Obtaining technical support

For support assistance by telephone call one of the numbers below:

- 1-877-754-7878 in North America
- 1-613-270-3700 outside North America

You can also email Customer Support at: support@entrust.com

Copyright © 2009 Entrust. All rights reserved.

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

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

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.
Overview .................................................................5
  Purpose and scope .................................................. 5
  Requirements ......................................................... 6
  Architecture ......................................................... 6

Configuring for Windows Smart Card Logon ....................9
  Obtaining the Entrust configuration tools for Windows Smart Card Logon  .... 10
  Obtaining the fully qualified host name and GUID ................... 12
  Creating a Domain Controller certificate ........................... 13
  Enrolling the certificate for the Domain Controller .................... 23
  Distributing the CA certificate(s) to the trusted root store of all Domain Controllers .................................................. 26
    Downloading the certification authority certificate(s) ............. 26
    Running the Entrust installCert.bat ................................ 28
  Configuring users for Windows Smart Card Logon .................. 30
  Smart Card Logon in Vista ........................................... 43
  Troubleshooting ..................................................... 44
Overview

This guide documents how to use Entrust digital certificates for Windows Smart Card Logon.

Using Windows Smart Card Logon technology provides:

- tamper-resistant storage for user logon credentials
- isolation of the secure processes involved in authentication, digital signing, and key exchange from other parts of the network
- portability of credentials

Note: For Microsoft Windows 2000 users, remote access for Windows Smart Card Logon is not supported as a result of a limitation with Microsoft Windows 2000.

Purpose and scope

This document details the steps required to configure Windows Smart Card Logon. To enable a Windows Smart Card Logon environment, you must:

1. Create Domain Controller certificates for Windows Smart Card Logon through a Web-based application.
2. Enroll all Domain Controller certificates on to the Windows Domain Controller through a Web-based application.
3. Distribute the certification authority (CA) certificate(s) to the trusted root store of all Domain Controllers.
**Requirements**

You require the following prior to configuring your environment for Windows Smart Card Logon:

- Machines with the Windows operating system
- Internet access for retrieving certificate revocation lists (CRLs)
- Directory with the users you want to configure for Windows Smart Card Logon
- Supported Web browser

**Architecture**

**Figure 1: Windows Smart Card Logon overview**

1. Insert either smart card or token into computer and enter PIN
2. Retrieve certificate from smart card or token
3. Send certificate
4. Verify certificate
5. Look up user entry in directory
6. Build TGT
7. Send TGT
8. Sent TGT

1. When the user inserts the smart card or token, Windows prompts for a Personal Identification Number (PIN) in a logon window.

**Note:** Windows Vista does not automatically prompt for logon. Users must press Ctrl+Alt+Del to call the logon window. For more information on Vista differences, see "Smart Card Logon in Vista" on page 43.

2. The smart card subsystem authenticates the user as the owner of the smart card or token, and retrieves the certificate from the card.
3 The smart card client software sends the certificate to the Kerberos Key Distribution Center (KDC) on the Domain Controller.

4 The KDC verifies the Smart Card Logon certificate by building a certificate chain until it finds the root CA certificate. During the verification process, each certificate in the chain is checked against the Certification Revocation List (CRL) in the CRL Distribution Point (CDP).

5 The KDC retrieves the UserPrincipalName (UPN) from the subjectAltName of the Smart Card Logon certificate, and uses it as a reference to look up the user entry in the directory.

6 The KDC builds a Kerberos ticket-granting ticket (TGT), which contains the user account and access control information.

7 The KDC encrypts the TGT with a session key, encrypts that key with the user's public key, and returns the encrypted TGT to the user's workstation.

8 The smart card decrypts the session key with its private key, and uses the session key to decrypt the TGT. At this point, the KDC lets the user log in to the Windows domain.
Configuring for Windows Smart Card Logon

This chapter provides the steps required to configure Windows Smart Card Logon using Entrust certificates.

This chapter includes:

- “Obtaining the Entrust configuration tools for Windows Smart Card Logon” on page 10
- “Obtaining the fully qualified host name and GUID” on page 12
- “Creating a Domain Controller certificate” on page 13
- “Enrolling the certificate for the Domain Controller” on page 23
- “Distributing the CA certificate(s) to the trusted root store of all Domain Controllers” on page 26
- “Configuring users for Windows Smart Card Logon” on page 30
- “Smart Card Logon in Vista” on page 43
- “Troubleshooting” on page 44
Obtaining the Entrust configuration tools for Windows Smart Card Logon

Entrust created tools to help with the configuration of Smart Card Logon. These tools include:

- `getGUID.bat` and `getGUID.vbs`: This tool extracts the fully qualified host name and the Global User ID (GUID) in the correct, dashed format, from the Domain Controller for inclusion in a Domain Controller certificate.
- `installCerts.bat` and `installCerts.vbs`: This tool helps you to install the certification authority (CA) certificate(s) as a trust anchor for Smart Card Logon. It can also install a Domain Controller certificate if Entrust Entelligence Security Provider for Windows is not being used.

