Entrust Entelligence™

Security Provider 9.3 for Windows

Error Message Guide

Document issue: 1.0

Date of Issue: July 2015

Entrust®
Securing Digital Identities
& Information

1

Error Messages

This error messages document provides a detailed table of Security Provider 9.3 for Windows error messages as well as solutions and ways to work around them.

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
File decryption and verification error messages.		
IDES_CANNOT_DELETE_PLAINTEXT_FILE		
Cannot delete '%1!s!'. %2!s! You will need to delete this file manually.	The attempt to delete the file has been failed by Windows. The second substitution will give the Windows error message giving more details.	No generic solution; see the Windows error message.
IDES_CANNOT_OPEN_FILE		
Cannot open '%1!s!'. There is no application associated with the file type.	The file cannot be opened because there is no registered application for the file's extension.	No generic solution; check the file extension.
IDES_CANNOT_WAIT_FOR_PLAINTEXT_FILE		
The application launched to view '%1!s!' cannot be monitored to see if it has exited. Do you wish to delete the file now? If the application is still using the file this may cause data loss.	The file was opened but Windows has not returned a handle to Security Provider to monitor the opened file. This can occur if the application registered to handle this file type is already running and a new process was not created.	To prevent the message in the future, ensure that the associated application is not already running when the file is opened. Otherwise, leave the dialog open until you close the file.

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
IDES_CANT_CREATE_OUTPUT_FILE		
Cannot create '%1!s!'. %2!s!	The output file cannot be created. The second substitution will give the Windows error message giving more details.	No generic solution; see the Windows error message.
IDES_CERTSTORE_NOT_OPENED		
Cannot decode '%1!s!'. Your personal certificate store could not be opened.	The input file cannot be decoded because the MY certificate store failed to open.	Check to see if the MY certificate store can be opened in another application such as Internet Explorer. A reboot may correct the problem.
IDES_CMD_LINE_ERROR		
The file was not successfully decoded. An error occurred while parsing the command line. Please type in correct command line arguments.	The input file cannot be decoded because the command line arguments are invalid. If you are specifying the command line, you are using the wrong arguments. If you are decoding using Windows Explorer, the configuration of Security Provider for Windows is likely corrupt.	Correct the command line if it is being specified. If using Windows Explorer, repair the installation of Security Provider for Windows.
IDES_DRIVE_FULL		
Cannot decode '%1!s!'. There is not enough free disk space.	The output file cannot be created because the disk is full.	Free up space on the disk.
IDES_NO_DATA_TO_DECODE		
Cannot decode '%1!s!'. The file is empty.	Decoding the file has failed because it is empty.	You cannot decode empty files.
IDES_NO_DECRYPT_VERIFY		
Cannot decode '%1!s!'. An internal error has occurred.	Decoding the file has failed with an unexpected error.	Consult the log file for detailed information about what problem occurred, and then correct the problem.
IDES_NO_DECRYPT_VERIFY_SUB_MESSAGE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Cannot decode '%1!s!'. %2!s!	Decoding the file has failed. The second substitution will give more details.	No generic solution; see the detailed message.
IDES_NO_ENCRYPTED_FILE		
No file has been supplied in the command line arguments.	The input file cannot be decoded because the command line arguments are invalid. If you are specifying the command line, you are using the wrong arguments. If you are decoding using Windows Explorer, the configuration of Security Provider for Windows is likely corrupt.	Correct the command line if it is being specified. If using Windows Explorer, repair the installation of Security Provider for Windows.
IDES_NO_FILE_TO_DECODE		
Cannot decode '%1!s!'. The file does not exist.	Decoding the file has failed because it does not exist.	Select another file.
Enrollment, recovery, or key update error messages.		
IDES_LOAD_RESDLL_ERROR_MSG		
The Entrust Entelligence Security Provider for Windows language resources could not be loaded. This will prevent Security Provider for Windows from functioning properly and it will now exit. Please reinstall or repair Security Provider for Windows.	This error will appear from any Security Provider for Windows component that tries to load its resource DLL, which contains dialog boxes and error strings, but is unable to. It is hard-coded in Security Provider for Windows code and cannot be translated.	Reinstall or repair Security Provider for Windows.
IDES_ERROR_SAS_BAD_INPUT		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Communication with the Certification Authority (CA) cannot be attempted. An invalid %1!s! has been received from the Entrust Authority Self-Administration Server. %1!s! will be either authorization code, reference number, or operation.	Occurs when eeEnlMim.exe is called. The wizard will not be displayed yet. The information file (`*.entpbd`) that has been passed from the Self-Administration Server to Security Provider for Windows is not syntactically valid. The authorization code, reference number, or operation (enrollment/recovery) cannot be read from this file.	The version of Self-Administration Server being used may not be supported. Refer to the ReadMe document (`eesp_readme.html`) for a list of supported versions. The Web browser installation may be corrupted — uninstall and reinstall the Web browser and attempt the enrollment/recovery/update process again.
IDES_ERROR_SAS_NO_TEMPFILE		
Communication with the Certification Authority (CA) cannot be attempted. A fatal error was encountered while communicating to the Web browser. Ensure the Web browser software is functioning properly.	Occurs when eeEnlMim.exe is called. The wizard will not be displayed yet. The information file (`*.entpbd`) that should have been passed from the Self-Administration Server to Security Provider for Windows was not found.	The version of Self-Administration Server being used may not be supported. Refer to the ReadMe document (`eesp_readme.html`) for a list of supported versions. The Web browser installation may be corrupted — uninstall and reinstall the Web browser and attempt the enrollment or recovery process again.
IDES_ERROR_WIZARD_CHOOSECA		
You have not selected a CA from the list. Choose an item in the list before advancing to the next page.	When the user selects **Next** on the CA page of the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard before selecting a CA from the list.	Choose a CA from the list on the CA page of the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard.
IDES_ERROR_WIZARD_CHOOSECSP		
You have not selected a CSP from the list. Choose an item in the list before advancing to the next page.	When the user selects **Next** on the CSP page of the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard before selecting a CSP from the list.	Choose a CSP from the list on the CA page of the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard.

Table 1: Security Provider for Windows IDES error messages

Error message	**When this message will occur**	**Solution or way to work around this message**
IDES_ERROR_WIZARD_BADCSP		
The CSP you selected is not available. Please choose a different CSP, or cancel out of this wizard.	When the user selects **Next** on the CSP page of the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard, but Security Provider for Windows was unable to retrieve the selection they made from the combo box.	Cancel out of the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard and retry.
IDES_ERROR_WIZARD_BADAUTHREF_USER		
The authorization code or reference number you specified are incorrect. Please re-enter these values, or cancel out of this wizard.	When the user clicks **Next** to generate their Entrust digital ID but has left the authorization code or reference number blank on the code page of the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard. (This shouldn't be possible because the **Next** button on the code page should be disabled something has been entered in the edit fields.)	Cancel out of the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard and retry, making sure they are entering the correct activation codes.
IDES_ERROR_WIZARD_BADAUTHREF_MIME		
The authorization code or reference number that were provided as input to this wizard is invalid. The wizard must terminate.	When the user clicks **Next** to generate their Entrust digital ID in the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard. (This should not be possible — the code page is hidden to the user, but no activation codes have been saved.)	Contact the Self Administration Server administrator to verify that the SAS server is working properly.
IDES_ERROR_WIZARD_BADCA_USER		

Table 1: Security Provider for Windows IDES error messages

Error message	**When this message will occur**	**Solution or way to work around this message**
Either the Authority Server or Proxy Server are invalid. These values are likely not properly configured in the PKI Configuration Data in the registry. Your administrator should correct the configuration settings.	When the user clicks **Next** on the CA page, or if that page is hidden, occurs when they click **Next** to generate their Entrust digital ID in the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard. The selected CA does not have an `Authority` or a `Proxy` value defined in the configuration settings in the registry.	Ensure that the Authority or Proxy value configuration settings are configured properly.
IDES_ERROR_WIZARD_BADCA_MIME		
Either the Authority Server or Proxy Server are invalid. These values are likely not properly configured in the PKI Configuration Data in the registry. Your administrator should correct the configuration setting. The wizard must terminate.	When the user clicks **Next** to generate their Entrust digital ID in the **Enroll for Entrust Digital ID** or **Recover Digital ID** wizard. The CA does not havean `Authority` or a `Proxy` value defined in the configuration settings in the registry.	Ensure that the Authority or Proxy value configuration settings are configured properly.
IDES_ERROR_WIZARD_BADREGDATA_CSP		
The wizard is unable to retrieve relevant CSP data from the registry. The list of available CSPs in the registry has been corrupted. The wizard must terminate.	When the CSP page of the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizard is displayed, the available CSPs are read from the registry. The registry is corrupted and there were none found.	You may need to re-install Internet Explorer.
IDES_ERROR_ENROLL_NULL_INPUT_PARAMS		
Insufficient information has been provided to eeEnroll.dll. One of the required input parameters is empty. %1!s! can not complete successfully.	EERecoverDigitalID() or EEEnrollDigitalID() has been called with the EE_NO_WIZARD flag, but one of the required input parameters is NULL.	Ensure that the PKI configuration settings are configured properly.
IDES_ERROR_ENROLL_BAD_PKI_CONFIG_DATA		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
PKI Configuration Data has not been properly entered into the registry. Inform your administrator of this problem.%1!s! can not complete successfully.	Checks for valid registry data are performed before showing the wizard, and again before showing the CA page. If they fail due to invalid (or lack of) configuration data, this error will be displayed.	Ensure that the PKI configuration settings are configured properly.
IDES_ERROR_ENROLL_CANT_LOAD_WIZARD		
The wizard is unable to load properly. Reinstallation is recommended. %1!s! can not complete successfully.	Occurs If a wizard page could not be loaded or created. This should never occur.	Reboot and try again. If this does not work, re-install Security Provider for Windows and try to enroll or recover again.
IDES_ERROR_WIZARD_BADPKIDATA_CSP		
The wizard is unable to retrieve correct PKI configuration data from the registry. The information relating to your CSP was not properly entered by your administrator. The wizard must terminate	When the user clicks **Next** to generate their digital ID using the **Enroll for Entrust Digital ID** or **Recover Entrust Digital ID** wizards, and the CSP name is NULL. Normally does not occur because the default CSP is set to Entrust Enhanced Cryptographic Provider.	Only appears during an internal error.
IDES_ERROR_MSG_FAIL_DELETE_CERT		
Failed to delete certificate with serial number %1!s! %2!s! from the certificate store.	When the user clicks **Delete Digital ID** from either the Digital ID Monitor's **Entrust Digital ID Update Request** or **Entrust Digital ID Recovery Request** notification dialog, and a failure occurred while deleting certificates.	Try to delete the certificates manually from the Internet Explorer certificate viewer.
IDES_ERROR_MSG_MISSING_CERT_FROM_STORE		

