WeakFileHashAlgorithms 443
- Entrust IdentityGuard 191
- Entrust Key Access Service CSP 131
- Entrust policy certificates 54
- Entrust Ready identity device setting
 - IdentityLibrary 469
- Entrust Ready identity setting 469
- Entrust security store 52
 - Default folder 408
 - definition 504
 - desktop 48
 - digit rule 413
 - how certificates are processed 54
 - import 3rd party keys to 124
 - logout 54
 - lowercase rule 412
 - maximum length 411
 - nonalphanumeric rule 412
 - password lifetime setting 413
 - preset a folder 408
 - preset name of 409
 - read-only 84
 - roaming 48, 504
 - specify extra text 409
 - timeout setting 410
 - versions 499
- Entrust security store creation settings
 - AppendToEPFName 409
 - DefaultEntrustSecurityStoreTimeout 410
 - DefaultEntrustSecurityStoreType 407
 - DefaultFolder 408
 - DisableEPFSubCACertsCompatibility 416
 - EPFEncryptionAlgorithm setting 415
 - EPFNameFromDNAttribute 410
 - EPFNameLocked setting 415
 - FolderLocked 408

■ 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 ■

- MaxEntrustSecurityStoreTimeout setting 414
- NameLocked 409
- NumOfPreviousPasswordsToBeChecked
 - previous passwords setting 414
- PasswordLifetime 413
- PasswordMaxLength 411
- PasswordMinLength 411
- PasswordMustContainDigit 413
- PasswordMustContainLower 412
- PasswordMustContainNonAlphanumeric 412
- PasswordMustContainUpper 411
- Entrust security store login settings
 - AllowLoginToReadOnlyExpiredEPF 405
 - Default 403
 - DeleteCertsAtLogout 402
 - DisableEnhancedLogout 400
 - DisableOfflineRoaming 403
 - EnableSmartCardCertificateRemoval 381
 - HideQuickLinks 398
 - LoginQuickLinks 398
 - OfflineRoamingFolder 404
 - OfflineRoamingLifetime 404
 - PIVCustomQuickLinkEnabled 401
 - PIVCustomQuickLinkTarget 401
 - PIVCustomQuickLinkTitle 401
 - PIVEnforceAdminAssignedPINChange 382
 - PIVHiddenReaders 402
 - ReAuthQuickLink1Target 399
 - ReAuthQuickLink1Title 399
 - ReAuthQuickLinks 398
 - SkipArchivedCertsNag 397
 - SkipNoCertHistoryNag 397
 - SkipOfflineRoamingNag 404
 - SkipReadOnlyEPFNag 397
 - Target 399
 - Title 399
 - UnlockQuickLinks 398
- Entrust security store name
 - minimum length setting 411
 - uppercase rule 411
 - use DN for 410
- Entrust security store startup and shutdown settings
 - DeleteRoamCertsAtStartup 417
 - PromptForSecurityStoreLoginAtStartup 418
 - PromptIfNoCertificatesAtStartup 418
- Entrust Symmetric CSP 130
- Entrust TruePass 176
 - overview 33

- setting 485
- Entrust user digital ID settings
 - CertUpdateInterval 375
 - DisableAutomaticEntrustSecurityStoreUpgrade 377
 - DllNamePKCS11 386
 - DoNotUseExpiredSignKeyInPkixCMP 383
 - EffectOfLoginOnWaitingUpdate 381
 - EnableEDSProfileFullSync 387
 - EntrustProfilePath 387
 - IgnoreEntrustSecurityStoreUpdateUntilLogin 378
 - IgnoreUpdateAttempts 384
 - ImportCACertChainForNonVerificationCertificates 379
 - ImportPreviousCACertificates 379
 - MonitorSmartCardDelay 384
 - MonitorStartingDelay 383
 - PIVOptimizeWindowsLoginPerformances 385
 - PrivateKeyUsagePeriodPercentage 388
 - RemoveEDSSupport 386
 - RetryManagementOfflineAttempts 376
 - RetryManagementOfflineInterval 375
 - SaveEPFOnKeyManagemen 380
 - SkipMissingCertsNag 376
 - SkipUpdateAfterEntrustSecurityStoreLogin 377
 - SkipUpdateNotification 385
 - UpdateDigitalIDSilently 382
 - WizardVisibility 387
- EntrustProfilePath 387
- EPF
 - definition 504
 - encryption algorithm
 - encryption algorithm 415
 - import 3rd party keys to 126
 - see also Entrust security store
- ERL
 - import 103
 - migration 102
- error messages 316
 - see also logging
- event logs
 - for computer digital ID 107, 114
- expiry
 - password 55
 - setting for connections 476
- export
 - key file 105
 - Personal Encryption Group 103
- Extended enterprise environment
 - definition 504