These tools must be saved to a folder on your Domain Controller.

Complete the following procedure to download the `SmartCardLogonTools.zip` file that contains the tools.

**To obtain the Entrust configuration tools for Windows Smart Card Logon**

1. Log in to Administration Services. See “To log in to Administration Services” on page 13 for more information.
2. From the left pane under **Help**, click **Smart Card Logon tools**.
   
The File Download dialog box appears.

![File Download dialog box](image)
3 Click **Save** to save the files to a folder on your Domain Controller. Files in the zip include:
   - `getGUID.bat` and `getGUID.vbs`
   - `installCerts.bat` and `installCerts.vbs`

4 Extract the files so they are available to run in the following procedure.
Obtaining the fully qualified host name and GUID

Smart Card Logon requires the Domain Controller certificate to contain the fully qualified host name and GUID. Entrust provides a tool that extracts this information, and presents it in the format required for inclusion in the Domain Controller certificate.

Complete the following procedure to obtain the fully qualified host name and GUID.

To obtain the fully qualified host name and GUID

1. Navigate to the folder on your Domain Controller where you saved the getGUID.bat and getGUID.vbs files as described in “To obtain the Entrust configuration tools for Windows Smart Card Logon” on page 10.

2. Double-click getGUID.bat.

A window appears listing the required information for your Domain Controller certificate. The tool also creates a file in the folder where the tool is saved named <hostname>-SANInfo.txt, which also contains this information. <hostname> is the host name of the Domain Controller. For example, if the host name is win2k8ms091dc.example.entrust.com, it produces a file named win2k8ms091dc-SANInfo.txt.

The content of the file looks like this:

Hostname = win2k8ms091dc
GUID = 15f99e6f9ab8fb48a6960e12e80588f4
DNS hostname = win2k8ms091dc.example.entrust.com
Dashed GUID = 6f9ef915-b89a-48fb-a696-0e12e80588f4

3. Record the value for the DNS hostname and Dashed GUID or keep the <hostname>-SANInfo.txt available. You will require this information shortly.
Creating a Domain Controller certificate

To configure your environment for Windows Smart Card Logon, your Domain Controller requires a digital certificate. This certificate must also contain the fully qualified host name and GUID of your Domain Controller, which you obtained in “Obtaining the fully qualified host name and GUID” on page 12.

You create a certificate for your Domain Controller and configure it using Administration Services, a Web-based application.

**Note:** This guide assumes you have already created and activated an administrator certificate so you can log into Administration Services and create additional certificates. If you enrolled for Entrust Managed Services PKI, but have not yet created an administrator certificate, see the *Entrust Managed Services PKI Administrator Guide* located under the Resources tab of www.entrust.com/managed_services.

After logging in to Administration Services as described below, complete the following procedures to create a Domain Controller certificate:

- “To create a Domain Controller certificate account” on page 15
- “To set the fully qualified host name and GUID on the Domain Controller certificate” on page 18

**To log in to Administration Services**

1. Enter the Administration Services URL provided by Entrust Managed Services PKI into a browser.
   
The following page appears.

   ![Administrator Login - Entrust Desktop Security Store](image)

2. Depending on where you stored your certificate, do one of the following:
<table>
<thead>
<tr>
<th>if you stored your certificate...</th>
<th>Do this</th>
</tr>
</thead>
</table>
| In the Entrust desktop security store on your computer | 1 Click **Browse** to navigate to the location where you stored your administrator digital ID (.epf file) and click **Open**.  
The file name and path appear in the **Entrust Desktop Security Store File Name** field. Select **Remember Entrust Desktop Security Store File Name** to retain the path.  
2 Enter the password and click **Log in**. |
| within the Windows framework or on a smart card or token. | 1 Click the **Log in with my Third-Party Security Store** link.  
The **Administrator Login - Third-Party Security Store** page appears.  
**Note:** If logging in with a smart card or token, ensure it is connected to your computer.  
2 Click **Display certificate list**.  
The **Select Certificate** dialog box appears listing one or more digital certificates.  
3 Select your certificate from the list and click **OK**. |

The main Administration Services page appears.
You successfully logged in to Administration Services.