Table 1: Security Provider for Windows IDES error messages

Error message	**When this message will occur**	**Solution or way to work around this message**
There are missing certificates in user %1!s! 's Entrust Digital ID. Your certificates cannot be managed.	When the digital ID management feature is checking a user for pending key updates, and some of the user's certificates are missing from the local store. An Entrust digital ID cannot be managed when there are certificates missing.	If the Entrust digital ID is spread across multiple CSPs, you must log into all portions of the Entrust digital ID before management can take place. For example, log into the smart card and the EPF.
IDES_ERROR_WRAPPER_ENROLL		
Enrolling for the Entrust Digital ID was unsuccessful. %1!s!	In the enrollment case, this string will come before any errors with prefix "IDESC".	N/A
IDES_ERROR_WRAPPER_RECOVER		
Recovering the Entrust Digital ID was unsuccessful. %1!s!	In the recovery case, this string will come before any errors with prefix "IDESC".	N/A
IDES_ERROR_WRAPPER_UPDATE		
Updating the Entrust Digital ID was unsuccessful. %1!s!	In the update/sync/move case, this string will come before any errors with prefix "IDESC".	N/A
IDES_ERROR_WRAPPER_UNKNOWN		
Completion of the current task was unsuccessful. %1!s!	In the unknown case, this string will come before any errors with prefix "IDESC".	N/A. This will only appear during an internal error.
IDESC_ERROR_MSG_POLICY_CERT_UNSUPPORTED_KEYTYPE		
The Entrust policy certificate specifies a key type (for example, DSA_1024) that is not supported by Security Provider for Windows. The required user key pair cannot be created. Your administrator should modify the Entrust policy certificate.	Occurs when Security Provider for Windows is reading the client settings policy certificate (for V1-key-pair users) or the certificate definition policy certificate (for V2-key-pair users). An unsupported key type has been encountered.	The Security Manager administrator must change the policy so that Security Provider for Windows can create or import the key pairs.
IDESC_ERROR_MSG_POLICY_CERT_MISSING_FROM_MESSAGE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust policy certificate is not present in the reply message from the Certification Authority (CA). The policy certificate is required to continue. Your administrator should modify the Entrust policy certificate.	When the reply message from the CA either does not contain the required policy, or there is an internal problem with Security Provider for Windows, preventing it from reading the response message properly.	Possibly the version of Security Manager and Security Provider for Windows are not compatible due to a change made to the ASN.1 definitions in either application.
IDESC_ERROR_MSG_UNSUPPORTED_ALGID_FROM_PKI		
A message from the CA contains an unsupported type of session key. Currently supported algorithm identifiers are: `CAST-80`, `CAST-128`, `DES`, `TRIPLE DES`, `AES`, or `IDEA`.	When a symmetric session key in the CA's response message is an unsupported algorithm.	This should not occur because Security Provider for Windows supports all algorithms supported by the CA.
IDESC_ERROR_MSG_BAD_SIGNING_CERT		
An attempt to extract the public signing key from the certificate used for signing has failed. The certificate may be corrupted. If possible, log out of your Entrust Digital ID, then log back in and try again.	When Security Provider for Windows could not access the public key specified in the user's signing certificate, or could not read the event identifier from the certificate properties (V2-key-pair users only).	Indicates internal problems. Recover the Entrust digital ID
IDESC_ERROR_MSG_NO_SIGNING_CERT		
Your certificate used for signing is required to complete this task, but it cannot be retrieved from the local certificate store. If possible, log out of your Entrust Digital ID, then log back in and try again.	When a signing certificate is not present in the list of certificates passed from the digital ID management feature to the enrollment and recovery feature, or if the signing certificate passed in from the digital ID management feature cannot be retrieved from the certificate store.	Indicates internal problems. Recover the Entrust digital ID.
IDESC_ERROR_MSG_CANT_GET_USER_KEYS		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Your public keys are required to complete this task, but they are inaccessible or corrupt. If possible, log out of your Entrust Digital ID, then log back in and try again.	If there were problems exporting a key. Examples of keys that are exported are: the session key used to encrypt dual usage keys being sent to the CA for backup, and the protocol encryption key.	Refer to the Security Provider for Windows log file (`logmain.htm`) for additional details and debugging information.
IDESC_ERROR_MSG_CANT_CREATE_USER_KEYS		
The creation of user keys is required to complete this task, but user keys could not be created. It is possible that the Cryptographic Service Provider (CSP) in use does not support key creation of the desired key type.	If any key creation fails (user keys or protocol encryption key).	The CSP may not support the type or size being requested. Change the key size and/or type in the policy certificate(s) and try again.
IDESC_ERROR_MSG_CANT_DETERMINE_KEY_TYPE		
The creation of user keys is required to complete this task, but the type of key found is unrecognizable. If possible, log out of your Entrust Digital ID, then log back in and try again.	If an unrecognizable key type is encountered during the key update process.	Refer to the Security Provider for Windows log file (`logmain.htm`) for additional details and debugging information.
IDESC_ERROR_MSG_UPDATE_NOT_ALLOWED		

Your administrator has configured your Entrust Digital ID in such a way that key updates are not permitted. Your certificates will not be updated, and will be invalid once they expire.	If an update request was sent to the CA, and the CA returned one of the following error codes:
	`FENC_ROLLOVER_NOT_ALLOWED (-1048)`
	`COMM_SEP_CLIENT_KEY_BACKUP_NOT_ALLOWED (-1542)`
		If the Security Manager administrator wants updates to be allowed, they must change the settings to allow key updates using Security Manager Administration.

IDESC_ERROR_MSG_BAD_AUTH_OR_REF		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The reference number or authorization code you entered was incorrect. Possibly you entered one of them incorrectly, or your administrator gave you invalid codes. Try entering your activation codes again, and if this error returns contact your administrator.	When the codes are sent to the CA and the following error code is returned: `COMM_SEP_BAD_REF_NUM_MGR (-1686)` Also occurs before the request is sent to the CA if the authorization code is not the correct length or the checksum fails.	Try enrolling or recovering again: incorrect codes may have been entered, or an administrator may have provided incorrect activation codes. You may be attempting to enroll or recover to the wrong CA.
IDESC_ERROR_MSG_CANT_ARCHIVE_CERT		
There was a problem archiving the user's old encryption certificate once the new certificate was placed in the certificate store. Your Entrust Digital ID is now in a corrupted state and a recovery is recommended. It is recommended that you contact your administrator about recovering your Entrust Digital ID.	After a key update, users' old encryption certificates must be archived. If they are not, their Entrust digital ID becomes corrupted, in which case they will see this message.	Recover the Entrust digital ID.
IDESC_ERROR_MSG_CANT_DELETE_CERT		
There was a problem deleting the user's old signing certificate once the new certificate was placed in the certificate store. Your Entrust Digital ID is now in a corrupted state and a recovery is recommended. It is recommended that you contact your administrator about recovering your Entrust Digital ID.	After a key update, users' old signing certificates must be deleted from the certificate store. If they are not, their Entrust digital ID becomes corrupted, in which case they will see this message.	Recover the Entrust digital ID.
IDESC_ERROR_MSG_PKIX_MSG_SEND_FAILURE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Communication with the Certification Authority (CA) cannot be achieved. Possibly you are not connected to the network.	When an attempt to send a message to the CA has failed. Possibly Security Manager is not running, the CA is not accessible, or the user is not properly connected to the network.	The Security Manager administrator should check the status of Security Manager. Ensure that the user is properly connected to the network.
IDESC_ERROR_MSG_CERTIFICATE_ACCESS_FAILURE		
An attempt to add a certificate to the local store, or to modify an existing certificate has failed. The certificate may be corrupted. If possible, log out of your Entrust Digital ID, then log back in and try again.	This error message covers any problems with a certificate: - cannot open certificate store - cannot read certificate - cannot attach a property to certificate - cannot modify a certificate - cannot add certificate to store.	Recover the Entrust digital ID.
IDESC_ERROR_MSG_KEY_ACCESS_FAILURE		
An attempt to use a public/private key pair to perform a cryptographic operation has failed. The key pair may be corrupted. If possible, log out of your Entrust Digital ID, then log back in and try again.	This error message covers any problems with accessing a key: - cannot get key length - cannot get public key information - cannot use a key to MAC data.	If possible, recover the Entrust Digital ID. If the error occurred while recovering the digital ID, ensure that all Security Provider system requirements have been met. For example, you may be using an unsupported version of Windows.
IDESC_ERROR_MSG_BAD_AUTHORITY		
There was a problem establishing communication with the Certification Authority (CA). The authority name is likely not properly configured in the PKI Configuration Data in the registry.	This can occur during `EEMoveUser()` if the new CA (that they are moving to) is not configured in the registry.This will also occur during all APIs if the authority or proxy server cannot be contacted.This will also occur if the syntax of the authority or proxy in the registry is not "`name:port`".	Ensure that the PKI configuration settings are configured properly.
IDESC_ERROR_MSG_ENCODE_DECODE_FAILURE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
There was an internal error while attempting to encode or decode data. The version of your Certification Authority (CA) is likely not supported by Security Provider for Windows.	Any failed attempt to encode or decode ans1 data will cause this. It could happen anywhere. A possible cause would be that changes were made to the Security Manager ans1 definitions, and were not updated in the Security Provider for Windows's ans1 definitions. Another possibility is that there is a bug in Objective's software.	Ensure that you are using a supported version of Security Manager.
IDESC_ERROR_MSG_OUT_OF_MEMORY		
The system is out of memory and the space needed to complete this task can not be allocated. If you have several applications running at this time, close any unneeded programs and try again.	An attempt to allocate memory failed. There is not enough memory available to complete the task.	Close other running applications and/or reboot machine and try again.
IDESC_ERROR_MSG_NULL_INPUT_PARAM		
One of the input parameters needed to complete this task is missing. Likely your Entrust Digital ID has become corrupted. It is recommended you contact your administrator about recovering your Entrust Digital ID.	Possible that the caller did not pass in the required input parameters to `EEUpdateDigitalID()` or `EESynchronizeDigitialID()` or `EEMoveDigitialID()`. Another possibility is an internal loss of data.	Reinstall Security Provider for Windows.
IDESC_ERROR_MSG_UNKNOWN		
An untraceable internal error has occurred. Reinstallation is recommended.	An error was thrown somewhere within the code, but the error code was lost internally. Should never happen.	Reinstall Security Provider for Windows.
IDESC_ERROR_MSG_MSG_VERIFICATION_FAILED		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The reply message received from the Certification Authority (CA) has failed the consistency checks. Consistency checks on received messages are performed to ensure a secure communication with the CA has been maintained. Since these checks have failed, the response from the CA is not trusted.	All messages received from the CA are verified for added security. There are various checks performed. If any of these fails, it is assumed that the message has been tampered with and this error is thrown.	Verify that your environment has not been compromised.
IDESC_ERROR_MSG_AUTHCODE_EXPIRED		
The activation codes you entered have expired, and are no longer valid. Your administrator must re-issue activation codes for you and distribute them to you in a secure manner.	The user waited too long to use the authorization codes and they have expired. During the enrollment/recovery attempt, the CA returned the following error code:`COMM_SEP_CLIENT_AUTH_CODE_EXPIRED(-1541)`	The Security Manager administrator must issue new authorization codes to the user.
IDESC_ERROR_MSG_PKI_ERROR_MSG_RECIEVED		
The reply message received from the Certification Authority (CA) is an error message which contains an unrecognized error code. If possible, your administrator should consult the log file for more information.	The CA returned an error code in place of the expected reply message. The error code is not one that Security Provider for Windows handles, don't know what type of error message to display. This error appears less often, the more error codes that are handled from the CA.	Check the Security Manager logs to see what went wrong.
IDESC_ERROR_MSG_CANT_CREATE_SESSION_KEYS		
The creation of a temporary session key is required to complete this task, but the key could not be created. It is possible that the Cryptographic Service Provider (CSP) in use does not support key creation of the desired key type.	A call to `CryptGenKey()` for a session key failed. Possibly the CSP does not support the requested algorithm, or there is a fatal problem somewhere in the CSP.	Ensure that you are using a supported version of Windows.
IDESC_ERROR_MSG_PKIX_MSG_RECIEVE_FAILURE		