- extended key usages 206
- extensions
 - checking 141
 - customizing checks of 146

F

- features, overview 26
- File Security application
 - overview 202
 - settings 430
- files
 - dump 248
 - monitoring decrypted 205
 - viewing properties of secured 204
- finding
 - version information 324
- firewall 31
- folder 42
 - for storing offline copy of Entrust roaming security store 404
- FolderLocked setting 408
- Force users to use default Entrust Security Store folder 408
- Force users to use default Entrust Security Store name 409
- ForceHttps 339
- four key pair
 - definition 501
- friendly name 340
- friendly setting for timestamp 449

G

- General CA settings
 - 349
 - Authority 349
 - CSP 352
 - DisplayOrder 350
 - Name 351
 - SelfAdminEnrollURL 351
 - SelfAdminRecoverURL 351
- Generate key at client 263
- Getting help
 - Technical Support 21
- group policy 285
 - see also Microsoft Group Policy 285
- GUI
 - customizing 478
 - settings 478

- GUI customization settings
 - EPFNamingDllName 481
 - HideCertExplorerInTrayMenu 480
 - HideEnrollInTrayMenu 479
 - HideHelpInTrayMenu 480
 - HideOptionsInTrayMenu 478
 - HideRecoverInTrayMenu 479
 - IncludeFullDNInName 480

H

- Hardened desktop environments 322
- help links
 - showing your own 399
 - specifying which to show 398
- hide
 - CA during enrollment and recovery setting 350
 - dialog box 376, 397, 404
 - menu options 479
 - quick help links 398
- HideQuickLinks setting 398
- HideSelfDecrypt setting 453
- history
 - certificate 55
- hot key 54
- How Security Provider works 45, 63, 123, 201, 499
- HTTP
 - settings 476
- HTTP connection and timeout settings
 - HTTPConnectTimeLimit 476
 - HTTPReceiveTimeLimit 476
 - HTTPSendTimeLimit 476
 - HTTPUserAgent 477

I

- icons
 - in taskbar 55
- IDEA algorithm 130, 131, 132, 133, 134
- IdentityGuard 191
- IdentityGuardURL 372
- IIS 43, 82
- IIS 7 compatibility 167
- import
 - 3rd party keys to .epf 126
 - Import a New Key dialog box 125
 - key file 105
 - PAB 102

■ 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 ■

- Personal Encryption Groups 103
- ImportPreviousCACertificates 379
- Inactivity timeout
 - configuring 255
- Include Additional Certificates 92
- Include Full DN 239
- Installation
 - choosing a distribution mechanism 304
 - of Security Provider 305
 - testing the installation package 303
- installation wizard
 - see Custom Installation Wizard
- installer
 - creating 285
 - packaging 297
 - testing 303
- Intermediate CA Certificate Store 100
- internal KAS cache 89
- Internet Information Server, see IIS

K

- KAS
 - application 89
 - CSP 89
 - smart cards 88
- key
 - backups 82
 - created on enroll 67
 - definition 504
 - file 105
 - history 67, 92
 - import and export 105
 - lifetime, definition 504
 - managing export of 256
 - one key pair 96
 - recovery, definition 504
 - store, definition 504
 - third-party 124
 - two key pair 96
 - update, definition 504
 - updates 82
 - usage policy 263
- key access certificates 249
- Key Access Service 88
- Key can sign CMP 262
- Key history
 - definition 504

- keys that are backed up 85
- key pairs
 - 1-key-pair user 96
 - 2-key-pair user 96
- definition 504
- EFS user 97
- nonrepudiation and EFS user 98
- nonrepudiation user 98
- number of allowable 500
- stand-alone EFS user 97
- supported 95
- Key Storage Providers 134
- key store 40
 - Microsoft 48
 - private 38, 40
 - Windows protected 40