To create a Domain Controller certificate account

1. If not already logged in to Administration Services, log in now. See “To log in to Administration Services” on page 13 for more information.

2. Click Create Account under Account Tasks in the main pain or under Tasks in the left-hand menu.

The initial Create Account page appears.
3 From the User Type drop-down list, select Web Server.
4 In the Certificate Type drop-down list, select Web – Domain Controller.
5 Click Submit.
   A second Create Account page appears.
6 From the **User Information** section:
   a In the **Name** field, enter a name to identify your Domain Controller. It is recommended that you use the fully qualified domain name (FQDN) of the server.

   **Note:** You can find your fully qualified domain name in the `<hostname>-SANInfo.txt` file under the **DNS hostname** entry. You created this file in “To obtain the fully qualified host name and GUID” on page 12.

   b Optionally, enter a description of the Domain Controller certificate account in the **Description** field.

7 Leave the **Notification Email** field empty.

8 From the **Group Membership** section, select the member option. If no groups are configured, only the default group appears.

9 From the **Role** section, select **End User** from the drop-down list.

10 From the **Location** section, click **Select the searchbase** and select your company name from the drop-down list (an entry for your organization was created in the directory when you signed up for Entrust Managed Services PKI). This specifies where to add the Domain Controller account in the Administration Services LDAP directory.

11 Click **Submit**.
The Create Account - Complete page appears.

12 Securely record the reference number and authorization code. You need these activation codes later during enrollment.

13 Proceed to the below procedure: “To set the fully qualified host name and GUID on the Domain Controller certificate” on page 18.

To set the fully qualified host name and GUID on the Domain Controller certificate

1 Once you create the Domain Controller certificate account as described in “To create a Domain Controller certificate account” on page 15, click the name of your Domain Controller in the Name column on the Create Account - Complete page.
Note: If you navigated away from the Create Account - Complete page, click Edit Account under the Tasks heading in the left menu, and conduct a search for the Domain Controller account. On the Edit Account - Search Results page, click the name of your Domain Controller in the Name column.

The Account Details - <Domain Controller name> page appears, where <Domain Controller name> is the name you entered for your Domain Controller in Step 6 on page 17.

2 Scroll down to the bottom of the page and click Edit Account.
The Edit Account - Basic Information page appears.
3 Scroll down to the bottom of the page and click the **Edit Advanced Information** link.

The **Edit Account - Advanced Information** page appears.
4 In the **Subject Alternative Naming Information** section, complete the following:
   
   a In the first **Add New** field, select **Email**, and enter the following (including the quotation marks):
   ```
   "dnsName=<DNS hostname>"
   ```
   where
   
   `<fully qualified host name>` is the **DNS hostname** entry in the `<hostname>-SANInfo.txt` file you created in “To obtain the fully qualified host name and GUID” on page 12.
   
   b In the second **Add New** field, select **Email**, and enter the following:
   ```
   "msGUID=<Dashed GUID>"
   ```
   where
   
   `<Dashed GUID>` is the Dashed GUID entry in the `<hostname>-SANInfo.txt` file you created in “To obtain the fully qualified host name and GUID” on page 12.
5 Click **Submit**.

You successfully added the fully qualified host name and GUID to your Domain Controller certificate. Proceed to “Enrolling the certificate for the Domain Controller” on page 23.
Enrolling the certificate for the Domain Controller

After you create an account for the Domain Controller certificate as described in “Creating a Domain Controller certificate” on page 13, you must enroll (or activate) the certificate. This is done through a Web-based application that has the ability to store certificates in the local machine store of your Domain Controller.

Complete the following procedure to enroll the Domain Controller certificate.

To enroll the Domain Controller certificate

1. On your Domain Controller, enter the Enrollment Server for Web URL provided by Entrust Managed Services PKI into a supported Internet Explorer browser.
   
   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
   
   where <admsvc_home> is the URL of your Entrust Managed Services PKI.

   The following page appears.

   2. From the left pane under Certificates, select Computer, Device or Windows Server.

3 Enter the reference number and authorization code you received when you created the account for the Domain Controller as described in “To create a Domain Controller certificate account” on page 15 in the respective fields.

4 From the Provider type drop-down list, select RSA and Schannel.

5 From the CSP drop-down list, select Microsoft RSA SChannel Cryptographic Provider.

6 Click Submit Request.

A dialog box appears informing you that the Web site is requesting a certificate on your behalf and that you should only allow trusted Web sites to request a certificate for you.
7 Click **Yes** to request a certificate.

Another dialog box appears informing you that the Web site is adding one or more certificates to your computer.

8 Click **Yes** to add the certificate to your computer.

A success message appears. You successfully created and installed your Domain Controller certificate. The certificate is stored in the local machine certificate store.