Table 1: Security Provider for Windows IDES error messages

Error message	**When this message will occur**	**Solution or way to work around this message**
There was a problem processing one of the messages received from the Certification Authority (CA). The version of your Certification Authority is likely not supported by Security Provider for Windows.	Possibly, an attempt to receive a message from the CA has failed. Maybe Security Manager is not running, or the CA is not accessible.The other possible problem is that the reply message was received, but it contains invalid or missing information that Security Provider for Windows cannot handle.	Check the status of Security Manager and confirm the version of Security Manager is compatible with Security Provider for Windows.
IDESC_ERROR_MSG_KEY_IMPORT_FAILURE		
An attempt to import a public/private key pair has failed. It is possible your Cryptographic Service Provider (CSP) does not support this operation, or the key size or type is not supported.	A call to `CryptImportKey()` has failed for some reason. This should not occur. The CSP probably cannot accept a key pair of this size or type.	Verify that the chosen CSP supports this key size and type.
IDESC_ERROR_MSG_DO_ENROLL_NOT_RECOVERY		
The activation codes you entered are valid for an enrollment, not a recovery. You should run the Enroll for Entrust Digital ID Wizard instead.	The user is trying to recover with codes that are meant for an enrollment. The user was created at Security Manager and is now in the "Added" state. The error code returned from the CA was:`COMM_SEP_CLIENT_WRONG_STATE_NEW_MGR (-1638)`	Run **Enroll for Entrust Digital ID** wizard.
IDESC_ERROR_MSG_DO_RECOVERY_NOT_ENROLLMENT		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The activation codes you entered are valid for a recovery not an enrollment. You should run the Recover Entrust Digital ID Wizard.	The user is trying to enroll with codes that are meant for a recovery. The user has already been active at one point, and the administrator moved them into "Key Recovery" mode. The error code returned from the CA was:`COMM_SEP_CLIENT_WRONG_STATE_KREC_MGR(-1637)`	Run the **Recover Entrust Digital ID** wizard.
IDESC_ERROR_MSG_SYSTEM_TIME_WRONG		
The Certification Authority (CA) has rejected the request since your computer's clock is more than 2 hours different than the CA's clock. Check that your computer's clock is correct, and correct it if necessary.	The user's clock and the CA's clock cannot differ by more than 2 hours. The error code returned from the CA was:`MGR_CLI_TIME_MISMATCH(-2908)`	Fix the user's clock.
IDESC_ERROR_MSG_BAD_PROXY_VALUE		
There was a problem establishing communication with the Certification Authority (CA). The proxy server name is likely not properly configured in the PKI Configuration Data in the registry.	The proxy server is syntactically incorrect in the registry. It must be in the form of `"name:port"`.	Fix the `Proxy` value in the PKI configuration settings.
IDESC_ERROR_MSG_DO_RECOVERY_NOT_UPDATE		
Communication with the Certification Authority (CA) has revealed that your Entrust Digital ID cannot be updated, but instead needs to be recovered. Contact your administrator for instructions on how to recover your Entrust Digital ID.	Security Provider for Windows is trying to update a user, but they received the following error code from the CA:`COMM_SEP_CLIENT_WRONG_STATE_KREC_MGR (-1637)`.Their state at Security Manager is "key recovery".	Give the user the authorization codes for recovery, and the user can run the **Recover Entrust digital ID** wizard.
IDESC_ERROR_MSG_CANT_DISPLAY_PROGRESS_DLG		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The progress dialog cannot be displayed. The requested operation will not be attempted.	There was an internal error while trying to display the progress bar during an update/sync/move.	Ensure that you are using a supported version of Windows.
IDESC_ERROR_MSG_CANT_MOVE_USER_TO_LEGACY_PKI		
The move cannot be completed since the new Certification Authority (CA) is not a supported version. Likely your administrator is attempting to move you from a version 7.0 CA to a version 6.0 CA. Entrust Entelligence Security Provider for Windows cannot do this move automatically and you must recover yourself at the new CA. Contact your administrator about recovering your Entrust Digital ID.	With Security Manager 7.0, Security Provider for Windows can automatically detect that the user must be moved to a different CA. Only automatic moves from 7.0 to 7.0 are supported.	Manually set the user up for recovery with the new CA. (This is the same as the functionality with a 6.0 CA.)
IDESC_ERROR_MSG_CANT_USE_ENROLLMENT_STATION		
This computer is configured to be an enrollment station for your company. However, certain aspects of your Entrust digital ID are not compatible with an enrollment station. You need to recover your Entrust Digital ID at a computer that is not an Enrollment station. You should speak to your administrator about obtaining activation codes for the recovery.	Enrollment at an enrollment station is only allowed if the user's CSP supports the action of saving certificates in the CSP's protected key store. The Entrust Enhanced CSP and Smart card CSPs will work, but the Microsoft CSPs will not work.	User should not be enrolling/recovering at an enrollment station. They should do the enrollment or recovery at their own computer. Issue recovery activation codes to the user because the enrollment was unsuccessful, and the user is now in the "Active" state in Security Manager.
IDESC_ERROR_CANT_USE_OLD_SIGNING_KEY		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Your Entrust digital ID contains information that is out-of-date and needs to be synchronized. However, your policy prohibits this action. If you have a more recent copy of your Entrust digital ID, discontinue using this older copy and use the newer copy from now on.	The certificate definition policy (in 7.x) states that old signing keys cannot be used to perform key updates. This prevents the user from synchronizing old copies of their Entrust digital ID.	The user should find the most recent copy of their Entrust digital ID and replace all old copies with the new one. Alternatively, the Security Manager administrator can change this policy setting so that the user can synchronize.
IDESC_ERROR_USER_IN_WRONG_STATE		
The Certification Authority (CA) has rejected the request since your state at Security Manager is not compatible with this action.	User's state in Security Manager - added, active, key recovery, etc. is not compatible with the action being requested.	Check the user's state in Security Manager and act accordingly.
IDESC_ERROR_USER_IN_DISABLED_STATE		
The Certification Authority (CA) has rejected the request since you are in the disabled state. You may choose to contact your administrator about why you have been disabled, and the possibility of recovering your Entrust Digital ID.	User's state in Security Manager is disabled. They can't update their Entrust digital ID while in this state.	This is not so much an error as a configuration made by an administrator. There is a reason the user is in the disabled state.
IDESC_ERROR_MGR_CANT_FIND_USER		
The Certification Authority (CA) has rejected the request since you can not be found in the CA's user database.	User's state in Security Manager is non-entrust, or they do not exist at all in the directory.	The Security Manager administrator must find out why the user no longer exists.
IDESC_ERROR_MSG_INTERNAL_ERROR		
An internal error occurred that prevents completion of this action. If possible, try this action again.	Something is corrupted internally and data has been lost.	Reinstall Security Provider for Windows.
IDESC_ERROR_CANT_ACQUIRE_CONTEXT_TO_CSP		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The creation of user keys is required to complete this task, but a context to the Cryptographic Service Provider (CSP) could not be acquired. It is possible that the desired CSP is not installed on your machine, or it does not support this type of request.	Before key creation/import a context to the correct CSP must be acquired. If this fails, this error is displayed.	The most likely cause will be that the CSP being requested is not installed on the user's machine.
IDESC_ERROR_CANT_CREATE_PROT_ENC_KEY		
An error occurred while creating the protocol encryption key pair. This key pair is required. You should consider repairing your installation of Entrust Entelligence Security Provider for Windows.	There was a failure while generating the protocol encryption key pair, or while calculating the required size of this key pair (the size is equal to the largest user key pair).	During enrollment, recovery, and key update, a protocol encryption key pair is created whenever there is a server-generated key pair. The public portion of the protocol encryption key pair is sent to the CA in the request message and the CA uses this key to encrypt a key that is returned in the response message.This key pair is created in the Entrust Enhanced Cryptographic Provider. The most likely cause for failure is that the Entrust Enhanced CSP is not installed properly.
IDESC_ERROR_CANT_PASS_CERT_TO_CSP		
An error occurred while passing a certificate to the Cryptographic Service Provider (CSP). If you are using a smart card, it is possible that your card does not have the required amount of free space to store the certificate.	If the `CryptSetKeyParam()` function with parameter `KP_CERTIFCATE` fails with an error other than "Invalid Type", this error is returned. When the CSP returns "Invalid Type", it indicates that the CSP does not support receiving certificates (like the Microsoft CSPs, for example). An error is not returned.	The most likely cause for this error is that a smart card CSP is in use, and there is not enough room on the card to store the certificate.