L

- LDAP Directory
 - overview 32
 - see also Directory
- Lifetime of offline copy (in days) 404
- link certificates
 - downloading 100
- links
 - showing your own 399
 - specifying which to show 398
- locating a digital ID 48
- log file location 315
- log in
 - how users 52
 - initiated by application 92
 - timeout (minutes) 255
 - timeout period 54
 - to your security store 82
 - with nonrepudiation key 53
 - with smart card 182
- log out
 - locked 54
 - of Entrust security store 54
 - when it occurs 54
 - when screensaver activated 57
- Log service 314
 - getting log files 315
 - log viewing options 315
 - viewing log files 315
- logging

- customizing 314
- log files 314
- setting viewing options 315
- settings 489
- viewing 315
- Windows Installer 316
- Logging settings
 - AutoEnrollMessageDumpLocation 492
 - CardMSUpdaterMessageDumpLocation 493
 - LogBinaryDetails 494
 - LogFile 489
 - LogLevel 490
 - MaxBackupLogFiles 491
 - MaxLogSize 490
 - OCSPDumpLocation 493
 - OverwriteLog 491
 - PKIXCMPDumpLocation 491
 - PolicyCertDumpLocation 492
- Login attempts
 - Login attempt window 252
 - managing 252
 - Maximum bad login attempts 252, 253
- LoginQuickLinks setting 398
- logout 57
- logs
 - for computer digital ID 107, 114

M

- MAC 55
- management
 - defined 82
 - when it occurs 83
- Mandatory
 - digest algorithm 435
 - encryption algorithm 432
- mandatory
 - encryption algorithm 432
- manual enrollment/recovery 65
- Max key count 88
 - calculating 91
- max key count 90, 264
- Maximum number of characters 411
- Maximum number of entries to return from a Directory
 - search 343
- MD2 algorithm 130, 132, 133, 134
- MD5 algorithm 130, 132, 133, 134
- menu items

- add extra text to 438
- customizing 478
- hide 479
- messages
 - auto-enrollment, CardMS, OCSP 319
 - PKIX-CMP 320
 - see also dump files
 - see also error messages
 - see also logging
- Microsoft
 - Base Cryptographic Provider 38
 - Base Cryptographic Provider v1.0 50
 - certificate stores 39
 - CryptoAPI 37
 - CSP 38
 - Enhanced Cryptographic Provider 50
 - RSA SChannel Cryptographic Provider 50
 - Strong Cryptographic Provider 50
- Microsoft Application Virtualization 199
- Microsoft Group Policy 285
 - purpose 295
 - things that can't be set through 296
- Microsoft Outlook 82
 - Auto-Associate MS Outlook 255
- Microsoft Windows
 - Installer logging 316
 - registry 66
 - security framework 35
- migrating PAB 465
- Minimum number of characters 411
- Miscellaneous settings
 - 488
 - CSPDoNotEnforceRSAPublicKeyExponentLength 484
 - CSPEnforceRSAKeyPairLength 485
 - DeleteOtherPeopleCertsAtLogout 485
 - DisableEPFSubCACertsCompatibility 484
 - DisableTruePassManagement 485
 - EnrollmentStation 486
 - FileUTF8FilenameEncoding 486
 - KASCacheLifetime 487
 - PreventSmartCardNativeSelectReaderUI 487
 - RemoveKnownProblemCACertificates 488
- MMC 107, 114
 - adding snap-in 107, 114
 - computer digital ID snap-in 107
 - Windows services digital ID snap-in 114
- monitoring
 - plaintext files 437

■ 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 ■

- MonitorSmartCardDelay 384
- MonitorStartingDelay 383
- moving
 - Security Manager user entries 83
 - users 83
 - users from one CA to another 275
- msi file 297
 - customizing 285
 - definition 504
- mst file 297
 - definition 504
- Must contain lower character 412
- Must contain upper character 411

N

- Name of CardMS client 370
- Name of the Cryptographic Service Provider (CSP) used to
 - protect users' private keys 352
- name setting for Timestamp 446, 447
- NoCheck 428
- non-Entrust digital IDs 124
- nonrepudiation
 - and EFS 98
 - and EFS user 98
 - certificate type 98
 - definition 505
 - key 53, 59
 - signing key pair, definition 505
 - signing private key 505
 - user 98
- nonrepudiation verification public key
 - definition 505