**Computer Certificate**

You have successfully created your certificate. It has been stored in the local machine certificate store and can be used to securely identify your system to VPN gateways, and to conduct private, encrypted communication over the Internet.
Distributing the CA certificate(s) to the trusted root store of all Domain Controllers

All parties must trust the root certification authority (CA) certificate. If your certificates were issued by a subordinate CA, the subordinate (or issuing) CA certificate must be trusted as well.

To distribute the root CA certificate and, if applicable, the issuing CA certificate, to the trusted root store of all Domain Controllers, you must complete the following procedures.

• “Downloading the certification authority certificate(s)” on page 26
• “Running the Entrust installCert.bat” on page 28

This tool adds the CA(s) to the trusted roots in an Active Directory Group Policy Object and adds the CA issuing the CA certificate to the NTAuth Store in Active Directory.

Downloading the certification authority certificate(s)

Download the root certification authority (CA) certificate, and if applicable, the issuing CA certificate, to your Domain Controller through Enrollment Server for Web.

• “To download the root CA certificate through Enrollment Server for Web” on page 26
• “To download the issuing CA certificate through Enrollment Server for Web” on page 28

To download the root CA certificate through Enrollment Server for Web

1. On your Domain Controller, enter the Enrollment Server for Web URL provided by Entrust Managed Services PKI into a supported Internet Explorer browser.

   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start

   where <admsvc_home> is the URL of your Entrust Managed Services PKI.

   The following page appears.
2. From the left pane under CA Certificates, click Install. The File Download dialog box appears.

3. Click Save and complete the following:
   - If the root CA and issuing CA are one and the same (the root CA is the issuer of your certificates), save the file as caCert.crt.
   - If the root CA and issuing CA are separate CAs, save the root CA certificate as rootCACert.crt.
• Save the root CA certificate to the same folder as the Smart Card Logon tools you downloaded in Step 2 on page 10.

4 Complete one of the following based on your requirements:

• If the root CA is not the issuing CA, you must download the issuing CA certificate. See the below procedure: “To download the issuing CA certificate through Enrollment Server for Web” on page 28.

• If the root CA is the issuing CA, proceed to “Running the Entrust installCert.bat” on page 28.

**To download the issuing CA certificate through Enrollment Server for Web**

1 Still in Enrollment Server for Web, click Display list under the Cross-certificate heading in the left pane.

The Cross-certificate(s) (PEM encoding) page appears displaying the cross-certificates.

2 Copy the entire issuing CA certificate, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines, and paste it into a text editor.

3 Save the file as issuerCACert.cer to the same location on your Domain Controller where you saved the Smart Card Logon tools in Step 2 on page 10 (also the location you just saved your root CA certificate in the preceding procedure).

**Running the Entrust installCert.bat**

Once you have downloaded the CA certificate(s) on your Domain Controller as described in “Downloading the certification authority certificate(s)” on page 26, run the installCert.bat you downloaded earlier. This adds the CA certificate(s) to the trusted roots in an Active Directory Group Policy Object and adds the CA issuing the CA certificate to the NTAuth Store in Active Directory.
To run the installCert.bat

1. Navigate to the folder on your Domain Controller where you saved the Smart Card Logon tools as described in Step 2 on page 10.

2. Double-click installCerts.bat to run the tool. This tool installs the certification authority (CA) certificate(s) as a trust anchor for Smart Card Logon.
   You successfully installed the CA certificate(s).
Configuring users for Windows Smart Card Logon

Windows Smart Card Logon users must have the userPrincipleName (UPN) value added to their certificate and the correct certificate type set. Both the UPN and certificate type are configured through the user's account in Administration Services.

Complete one of the following procedures depending on whether you are creating a new Windows Smart Card Logon user (a single user or multiple users in bulk), or configuring an existing user for Windows Smart Card Logon:

- “To create a new Windows Smart Card Logon user” on page 30

Note: If your administrator account role includes the “Create accounts in batch from a file” permission, the Create Accounts from File option is available. This option allows you to use an input file to submit multiple create account operations in one simple procedure. For more information on creating user accounts in batch, see the Entrust Authority Administration Services Administration Guide for details.

- “To configure an existing user for Windows Smart Card Logon” on page 38

To create a new Windows Smart Card Logon user

1. Log in to Administrative Services. See “To log in to Administration Services” on page 13 for more information.

2. Click Create Account under Account Tasks in the main pain or under Tasks in the left-hand menu.

The initial Create Account page appears.
3 From the **User Type** drop-down list, select **Person**.