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
IDESC_ERROR_MGR_WANTS_VER_PUB_KEY_ERROR		
The Certification Authority (CA) has rejected the request since a public verification key was not found. It is likely that the policy specifies a server-generated verification key, which is not supported by your version of Security Manager.	The certificate definition policy specifies that the verification key is backed up. This configuration is possible even though Security Manager does not support it.	The certificate definition policy must be changed to specify that the verification key is NOT backed up.
IDESC_ERROR_WONT_ALLOW_OLD_METHOD_FOR_SKP_USERS		
Your administrator has configured your Entrust Digital ID in an unsupported manner. Your policy certificate indicates that you should have only one key pair, but your list of certificate definitions includes two or more certificates. This contradiction must be corrected.	Appears during enrollment or recovery to a 7.x CA only. If the user's client settings policy certificate has `NumKeyPairs = 1`, and the certificate type contains more than one certificate definition, this error is thrown to prevent the enrollment/recovery. This prevents the administrator from creating SKP users in Security Manager 7.x the same way they did in Security Manager 6.0.	To create an SKP user, use the new certificate type called `ent_skp_dualusage`. Or, to create a 2-key-pair user, change the client settings policy certificate so that it does not say `NumKeyPairs = 1`.
IDESC_ERROR_CANNOT_MIGRATE_OLD_METHOD_FOR_SKP_USERS		
Your administrator has configured %1!s!'s Entrust Digital ID in an unsupported manner. Your policy certificate indicates that you should have only one key pair, but your list of certificate definitions includes two or more certificates. This contradiction must be corrected.	Appears during migration to a 7.x CA only. If the user's client settings policy certificate has `NumKeyPairs = 1`, and the certificate type contains more than one certificate definition, this error is thrown to prevent the migration. This prevents legacy single key pair users from getting 2 certificates when they migrate to 7.x.	If you want the user to migrate to Security Manager 7.x and continue to work as a single key pair user, change the user's certificate type to `ent_skp_dualusage`. Or, if you want the user to migrate to a regular 2-key-pair user `(ent_default)`, change the client settings policy certificate so that it does not say `NumKeyPairs = 1`.
IDESC_ERROR_MGR_SAYS_NOARCHIVE_NOT_ALLOWED_ERROR		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Certification Authority (CA) has rejected the request because your Entrust Digital ID has been incorrectly configured. Your administrator must configure your Certificate Definitions so that all server-generated key pairs are also archived.	The certificate definition policy certificate specifies a server-generated not backed-up key pair. This configuration is possible in Security Manager Administration even though Security Manager does not support it.	The certificate definition policy must be changed to specify that the server-generated key pair is backed up, or the policy should be changed to specify a client-generated key pair.
IDESC_ERROR_MGR_SAYS_NO_EPF_WITH_WEB		
The Certification Authority (CA) has rejected the request since your Certificate Category is "Web". Entrust Security Manager will not allow enrollment for this type of digital ID in this manner. Your administrator will have to change your Certificate Category to "Enterprise".	Security Provider for Windows cannot be used to enroll users to the Web Certificate Category.	Add a user to the Enterprise Category in Security Manager Administration and give those activation codes to the user.
IDESC_ERROR_MGR_SAYS_POL_SETTINGS_ERROR		
The Certification Authority (CA) has rejected the request since there is a disagreement between the information in the policy certificates and the information in the master.certspec file. Your administrator must correct this inconsistency	There is a disagreement between the policy certificates and the information in the master.certspec file. This inconsistency must be corrected. An example is that the key usage specified in the master.certspec file for a particular certificate definition does not match the key usage certificate definition policy attribute.	Adjust the policy certificates so that they agree with the master.certspec in Security Manager Administration.
IDESC_ERROR_MSG_SIGN_CERT_MISSING_PROPS		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
An attempt to read a certificate property from the certificate used for signing has failed. This property is required. You will need to recover your digital ID.	At the start of synchronization and update, the event identifier property is read from the message-signing certificate. It was not found. The event identifier is required because it must be sent to the CA as a form of identification.	Recover the Entrust digital ID. The event identifier property will be added back to the message-signing certificate during recovery.
IDESC_ERROR_WONT_ALLOW_BACKED_UP_VER_CERT		
Your Entrust Digital ID has been incorrectly configured. Your administrator must change your policy so that the verification key pair is not archived.	Security Provider for Windows cannot support verification key pairs that are client-generated and backed-up (archived). This configuration is detected in the certificate definition policy certificate(s) and the enrollment fails. There is no loss of functionality because Security Manager does not support this configuration either.	Turn off the "backed up" setting in the verification certificate definition policy. The user's activation codes are still valid and can be re-used once you make this change.
IDESC_ERROR_MULTIPLE_CERTS_IN_MOVE_REPLY_MSG		
An attempt is being made to move your Entrust digital ID to a new Certification Authority (CA) but this move has already been completed. If you have a more recent copy of your Entrust digital ID, stop using this older copy and use the newer copy from now on. Otherwise, you need to recover your Entrust digital ID. To begin the recovery process, start the **Recover Entrust Digital ID** wizard.	The automatic move user response from the CA contains unsupported data. This will occur when the automatic move is being attempted a second time. That is possible if the first attempt at the move failed because the user chose "cancel" during the move on a dialog from the CSP, or if the user is logging into an old copy of their Entrust security store (from before the move).	If applicable, old copies of the Entrust security store should be deleted and the most recent copy should be used. Otherwise, a recovery is required.
IDES_EE_DIG_ID_MONITOR_CANNOT_START		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Entrust Entelligence Digital ID Monitor could not successfully initialize. Management of your Entrust digital IDs will not occur during this logon	The `eecwatch.exe` application was unable to initialize properly. Either the mutex, events, or threads, could not be created.	Restart eecwatch.exe manually, or by restarting Windows. If the problem is still not resolved, try uninstalling and re-installing Security Provider.
IDES_CA_REVOKED		
%1!s!'s Certification Authority (CA) certificate has been revoked. You can continue to work but your digital signatures will not be trusted. You will need to recover your digital ID to ensure your digital signatures are trusted and that you receive any necessary updates	During digital ID management, the complete certificate chain (from end certificates to root certificate) is validated. If an intermediate CA or root CA certificate in the chain is found to be revoked, this error is displayed.	The revoked CA certificate must be updated. Security Provider will pick up the new CA certificate the next time digital ID management is performed.
IDES_PATH_VALIDATION_FAILED		
Management of %1!s!'s Entrust digital ID was not successful. Validating your certificate could not be successfully completed.	During digital ID management, the complete certificate chain (from end certificates to root certificate) is validated. Either certificate path validation could not be completed, or the certificate path is invalid.	Consult the log file for detailed information about what problem occurred, and then correct the problem.
IDES_UPDATE_FAILED_AUTO_RECOVERY_FAILED		
Management of %1!s!'s Entrust digital ID could not be successfully completed. Your digital ID is in a state that requires a recovery, but the automatic recovery was unsuccessful. Your administrator must correct the problem before the recovery can proceed.	Auto-Recovery is enabled for this user, and an auto-recovery was attempted. An error was returned from the Auto-Enrollment Server instead of activation codes.	Consult the log file for detailed information about what problem occurred, and then correct the problem.
IDES_UPDATE_FAILED_AUTO_RECOVERY_QUEUED		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Management of %1!s!'s Entrust digital ID could not be successfully completed. Your digital ID is in a state that requires a recovery, but the request to automatically recover has been placed in an administrative queue. Once your administrator approves this request, the recovery will proceed.	Auto-Recovery is enabled for this user, and an auto-recovery was attempted. The Auto-Enrollment Server returned a queued response message instead of activation codes.	Approve the user's request to recover that is pending in the administrative queue (in Entrust Authority UMS). The next time digital ID management occurs, the auto-recovery will be attempted again and this time should succeed.
IDES_UPDATE_FAILED_AUTO_RECOVERY_REJECTED		
Management of %1!s!'s Entrust digital ID could not be successfully completed. Your digital ID is in a state that requires a recovery, and the request to automatically recover was placed in an administrative queue. However, the administrator has rejected (cancelled) this request for recovery. Your administrator can explain why the request was rejected.	Auto-Recovery is enabled for this user, and an auto-recovery was attempted. The Auto-Enrollment Server returned a rejected response message instead of activation codes.	If the request to auto-recover was rejected intentionally, then the user can manually recover. Communicate the activation codes to the user and instruct them to run the Recover Digital ID Wizard. If the request to auto-recover was rejected by mistake, delete the item in the administrative queue (in Entrust Authority UMS) for this user. The next time digital ID management occurs, the auto-recovery will be attempted again and this time a new request will be placed in the queue. This request can be granted so that the auto-recovery will be allowed.
IDES_UPDATE_FAILED_MISSING_LEGACY_CERT_FROM_STORE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Management of %1!s!'s Entrust digital ID could not be successfully completed. You are missing a certificate. If you are using a smart card with your Entrust digital ID, inserting the smart card may restore the missing certificate. If this is not your primary computer, the missing certificate may only be available on your primary computer.	Security Provider is attempting to perform digital ID management, but the complete digital ID is not available on this computer. The common cause is that the user has roamed to a new computer with a portion of their digital ID, but the other portion was left on the original computer. For example, a user with a smart card containing one certificate and an Entrust Security Store containing other certificates may roam to a second computer using only the smart card.	Digital ID management will resume once all certificates and key pairs are available on the same computer.
Entrust security store, enrollment, update, recovery error messages.		
IDES_PROFILE_NOT_FOUND		
The Entrust security store '%1!s!' does not exist. Please check the name.	If the user selects a security store from the MRU that no longer exists during login.	Select another store or browse to the file if it has been moved.
IDES_NOT_PROFILE		
The file '%1!s!' is not an Entrust security store.	f the user selects a file that isn't a valid Entrust security store during login.	Select a file that is an Entrust security store.
IDES_TOOMANY_LOGINS		
You have supplied an incorrect password 3 times. The login will be cancelled. Please ensure you are typing your password correctly.	If the user enters an incorrect password 3 times during login. The dialog closes to slow down password crackers that may be attempting to script the login dialog	A new login must be initiated. Once the login dialog is available, enter the correct password.
IDES_CONFIRM_PASSWORD_FAILED		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Password change did not complete successfully. The passwords you typed do not match. Please type the same password in both boxes.	User doesn't type the same password in the confirm dialog during password change.	Type the same password in both fields.
IDES_LOGIN_FAILED_INCORRECT_PASSWORD		
The login was not successful because the password is not correct. Please retype your password. Please ensure you are using the correct case and that Caps Lock is not accidentally on.	User typed incorrect password for the selected Entrust security store during password change.	Type the correct password for the selected Entrust security store.
IDES_CHNG_PWD_BAD_OLD		
Password change did not complete successfully. The current password is not correct. Please retype your password. Please ensure you are using the correct case and that Caps Lock is not accidentally on.	The user enters their current password incorrectly, during password change.	Type the correct password for the selected Entrust security store.
IDES_READONLY_PROFILE		
The file '%1!s!' is a read-only file. The Entrust security store must not be read-only to login.	If the user selects a read-only Entrust security store during login.	Remove the read-only attribute from the Entrust desktop security store.
IDES_LOGIN_FAILED_UNKNOWN_CRED_STORE_TYPE		
The login was not successful because Entrust Entelligence does not support logging into this security store format.	The user has selected a file that Security Provider for Windows doesn't currently support. This should not actually happen anymore, because the check will be done earlier and `IDES_NOT_PROFILE` should occur instead.	Select a file that is an Entrust security store. (Same as: `IDES_NOT_PROFILE`).
IDES_LOGIN_FAILED_CANNOT_OPEN_CRED_STORE		