O

- Obsolete certificate types 274
- OCSP
 - how certificate checks work 139
 - lookup order 427
 - Responder settings 367
 - responder URL 427
 - Revocation Provider 139
 - Revocation Provider settings 425
- OCSP Revocation Provider settings
 - 426
 - DefaultOCSPResponderURL 427
 - EnableOCSPCache 427

- OCSPAcceptMissingNoCheckExtension 428
- OCSPAllowableInterval 429
- OCSPCacheStoreUpdateInterval 428
- OCSPEnableNonce 428
- OCSPTrustedResponders 429
- OfflineRoamingFolder setting 404
- OfflineRoamingLifetime 175
- OID
 - for cn 410
 - for critical extensions 472
 - for UID 410
- OIDs and timestamping 448
- one key pair 96
 - definition 501
- one key pair user 96
- Online Certificate Status Protocol, see OCSP
- Only latest key can sign CMP 262, 273
- Options settings
 - DefaultFolder 408
- Other Security Manager features 273
- Outlook, see Microsoft Outlook
- overview, features 26

P

- p7m file 204
- PAB
 - import 102
 - migrating 101, 465
- packaging the installer 297
- password
 - attempts 403
 - expires in (weeks) setting 254
 - expiry check 55
 - expiry times 254
 - for dump file 249
 - prompts, disabling 50
 - registry settings 411
 - validation 55
- Password Encrypt settings 451
 - EncryptPasswordMaxLength 453
 - EncryptPasswordMinLength 453
 - EncryptPasswordMustContainDigit 453
 - EncryptPasswordMustContainLower 453
 - EncryptPasswordMustContainNonAlphanumeric 453
 - EncryptPasswordMustContainUpper 453
 - HideEncryptPasswordFilesForCert 452
 - HideSelfDecrypt 452

- PEFileDeletePlainText 453
- PEFileDeletePlainTextDefault 454
- patches
 - deploying 308
- path validation, see certificate path validation
- PEG 103
- Permit desktop 255
- Permit roaming 254, 255
- Personal Encryption Groups
 - export 103
 - hiding 466
 - import 103
- PIV 191
- PIV Feature Pack 306
- PIVCustomQuickLinkEnabled 401
- PIVCustomQuickLinkTitle 401
- PIVInsertRetiresSystemTrayOptions 483
- PKI settings 347
 - AutoEnrollRetryInterval 364
 - CSP 352
 - LDAPVersion 336
 - OCSPResponderURL 368
- PKIX-CMP
 - definition 505
 - dump files 321
 - protocol 92
- plaintext files
 - delete 437
 - monitoring setting 437
 - removal of 205
- Policy certificate 66
 - certificate definition settings 92
 - certificate type 92
 - client settings 92
 - definition 505
 - for Security Manager users 92
 - processing 54
- preset name per-CA 415
- Prevent decryption to network 438, 439
- preventing certificates from entering store 106
- Private key
 - definition 505
 - export from CSP 264
 - store 38, 40
- Private key export from CAPI 256
- ProblemCDPs 423
- Professional Services 21, 23
- Profile Server, see Roaming Server

- profile, see digital ID
- Protected key storage for CSP 264
- Proxy Order 360
- Proxy Server
 - and Security Manager 31
 - enable Entrust Authority Proxy Server 359
 - Host Name or IP Address 359
 - overview 33
 - Port Number 359
 - settings 357
- Proxy server settings
 - AutoEnrollUserURL 362
 - ForceHttps 360
 - Proxy 359
 - ProxyOrder 360

R

- RC2 algorithm 130, 132, 133, 134
- Read the Entrust Security Store name from DN
 - attribute 410
- recipient lists, see ERL
- recover
 - a computer digital ID 107, 114
 - definition 505
 - using Entrust Digital ID wizard 68
- Recover Entrust Digital ID wizard 69
- recovery
 - archived keys 67
 - automatic 65
 - dump files 318
 - manual 65
 - of smart cards 181
 - overview 64
 - procedure 69
 - Web 65
 - why it occurs 68
- reference number 66, 71, 148
 - definition 505
- Registration of new users in Security Manager 268
- registry
 - location of Security Provider settings 329
 - settings 327
- remote update
 - of computer digital IDs 107, 114
- remote viewing
 - of certificates 107, 114
- RemoveEDSSupport setting 386