Table 1: Security Provider for Windows IDES error messages

Error message	**When this message will occur**	**Solution or way to work around this message**
The login was not successful because the Entrust security store cannot be opened.	Some kind of internal error occurred that should never happen.	The logs may indicate the problem.
IDES_LOGIN_FAILED_ROAM_SUSPENDED		
The login was not successful because the Entrust security store is suspended by the Entrust Authority Roaming Server.	If the user is attempting to login to an Entrust security store that is suspended by the Entrust Authority Roaming Server.	Wait until the suspension is over (hard to tell because it is configurable), or recover the Entrust digital ID, or unsuspend on the server.
IDES_ALL_CERTS_REVOKED		
All of your certificates have been revoked. You can continue to work but your digital signatures will not be trusted and updates will not be performed. You will need to recover your digital ID to ensure your digital signatures are trusted and that you receive any necessary updates.	All of the Entrust digital ID's certificates have been revoked.	Recover the Entrust digital ID.
IDES_LOGIN_FAILED_CRED_STORE_SUSPENDED		
The login was not successful because the Entrust security store is suspended due to too many unsuccessful password attempts.	If the user is attempting to login to an Entrust security store that is suspended locally.	Wait until the suspension is over (hard to tell because it is configurable), or recover the Entrust digital ID.
IDES_LOGIN_FAILED_UNKNOWN_CRED_STORE_TYPE		
The login was not successful because Entrust Entelligence does not support logging into this security store format.	The user has selected a file that Security Provider for Windows doesn't currently support. This should not actually happen anymore, because the check will be done earlier and `IDES_NOT_PROFILE` should occur instead.	Same as: `IDES_NOT_PROFILE`.
IDES_LOGIN_FAILED_CANNOT_OPEN_CRED_STORE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The login was not successful because the Entrust security store cannot be opened.	Some kind internal error occurred that should never happen.	The logs may indicate the problem.
IDES_LOGIN_FAILED_ROAM_SUSPENDED		
The login was not successful because the Entrust security store is suspended by the Entrust Authority Roaming Server.	If the user is attempting to login to an Entrust security store that is suspended by the Entrust Authority Roaming Server.	Wait until the suspension is over (hard to tell because it is configurable), or recover the Entrust digital ID, or unsuspend on the server.
IDES_ALL_CERTS_REVOKED		
All of your certificates have been revoked. You can continue to work but your digital signatures will not be trusted and updates will not be performed. You will need to recover your digital ID to ensure your digital signatures are trusted and that you receive any necessary updates.	All of the Entrust digital ID's certificates have been revoked.	Recover the Entrust digital ID.
IDES_NO_KEYS		
Your Entrust security store contains no keys. You will need to recover your digital ID.	The user has just logged into an Entrust security store that doesn't contain any keys. This should never happen but strange development situations have caused it to occur.	Recover the Entrust digital ID.
IDES_UPDATE_FAILED_UNKNOWN		
Your digital ID was not successfully updated. The update failed because an unknown error was encountered.	An update was attempted but an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_UPDATE_FAILED_CERT_TYPE_REMOVED		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Management of your Entrust digital ID was not successful. Your Entrust digital ID type has been removed from the Certification Authority's policy certificate.	An update was attempted but user's certificate type was removed from the CA's policy certificate.	Recover the Entrust digital ID. Restore certificate type to the CA.
IDES_LOGIN_FAILED_ROAM_UNKNOWN_USERID		
The login was not successful because the specified Entrust roaming security store could not be found. Please ensure you typed the correct Entrust roaming security store name.	The specified Entrust roaming security store does not exist on any known Entrust Authority Roaming Server.	Type the correct Entrust roaming security store name. Check that the Entrust Authority Roaming Server is configured to search the correct Directory areas for the security stores.
IDES_PASSWORD_HISTORY_FAILED		
Password change did not complete successfully. The password you typed was previously used. You must not reuse your last %1!i! passwords. Please select a new password.	User typed a password that was previously used for the selected Entrust security store during password change.	Select a new password.
IDES_LOGIN_FAILED_EPF_CORRUPT		
The login was not successful because the Entrust security store is corrupt. You will need to recover your digital ID.	If the user selects an Entrust security store that is corrupt during login. The file has likely been modified using a application that doesn't recognize the format.	Recover the Entrust digital ID.
IDES_LOGIN_FAILED_EPF_INVALID_VERSION		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The login was not successful because the Entrust security store is not a supported version. You will need to recover your digital ID with Entrust Entelligence Security Provider for Windows to update to a supported version.	If the user selects an Entrust security store that isn't a supported version. Security Provider for Windows supports version 3 and the new version 4. Version 1 and 2 are not supported and haven't been used since Entrust/PKI 2.0.	Recover the Entrust digital ID.
IDES_LOGIN_FAILED_EPF_INVALID_FORMAT		
The login was not successful because the Entrust security store is has been modified incorrectly. The contents can not be trusted. You will need to recover your digital ID.	If the user selects an Entrust security store that is not in a valid format. An invalid format means that while the file is not corrupt and the data format is recognized, something is not correct for the specified version. The file has likely been modified using a application that does not recognize the format version.	Recover the Entrust digital ID.
IDES_LOGIN_FAILED_ROAM_ERROR		
The login was not successful because there was an error communicating with the Entrust Authority Roaming Server.	The communication with the Entrust Authority Roaming Server failed during login.	The logs may indicate the problem.
IDES_LOGIN_FAILED_ROAM_INVALID_VERSION		
The login was not successful because the Entrust Authority Roaming Server is not a supported version.	The Entrust Authority Roaming Server that has the Entrust roaming security store isn't a supported version. Security Provider for Windows required version 6.0 and higher. Note: Security Provider for Windows requires a patched 6.0 Roaming Server.	Roaming Server must be upgraded to the patched 6.0 or higher release.
IDES_LOGIN_FAILED_ROAM_INVALID_ALG_TYPE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The login was not successful because the Entrust Authority Roaming Server does not support the encryption algorithm configured for communication.	The communication with the Entrust Authority Roaming Server failed because the server doesn't support the encryption algorithm configured in the registry.	Enable the required encryption algorithm on the server or change the algorithm specified in the registry.
IDES_LOGIN_FAILED_ROAM_NO_SERVERS		
The login was not successful because no Entrust Authority Roaming Servers are configured locally.	The login cannot be processed because the registry doesn't list an Entrust Authority Roaming Server.	Check the registry configuration to ensure an Entrust Authority Roaming Server is specified.
IDES_UPDATE_FAILED_FAIL_UPDATE_CERT_LIST		
Your digital ID was not successfully updated. The update failed because an internal list of certificates could not be updated.	An update was attempted by an internal error occurred updating the internal certificate lists.	The logs may indicate the problem.
IDES_UPDATE_FAILED_FAIL_DECODE_ROLE_MAP		
Management of your Entrust digital ID was not successful. Your Certification Authority's policy certificate could not be processed.	An update was attempted but the CA's policy certificate could not be decoded.	The logs may indicate the problem.
IDES_UPDATE_FAILED_CANNOT_FIND_CSETTING_POLICY_CERTIFICATE		
Management of your Entrust digital ID was not successful. Your Certification Authority's policy certificate could not be found.	An update was attempted but the role base policy certificate could not be found.	Check that CA's role base policy certificates are being published.
IDES_UPDATE_FAILED_CANNOT_FIND_MAIN_POLICY_CERT		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Management of your Entrust digital ID was not successful. Your Certification Authority's policy certificate could not be found in the local certificate stores.	An update was attempted but the main policy certificate could not be found.	Check that CA's main policy certificates are being published.
IDES_UPDATE_FAILED_FAIL_GET_ISSUER_CERT_FROM_STORE		
Your digital ID was not successfully updated. The update failed because the your certification authority's certificate could not be found.	An update was attempted but the CA's certificate could not be found in the certificate store.	Recover the Entrust digital ID or try to re-login to the Entrust security store.
IDES_UPDATE_FAILED_FAIL_SET_CSET_POLICY_CERT_PROP		
Your digital ID was not successfully updated. The update failed because the policy certificate could not be saved for the certificate with serial number %1!s!.	An update was attempted but the role base policy certificate could not be saved.	Ensure that the registry has not run out of room.
IDES_UPDATE_FAILED_FAIL_SET_CD_POLICY_CERT_PROP		
Your digital ID was not successfully updated. The update failed because the certificate definition policy certificate could not be saved for the certificate with serial number %1!s!.	An update was attempted but the certificate definition policy certificate could not be saved.	Ensure that the registry has not run out of room.
IDES_LOGIN_FAILED_EPF_INVALID_V4_FORMAT		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The login was not successful because the Entrust security store is has been modified incorrectly by another application. The contents can not be trusted. You will need to recover your digital ID.	If the user selects an Entrust security store that is not in a valid format for version 4. An invalid format means that while the file is not corrupt and the data format is recognized, something is not correct for the specified version. The file has likely been modified using an application that does not recognize the format version 4 but does recognize version 3 and properly updated the version 3 sections.	Recover the Entrust digital ID and stop using the older application.
IDES_LOGIN_FAILED_OUT_OF_MEMORY		
The login was not successful due to lack of memory.	While logging in to the Entrust security store, a memory allocation failed.	Close a few applications or adjust the virtual memory settings.
IDES_LOGIN_FAILED_EPF_CANNOT_READ		
The login was not successful because the security store could not be read. This is not a valid security store. Please ensure you logging in to a valid security store.	While logging in, the Entrust security store was found to be invalid. This can occur if the security store in the roaming server is invalid.	Recover the Entrust digital ID.
IDES_LOGIN_FAILED_UNKNOWN		
The login was not successful due to an internal error.	While logging in the Entrust security store an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_LOGIN_FAILED_FILE_ERROR		
The login was not successful because of an error processing the Entrust security store file. %1!s!.	While logging in the Entrust security store an error was encountered opening or reading the file. The OS-specific message is included inside our message.	Depends on the OS-specific message.