■ 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 ■

- repudiation key, see nonrepudiation key
- retry 364
- RetryManagementOfflineAttempts setting 376
- RetryManagementOfflineInterval 375
- revocation status 240
- roaming
 - Algorithm for digital signature 255
 - capability 202
 - configuring 170
 - for smart card users 172
 - implications 84
 - troubleshooting 175
 - user, definition 505
 - using 170
- Roaming Server
 - encryption algorithm 356
 - Host Name or IP Address 356
 - offline folder setting 404
 - offline lifetime 404
 - overview 33
 - Port Number 356
 - problems 175
 - settings 354
 - skip offline warning 404
 - TLS Port 356
- Roaming Server settings
 - EnableAutomaticEntrustSecurityStoreTypeSwitch 357
 - RoamingEncryptionAlgorithm 356
 - RoamingServer 356
- root
 - building path to 141
 - certificate store 505
- RSA algorithms
 - supported 130, 132, 133

S

- screensaver
 - and logout 57
- search base
 - Friendly Name 342
 - Search Base setting 342
- Search Query setting 436
- Secure Email EKU 443
- securing files 202
- Security 202, 327
 - considerations 323
 - evaluating your cryptographic security 323
 - securing your environment 323
 - securing your password 323
- Security Manager
 - algorithm for key pair 262
 - backup private key 263
 - cert update date 261
 - certificate definition policy configuration 259
 - client policy settings 252
 - create a user 268, 269
 - CSP to manage keys 259
 - deactivating a user 277
 - Directory 32
 - distinguished name (DN) changes 276
 - enable cert update date 261
 - end user activation 271
 - end user registration 268
 - Entrust digital ID synchronization 273
 - generate key at client 263
 - key can sign CMP 262
 - key usage policy 263
 - keys and certificates with no policy 265
 - max key count 90
 - max keys per CSP 264
 - move users from one CA to another 275
 - obsolete certificate types 274
 - only latest key can sign CMP 262
 - other features 273
 - overview 32
 - private key export from CSP 264
 - protected key storage for CSP 264
- Proxy 178
- Proxy Server 31
- Proxy Server overview 33
- update cert at % of lifetime 261
- user policy 252
- Security Manager Proxy
 - ForceHttps 339, 360
- security properties
 - of files 204
- Security Provider
 - about 25
 - communication with the Certification Authority (CA) 92
 - deploying 281
 - deployment worksheet 282
 - distribution mechanism 304
 - enroll for Entrust Digital ID wizard 69
 - Entrust digital ID 82

- event logs 314
- finding version 324
- for Outlook 82
- installing 305
- logging in to your security store 82
- supported key pairs 95
- taskbar icons 55
- taskbar status icon overview 56
- testing 303
- troubleshooting 313
- upgrading 306
- security store 40
 - creation settings 405
 - definition 505
 - Entrust 48
 - login settings 396
 - preventing certs from entering 106
 - smart card 48
 - startup shutdown settings 416
 - third-party 48
 - unavailable during update 84
- self-signed certificate 160
- serial number
 - checking 137
- server name setting for Timestamp 446
- server URL of Timestamp server 447
- service packs
 - deploying 308
- Settings
 - timestamp 445
- settings
 - auto-enrollment 361
 - CA 348, 352
 - CardMS 368
 - Certificate Explorer 463
 - certificates 470
 - default directory 344
 - digital ID computer 389, 392
 - directory connection 332
 - directory search 341
 - enrollment station 486
 - Entrust Ready 469
 - file security 430
 - GUI 478
 - HTTP 476
 - logging 489
 - OCSP 367, 425
 - Password Encrypt 451
 - PKI 347
 - Proxy Server 357
 - Roaming Server 354
 - security store creation 405
 - security store login 396
 - security store startup shutdown 416
 - timeout 476
 - TrueDelete 455
 - TruePass 484
 - user digital ID 373
- settings CRL 419
- settings, registry 327
- setup.exe 297
- setup.ini 297
- SHA algorithms
 - supported 130, 132, 133, 134
- Show Archived Certificates 238
- Show Expired Certificates 238
- signing
 - files 202
- signing algorithm
 - mandatory 435
- Signing key pair
 - definition 505
- Signing private key
 - definition 506
- silent updates 86, 87
- Skip warning about login to offline copy of Entrust roaming
 - security store 404
- SkipNoCertHistoryNag setting 397
- SkipOfflineRoamingNag 175
- smart card
 - Any SC 183, 260
 - configuring CSP 182
 - CSP 186
 - CSP, generating IDs within 183
 - digital IDs 88
 - enrollment 180
 - limit stored keys 88
 - logging in 182
 - logging in with 182
 - moving digital ID to 185
 - moving ID off of 80
 - recovery 181
 - roaming with 172
 - security store 48
 - troubleshooting 186
 - updates 182