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
IDES_UNLOCK_FAILED_INCORRECT_PASSWORD		
The Entrust security store was not successfully unlocked because the password is not correct. Please retype your password. Please ensure you are using the correct case and that Caps Lock is not accidentally on.	User typed incorrect password for the selected Entrust security store during unlock.	Type the correct password for the current Entrust security store.
IDES_UNLOCK_FAILED_CRED_STORE_SUSPENDED		
The Entrust security store was not successfully unlocked because the Entrust security store is suspended due to too many unsuccessful password attempts.	If the user is attempting to unlock to an Entrust security store that is suspended by the Entrust Authority Roaming Server.	Wait until the suspension is over (hard to tell because it is configurable,) or recover the Entrust digital ID, or unsuspend on the server.
IDES_UNLOCK_FAILED_UNKNOWN		
The Entrust security store was not successfully unlocked due to an internal error.	While unlocking the Entrust security store an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_INITIAL_SAVE_FAILED_UNKNOWN		
The Entrust security store was not successfully saved due to an internal error. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	While saving the Entrust security store for the first time an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_INITIAL_SAVE_FAILED_CANNOT_SAVE_CRED_STORE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust security store was not successfully saved due to an internal error. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	While saving the Entrust security store for the first time an internal error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_INITIAL_SAVE_FAILED_OUT_OF_MEMORY		
The Entrust security store was not successfully saved due to a lack of memory. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	While saving the Entrust security store for the first time a memory allocation failed.	Close a few applications or adjust the virtual memory settings.
IDES_INITIAL_SAVE_FAILED_FILE_ERROR		
The Entrust security store was not successfully saved because of an error processing the Entrust security store file. %1!s!. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	While saving the Entrust security store the very first time an error was encountered opening or reading the file. The OS-specific message is included inside our message.	Depends on the OS-specific message.
IDES_INITIAL_SAVE_FAILED_ROAM_ERROR		
The Entrust security store was not successfully saved because there was an error communicating with the Entrust Authority Roaming Server. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	While saving the Entrust security store for the first time an error was encountered communicating with the Entrust Authority Roaming Server.	The logs may indicate the problem.
IDES_INITIAL_SAVE_FAILED_ROAM_INVALID_VERSION		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust security store was not successfully saved because the Entrust Authority Roaming Server is not a supported version. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	The Entrust Authority Roaming Server that has the Entrust roaming security store isn't a supported version. Security Provider for Windows required version 6.0 and higher. Note: Security Provider for Windows requires a patched 6.0 Roaming Server.	Roaming Server must be upgraded to the patched 6.0 or higher release.
IDES_INITIAL_SAVE_FAILED_ROAM_INVALID_ALG_TYPE		
The Entrust security store was not successfully saved because the Entrust Authority Roaming Server does not support the encryption algorithm configured for communication. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	The communication with the Entrust Authority Roaming Server failed because the server doesn't support the encryption algorithm configured in the registry.	Enable the required encryption algorithm on the server or change the algorithm specified in the registry.
IDES_INITIAL_SAVE_FAILED_ROAM_UNKNOWN_USERID		
The Entrust security store was not successfully saved to the Entrust Authority Roaming Server because the specified Entrust roaming security store name is already in use. Please select a new Entrust roaming security store name.	The specified Entrust roaming security store does not exist on any known Entrust Authority Roaming Server.	Type the correct Entrust roaming security store name. Check that the Entrust Authority Roaming Server is configured to search the correct Directory areas for the security stores.
IDES_INITIAL_SAVE_FAILED_ROAM_NO_SERVERS		
The Entrust security store was not successfully saved because no Entrust Authority Roaming Servers are configured locally. The contents of the Entrust security store will be lost. You will need to recover your digital ID.	The login cannot be processed because the registry doesn't list any Entrust Authority Roaming Servers.	Ensure that an Entrust Authority Roaming Server is specified in the registry.