■ 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 ■

- using 180
- Smart Card Cryptographic Provider 133
- Smart Card Logon, see Windows Smart Card Logon
- snap-in
 - adding 107, 114
 - computer digital ID 107
 - Windows services digital ID 114
- solid state drives 458
- SRL 103
- SSD 458
- stand-alone EFS user 97
- Standard enterprise environment
 - definition 506
- standards
 - CryptoAPI 37
- Storage
 - digital ID 48
- Storage Providers 134
- store
 - preventing certificates from entering 106
- supported
 - certificates and keys 95
 - key pairs 95
- suspend 253
- Switching between a roaming and desktop user 171
- system architecture 31

T

- Target setting 399
- Taskbar status icon 55
 - overview 56
- Technical Support 21
- text
 - adding to context menus 438
 - setting 399
 - to append to the Entrust Security Store name 409
- third-party
 - keys 124
- Third-party security store
 - definition 506
 - overview 58
- three key pair
 - definition 501
- Time limit (in seconds) for the Directory to spend on a
 - search 343
- timeout
 - connection settings 476

- timeout setting 414
- Timestamp default policy setting 448
- Timestamp name setting 447
- Timestamp server name setting 446
- Timestamp server settings
 - 446
 - default policy OID 448
 - DefaultImprintHashAlgorithm 447
 - DefaultPolicy 449
 - friendly name setting 449
 - ImprintHashAlgorithm 450
 - name setting 446
 - Timestamp server URL 447
- topography 31
- transform file, see .mst file
- Triple-DES 130, 132
- Triple-DES algorithm 133, 134
- troubleshooting 313
 - creating dump file 248
 - Roaming Server 175
 - smart cards 186
- TrueDelete settings 455
 - 456
 - DriveTypes 458
 - ExcludedFileTypes 458
 - FilterOrder 456
 - IncludedFileTypes 459
 - IncludedFolders 460
 - OverwriteFilename 462
 - OverwritingMethod 461
 - Source 457
 - UserDefinedCharacter 462
- TruePass
 - settings 484
- trust signer 204
- two key pair 96
 - definition 501
 - user 96

U

- UID OID 410
- update
 - cert at % of lifetime 261
 - digital ID for computer 107, 114
 - key 82
 - request icon 85
 - silent 86, 87

■ 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 ■

- with smart cards 182
- upgrading
 - Security Provider 306
- URL for Timestamp server 447
- user
 - configuring in Security Manager 251
 - login 52
 - moving 83
 - moving entry for 83
- UTF-8 486

- certificate type 98
- wizard
 - address book 102
 - hide CA 75, 78
 - key file 105
 - personal encryption group 103
 - see Custom Installation Wizard
- worksheet
 - deployment 282

V

- V1-key-pair
 - definition 506
- V2-key-pair
 - definition 506
- validation
 - of Entrust security store 55
- Verification public key
 - certificate definition 506
 - definition 506
- version
 - finding for Security Provider 324
 - of Entrust digital ID 499
 - of Entrust security store 499
- viewing
 - certificates 234
 - event logs for computer digital IDs 107, 114
 - log files 315
 - security properties of files 204
- viewing computer certificates 107, 114
- VPN Client

W

- Web applications 33
- Web enrollment/recovery 65
- Windows Explorer
 - securing files through 202
- Windows Service Digital ID Service
 - Disabling 470
- Windows Service Digital ID settings 389
 - ServiceCertUpdateInterval 390
 - ServiceRetryManagementOfflineAttempts 391
 - ServiceRetryManagementOfflineInterval 390
- Windows services Digital ID Snap-in 114
- Windows Smart Card Logon 96, 185