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
IDES_SAVE_FAILED_UNKNOWN		
The Entrust security store was not successfully saved due to an internal error. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	While saving the Entrust security store an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.Try to log back in to the Entrust security store and continue working.
IDES_SAVE_FAILED_CANNOT_SAVE_CRED_STORE		
The Entrust security store was not successfully saved due to an internal error. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	While saving the Entrust security store an internal error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_SAVE_FAILED_OUT_OF_MEMORY		
The Entrust security store was not successfully saved due to a lack of memory. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	While saving the Entrust security store a memory allocation failed.	Close a few applications or adjust the virtual memory settings.
IDES_SAVE_FAILED_FILE_ERROR		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust security store was not successfully saved because of an error processing the Entrust security store file. %1!s!. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	While saving the Entrust security store an error was encountered opening or reading the file. The OS-specific message is included inside our message.	Depends on the OS-specific message.
IDES_SAVE_FAILED_ROAM_ERROR		
The Entrust security store was not successfully saved because there was an error communicating with the Entrust Authority Roaming Server. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	While saving the Entrust security store an error was encountered communicating with the Entrust Authority Roaming Server.	The logs may indicate the problem.
IDES_SAVE_FAILED_ROAM_INVALID_VERSION		
The Entrust security store was not successfully saved because the Entrust Authority Roaming Server is not a supported version. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	The Entrust Authority Roaming Server that has the Entrust roaming security store isn't a supported version. Security Provider for Windows required version 6.0 and higher. Note: Security Provider for Windows requires a patched 6.0 Roaming Server.	Roaming Server must be upgraded to the patched 6.0 or higher release.
IDES_SAVE_FAILED_ROAM_INVALID_ALG_TYPE		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust security store was not successfully saved because the Entrust Authority Roaming Server does not support the encryption algorithm configured for communication. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically redone after the next login, other changes will need to be redone manually.	The communication with the Entrust Authority Roaming Server failed because the server does not support the encryption algorithm configured in the registry.	Enable the required encryption algorithm on the server or change the algorithm specified in the registry.
IDES_SAVE_FAILED_ROAM_UNKNOWN_USERID		
The Entrust security store was not successfully saved because the specified Entrust Roaming security store could not be found. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically be redone after the next login, other changes will need to be redone manually.	The specified Entrust roaming security store does not exist on any known Entrust Authority Roaming Server.	Type the correct Entrust roaming security store name. Check that the Entrust Authority Roaming Server is configured to search the correct Directory areas for the security stores.
IDES_SAVE_FAILED_ROAM_NO_SERVERS		
The Entrust security store was not successfully saved because no Entrust Authority Roaming Servers are configured locally. All changes and digital ID updates to the Entrust security store will be lost. Updates to your digital ID will automatically be redone after the next login, other changes will need to be redone manually.	The registry does not list any Entrust Authority Roaming Servers, so the save cannot be processed.	Check the registry configuration to ensure that an Entrust Authority Roaming Server is specified.
IDES_SWITCH_TO_ROAMING_FAILED_UNKNOWN		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server due to an internal error. You will continue to work as an Entrust desktop user.	While saving the Entrust security store to the roaming server an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_SWITCH_TO_ROAMING_FAILED_CANNOT_SAVE_CRED_STORE		
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server due to an internal error. You will continue to work as an Entrust desktop user.	While saving the Entrust security store to the roaming server an internal error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_SWITCH_TO_ROAMING_FAILED_OUT_OF_MEMORY		
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server due to a lack of memory. You will continue to work as an Entrust desktop user.	While saving the Entrust security store to the roaming server a memory allocation failed.	Close a few applications or adjust the virtual memory settings.
IDES_SWITCH_TO_ROAMING_FAILED_ROAM_ERROR		
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server because there was an error communicating with the Entrust Authority Roaming Server. You will continue to work as an Entrust desktop user.	While saving the Entrust security store to the roaming server an error was encountered communicating with the Entrust Authority Roaming Server.	The logs may indicate the problem.
IDES_SWITCH_TO_ROAMING_FAILED_ROAM_INVALID_VERSION		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server because the Entrust Authority Roaming Server is not a supported version. You will continue to work as an Entrust desktop user.	The Entrust Authority Roaming Server that has the Entrust roaming security store isn't a supported version. ESP required version 6.0 and higher. Note: Security Provider for Windows requires a patched 6.0 Roaming Server.	Roaming Server must be upgraded to the patched 6.0 or higher release.
IDES_SWITCH_TO_ROAMING_FAILED_ROAM_INVALID_ALG_TYPE		
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server because the Entrust Authority Roaming Server does not support the encryption algorithm configured for communication. You will continue to work as an Entrust desktop user.	The communication with the Entrust Authority Roaming Server failed because the server doesn't support the encryption algorithm configured in the registry.	Enable the required encryption algorithm on the server or change the algorithm specified in the registry.
IDES_SWITCH_TO_ROAMING_FAILED_ROAM_UNKNOWN_USERID		
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server because the specified Entrust roaming security store name is already in use. Please select a new Entrust roaming security store name.	The specified Entrust roaming security store does not exist on any known Entrust Authority Roaming Server.	Type the correct Entrust roaming security store name. Check that the Entrust Authority Roaming Server is configured to search the correct Directory areas for the security stores.
IDES_SWITCH_TO_ROAMING_FAILED_ROAM_NO_SERVERS		
The Entrust desktop security store was not successfully saved to the Entrust Authority Roaming Server because no Entrust Authority Roaming Servers are configured locally. You will continue to work as an Entrust desktop user.	The registry does not list an Entrust Authority Roaming Servers, so the save cannot be processed.	Check the registry configuration to ensure that an Entrust Authority Roaming Server is specified.
IDES_SWITCH_TO_DESKTOP_FAILED_UNKNOWN		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust roaming security store was not successfully saved to %1!s! due to an internal error. You will continue to work as an Entrust roaming user.	While saving the Entrust security store locally an unknown error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_SWITCH_TO_DESKTOP_FAILED_CANNOT_SAVE_CRED_STORE		
The Entrust roaming security store was not successfully saved to %1!s! due to an internal error. You will continue to work as an Entrust roaming user.	While saving the Entrust security store locally an internal error has occurred. This should never happen but the error message exists as a final catch all.	The logs may indicate the problem.
IDES_SWITCH_TO_DESKTOP_FAILED_OUT_OF_MEMORY		
The Entrust roaming security store was not successfully saved to %1!s! due to a lack of memory. You will continue to work as an Entrust roaming user.	While saving the Entrust security store locally a memory allocation failed.	Close a few applications or adjust the virtual memory settings.
IDES_SWITCH_TO_DESKTOP_FAILED_FILE_ERROR		
The Entrust roaming security store was not successfully saved to %1!s! because of an error processing the Entrust security store file. %2!s!. You will continue to work as an Entrust roaming user.	While saving the Entrust security store locally an error was encountered opening or reading the file. The OS-specific message is included inside our message.	Depends on the OS-specific message.
IDES_STORE_DOESNT_HAVE_REQUIRED_KEY		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The Entrust security store you selected to log into does not contain the private key that is required to complete the current operation. This login will be cancelled so that the correct Entrust security store can be selected. If you have multiple Entrust security stores, please select another store. If you have only one Entrust security store, your digital ID may be corrupt and you will need to recover it.	If the user selects a security store that doesn't contain the keys that the CSP needs.	Select the Entrust security store that was initially specified in the login dialog (the correct security store is pre-selected).
IDES_CHANGE_PWD_FAILED_TOOMANY_LOGINS		
You have supplied an incorrect password 3 times. The Entrust Security Store Change Password Wizard will be cancelled. Please ensure you are typing your password correctly.	If the user enters an incorrect password three times during password change. The wizard closes to slow down a password crackers that may be attempting to script the change password wizard.	The change password wizard must be restarted.
IDES_UPDATE_FAILED_MISSING_MSG_SIGNING_CERT		
Management of your Entrust digital ID was not successful. You are missing a verification certificate to authenticate to the Certification Authority. If you are using a smart card with your Entrust digital ID, inserting the smart card may restore the missing certificate.	Management of the Entrust digital ID was not done because a verification certificate could not be found on the machine capable of signing requests to the CA.	The missing certificate must be added to the certificate store. If you have a mixed Entrust digital ID, then logging into all parts of the digital ID should replace the missing certificate. If not, a recovery must be performed.
IDES_UPDATE_FAILED_INCORRECT_SKP_CLIENT_SETTINGS		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Management of your Entrust digital ID was not successful. Your single key pair Entrust digital ID has been incorrectly configured. Your administrator must configure your Certification Authority to support a single key pair Entrust Digital ID.	Management of the Entrust digital ID was not done because the user has a single key pair in their certificate definitions but the client side settings policy certificate does not say they are a single key pair user.	Change the client-side settings policy to say the number of key pairs is one.
IDES_UPDATE_FAILED_MISSING_CERT_FROM_STORE		
Management of your Entrust digital ID was not successful. There are missing certificates. If you are using a smart card with your Entrust digital ID, inserting the smart card may restore the missing certificates.	Management of the Entrust digital ID was not done because not all the user's certificates are available.	The missing certificates must be added to the certificate store. If you have a mixed Entrust digital ID, then logging into all parts of the digital ID should replace the missing certificates. If not, a recovery must be performed.
IDES_UPDATE_FAILED_DISABLE_USER_STATE		
Updating your Entrust digital ID was not successful. Your digital ID has been disabled at the Certification Authority. Your digital ID needs to be enabled to ensure you receive the necessary updates.	Management of the Entrust digital ID was not done because the user is in the disabled state at the CA.	Enable the Entrust digital ID at the CA.
IDES_CANNOT_READ_PROFILE		
The file '%1!s!' cannot be read. %2!s!	The specified Entrust security store could not be read. The system error will appear as the second sentence.	Depends on the system error.
IDES_UPDATE_FAILED_UNKNOWN_CERT_ERROR		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Your digital ID was not successfully updated. The update failed due to an internal error when processing the certificate with serial number %1!s!.	Management of the Entrust digital ID was not done because something internal failed when processing the specified certificate.	If the certificate is corrupted in the certificate store, an export/import of the certificate may fix the problem. Check the logs for more details.
IDES_NO_CERT_HISTORY		
Your Entrust security store does not contain a certificate history. A certificate history is required to decrypt data that has been protected using old encryption certificates. You may need to recover your digital ID if you are unable to decrypt existing data.	The user is using a V3 EPF with Security Provider for Windows. A V3 EPF does not contain a certificate history and thus old data may not be successfully decrypted.	Recover the Entrust digital ID to create a V4 EPF.
IDES_PROFILE_WIZARD_CANNOT_WRITE_FILE		
The folder %1!s! could not be written to. %2!s!	The specified folder for the Entrust security store could not be written to. The system error will appear as the second sentence.	Depends on the system error.
IDES_ENROLL_FAILED_ROAM_UNKNOWN_ERROR		
Creating an Entrust roaming security store is not possible because an internal error was encountered connecting to the Entrust Authority Roaming Server.	An internal error was encountered when trying to verify if the Entrust Authority Roaming Server is running.	Check the logs and ensure that the server is running.
IDES_ENROLL_FAILED_ROAM_INVALID_VERSION		
Creating an Entrust roaming security store is not possible because the Entrust Authority Roaming Server is not a supported version.	An unsupported version of the Entrust Authority Roaming Server was detected.	Upgrade the server to a supported version.
IDES_ENROLL_FAILED_ROAM_CANNOT_CONNECT		

Table 1: Security Provider for Windows IDES error messages

Error message	**When this message will occur**	**Solution or way to work around this message**
Creating an Entrust roaming security store is not possible because the Entrust Authority Roaming Server is not responding.	The Entrust Authority Roaming Server did not respond.	Check that the server is running.
IDES_UPDATE_FAILED_ROLLOVER_NOT_ALLOWED		
Your digital ID needs to be updated but cannot because updates are not allowed. You will need to recover your digital ID to ensure you receive the necessary updates.	An update must be performed but updates are not allowed for this Entrust digital ID.	Recover the Entrust digital ID.
IDES_UPDATE_FAILED_EXPIRED_SIGN_CERT		
Your digital ID needs to be updated but cannot because your signing certificate has expired. You will need to recover your digital ID to ensure you receive the necessary updates.	An update must be performed but the Entrust digital ID's signing certificate has expired.	Recover the Entrust digital ID.
IDES_UPDATE_FAILED_EXPORT_HOLD_USER_STATE		
Updating your Entrust digital ID was not successful. Your digital ID has been disabled at the Certification Authority. Your digital ID needs to be enabled to ensure you receive the necessary updates.	Management of the Entrust digital ID was not done because it has been exported from the CA.	Recover the user from the exported CA or allow Security Provider for Windows to perform an automatic move.
IDES_UPDATE_FAILED_RECOVERY_USER_STATE		
Your digital ID needs to be updated but cannot because you have been placed in key recovery mode at the CA. You will need to recover your digital ID to ensure you receive the necessary updates.	An update must be performed but updates are not allowed because the Entrust digital ID is already in key recover mode.	Complete the recovery already in progress.

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
IDES_UPDATE_FAILED_NO_SIGN_CERT		
Your digital ID needs to be updated but cannot because you don't have a valid signing certificate. You will need to recover your digital ID to ensure you receive the necessary updates.	An update must be performed but the Entrust digital ID doesn't contain a signing certificate.	Recover the Entrust digital ID.
IDES_NOT_GENERATED_PASSWORD		
The password you typed is not one of the generated passwords provided. Please select one of the generated passwords.	The user was given three choices for password selection, and the user did not type one of those three passwords correctly.	Choose one of the passwords and enter it correctly.
IDES_LOGIN_FAILED_EPF_UNKNOWN_MAC_ALG		
The login was not successful because the Entrust security store is protected using an unknown protection method. You will need to recover your digital ID.	The MAC algorithm used to protect the Entrust Security Store is not supported. The likely cause is that the Entrust Security Store was created by a different application, which is using an unsupported MAC algorithm.	Recover the Entrust digital ID using Security Provider.
IDES_LOGIN_FAILED_UNAVAILABLE_MAC_ALG		
The login was not successful because the Entrust security store is protected using a protection method that is unavailable from this computer. You will need to recover your digital ID if you need to use it on this computer.	The special MAC algorithm used to support the HP Protect tools was used to protect the Entrust Security Store, but the user is logging into their Entrust Security Store at a computer that does not have the HP Protect Tools installed.	If it is necessary to log into computers that do not have the HP Protect tools installed, recover the Entrust digital ID so that a supported MAC algorithm can be used to protect the Entrust Security Store.
IDES_PROFILE_WIZARD_CREATE_FAILED		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Creating the Entrust security store '%1!s!' was not successful. An internal error has occurred.	An unexpected internal error occurred when creating the Entrust Security Store. This should not occur.	Try the enrollment or recovery again.
IDES_INVALID_POLICY_CERTS		
The mandatory policy for your Entrust security store is unavailable. You will not be able to modify any Entrust security store options. The policy will be updated automatically when communication with the Directory is established.	The Main policy certificate has not been retrieved from the directory, and cached locally for the Entrust Login Service to use.	When communication with the Directory is established, the policy will be updated automatically.
IDES_OFFLINE_ROAM		
You have logged in offline to your Entrust roaming security store. Updates to your Entrust digital ID will not be performed and password changes are disabled. You may modify your Entrust security store options but those changes will be lost when you access the online version of your Entrust roaming security store.	The user has logged in offline to a roaming security store.	Go on-line to receive updates.
IDES_OFFLINE_ROAMING_OPTIONS		
You are working offline with your Entrust roaming security store. The changes you have made to your Entrust security store options will be lost when you access the online version of your Entrust roaming security store.	The user has logged in offline to a roaming security store, and has made changes to their options.	Do not make changes to options when off-line, or understand that they will not be saved when the user goes on-line.
IDES_LOGIN_FAILED_OFFLINE_ROAM_EXPIRED		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
The login was not successful because the Entrust Authority Roaming Server is not available and the offline version of your Entrust roaming security store has expired.	The offline version has expired and is no longer valid.	Go on-line to receive a fresh copy of the Entrust roaming security store.
File encryption and digital sign error message		
IDES_CANNOT_REPROTECT_FILE		
Cannot re-protect '%1!s!'.\n\n An error occurred while associating with Entrust Entelligence Security Provider Shell Extension.	The Security Provider Sign/Encrypt/Sign and Encrypt wizard was unable to open the prompt.	The Security Provider shell extension has not been correctly installed. Repair the Security provider installation.
IDES_DELETE_FAILURE		
Cannot delete '%1!s!'. %2!s! You will need to delete this file manually.	The attempt to delete the file has been failed by Windows. The second substitution will provide the Windows error message giving more details.	No generic solution; see the Windows error message.
IDES_ENC_CERT_ERRORS_ENCOUNTERED_HAVE_REASON		
Your encryption certificate was not successfully validated. %1!s! Recovering your digital ID may fix the validation problem.	The validation of the selected encryption certificate has failed. The second substitution will give more details about the failure.	No generic solution; see the details part of the message. Recover the Entrust digital ID.
IDES_ENC_CERT_ERRORS_ENCOUNTERED_NO_REASON		
Your encryption certificate was not successfully validated. Recovering your digital ID may fix the validation problem.	The validation of the selected encryption certificate has failed. A detailed description is not available for this failure.	Recover the Entrust digital ID.
IDES_ENCRYPT_FAILURE		
Cannot encrypt '%1!s!'. %2!s!"	Encrypting the file has failed. The second substitution will give more details about the failure.	No generic solution; see the details part of the message.
IDES_ENCRYPT_FAILURE_NO_CONTENTS		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Cannot encrypt '%1!s!'. The file is empty.	Encrypting the file has failed because it is empty.	You cannot encrypt empty files.
IDES_ENCRYPT_FAILURE_NO_FILE		
Cannot encrypt '%1!s!'. The file does not exist.	Encrypting the file has failed because it does not exist.	Select another file.
IDES_ENCRYPTSIGN_FAILURE		
Cannot encrypt and sign '%1!s!'. %2!s!	Encrypting and signing the file has failed. The second substitution will give more details about the failure.	No generic solution; see the details part of the message.
IDES_ENCRYPTSIGN_FAILURE_NO_CONTENTS		
Cannot encrypt and sign '%1!s!'. The file is empty.	Encrypting and signing the file has failed because it is empty.	You cannot encrypt empty files.
IDES_ENCRYPTSIGN_FAILURE_NO_FILE		
Cannot encrypt and sign '%1!s!'. The file does not exist.	Encrypting and signing the file has failed because it does not exist.	Select another file.
IDES_FILE_TOO_LARGE		
Cannot create '%1!s!'. There is not enough free disk space.	The output file cannot be created because the disk is full.	Free up space on the disk.
IDES_dd_ERRORS_ENCOUNTERED_HAVE_REASON		
"%1!s!'s encryption certificate was not successfully validated.%2!s! You cannot encrypt for %1!s!.	The validation of the selected encryption certificate has failed. The second substitution will give more details about the failure.	No generic solution; see the details part of the message. Recover the Entrust digital ID.
IDES_OTHER_CERT_ERRORS_ENCOUNTERED_NO_REASON		
%1!s!'s encryption certificate was not successfully validated. You cannot encrypt for %1!s!.	The validation of the selected encryption certificate has failed. A detailed description is not available for this failure.	Recover the Entrust digital ID.
IDES_SEARCH_FAILURE_NO_CERTS_FOUND		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Your search for people has completed successfully but no certificates were found.	The searching of the Directory has completed but no certificates were found that matched the search.	The search may have been done incorrectly (for example, a misspelled name) or the Directory is not configured properly
IDES_SEARCH_FAILURE_NO_DIRECTORIES		
You cannot search for people because no directories are available. Your computer has not been configured to access any directories.	Searching the Directory cannot be done because Security Provider for Windows hasn't been configured with any Directories to search. This message will appear before the Search for People dialog appears.	Configure at least one Directory. This can be done in the Custom Installation Wizard.
IDES_SEARCH_FAILURE_NO_SERVERS		
Your search for people has been unsuccessful. Your computer has not been configured to access any directories.	Searching the Directory cannot be done because Security Provider for Windows hasn't been configured with any Directories to search. This message will appear if the Search for People dialog appears but no Directories are configured when the OK button is pressed.	Configure at east one Directory. This can be done in the Custom Installation Wizard.
IDES_SEARCH_FAILURE_SEARCH_ERROR		
Your search for people has been unsuccessful. An error occurred during the search.	A search of the Directory has failed.	Check the Security Provider for Windows log file for more information about the failure.
IDES_SIGN_CERT_ERRORS_ENCOUNTERED_HAVE_REASON		
Your signing certificate was not successfully validated. %1!s! Recovering your digital ID may fix the validation problem.	The validation of the selected signing certificate has failed. The second substitution will give more details about the failure.	No generic solution; see the details part of the message says. Recover the Entrust digital ID.
IDES_SIGN_CERT_ERRORS_ENCOUNTERED_NO_REASON		

Table 1: Security Provider for Windows IDES error messages

Error message	When this message will occur	Solution or way to work around this message
Your signing certificate was not successfully validated. Recovering your digital ID may fix the validation problem.	The validation of the selected signing certificate has failed. A detailed description is not available for this failure.	Recover the Entrust digital ID.
IDES_SIGN_FAILURE		
Cannot sign '%1!s!'. %2!s!	Signing the file has failed. The second substitution will give more details about the failure.	No generic solution; see the details part of the message.
IDES_SIGN_FAILURE_NO_CONTENTS		
Cannot sign '%1!s!'. The file is empty.	Signing the file has failed because the file is empty.	You cannot sign empty files.
IDES_SIGN_FAILURE_NO_FILE		
Cannot sign '%1!s!'. The file does not exist.	Signing the file has failed because the file does not exist.	Select another file.

Index

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