4 From the **Certificate Type** drop-down list, select **Enterprise - Smart Card Logon for MS Security Framework Users**.

5 Click **Submit**.

   A second **Create Account** page appears.
From the **User Information** section:

a. Enter the end user’s first name and last name in the **First Name** and **Last Name** fields respectively.

b. Optionally, fill in the **Serial Number**, **Email**, and **Comment** fields.

Optionally, from the **Notification Email** section, enter an email address if you want the user to receive account status notifications, which include emails that:

- indicate account registration
- provide the reference number the user needs to enroll for their certificate. (You would still need to provide the user with the matching authentication code)

If the email address is the same as the one entered in the **User Information** section, select **Same as above email address**.

From the **Group Membership** section, select the member option. If no groups are configured, only the default group appears.

From the **Role** section, select **End User** from the drop-down list.

From the **Location** section, click **Select the searchbase** and select your company name from the drop-down list (an entry for your company was created in the
directory when you signed up for Entrust Managed Services PKI). This specifies where to add the user in the Administration Services LDAP directory.

11 Click **Submit**.

The **Create Account – Complete** page appears.

<table>
<thead>
<tr>
<th>Name</th>
<th>Group</th>
<th>Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartCardLogon User</td>
<td>default</td>
<td>End User</td>
<td>New</td>
</tr>
</tbody>
</table>

**Activation Codes**

- **Name:**
  - cn=SmartCardLogon User,o=entrust,c=ca
- **Reference Number:** 23605717
- **Authorization Code:** FXE8-BL3R-SAXO
- **Codes were created on:** Friday, June 19, 2009 10:37:44 AM
- **Codes will expire on:** Friday, July 03, 2009 10:37:44 AM

12 Securely record the reference number and authorization code. You need to provide these activation codes to the Smart Card Logon user so they can enroll their certificate.

13 Click the name of your Smart Card Logon user in the **Name** column on the **Create Account - Complete** page.

The **Account Details - <user name>** page appears, where `<user name>` is the name you entered for your Domain Controller in **Step 6**.
Scroll down to the bottom of the page and click **Edit Account**.

The **Edit Account - Basic Information** page appears.
15 Scroll down to the bottom of the page and click the Edit Advanced Information link.

The Edit Account - Advanced Information page appears.
In the Subject Alternative Naming Information section, complete the following:

a. In the first Add New field, select UPN.

b. In the same Add New field, enter the user’s userPrincipalName (UPN). The UPN is defined when you add a user to the directory and its syntax looks similar to an email address:

```
Subject Alternative Naming Information
Add New: Email  UPN
SmartCardLogon@example.entrust.com
```

For example, in Active Directory, you can find the UPN in the `<username>` Properties dialog box, under the Account tab.
17 Click **Submit**.

A success message appears. You successfully created a Smart Card Logon user.

18 Provide the end-user with the details required to enroll their certificate. This includes:

- The Administration Services URL for end users (User Registration Service application) provided to you by Entrust.
- The reference number and authorization code obtained in Step 12.
- The end-user guide for certificate enrollment to walk the user through the procedure: *Getting an end-user certificate using Entrust Authority*
To configure an existing user for Windows Smart Card Logon

1. Log in to Administrative Services. See “To log in to Administration Services” on page 13 for more information.

2. From the left-hand menu under Search, click Search Accounts to search for the user you want to configure for Windows Smart Card Logon.

The Search Accounts - Search page appears.

3. Fill out any account criteria needed to find the user and click Submit.

Note: You can leave the form blank and click Submit to return all results.

The Search Accounts - Search Results page appears.
4 Complete Step 13 on page 33 to Step 16 on page 36.
5 Scroll down to the Certificate Type section and select Enterprise - Smart Card Logon for MS Security Framework Users from the drop-down list.
6 Click Submit.
   The Edit Account - Complete page appears. Since you modified the user certificate for Smart Card Logon, you must now initiate a key recovery. See the below procedure: “To initiate a key recovery” on page 39.

To initiate a key recovery
1 If you are not logged into Administration Services, log in now. See “To log in to Administration Services” on page 13 for more information.
2 From the left menu under Tasks, click Reset Account.
   The Reset Account - Search page appears.
3 Fill out any account criteria needed to find the user and click **Submit**.

**Note:** You can leave the form blank and click **Submit** to return all results.

The **Reset Account - Search Results** page appears.
Based on your search results, select either the radio button or check box to the left of the user name, and click one of the following based on the current account status:

- Select **Reauthorize** if the user account exists, but the user has not yet created their certificate.
- Select **Reset** if the user account is active (the user has created a certificate already).

**Note:** Depending on your search results and the status of the user's account, you may not receive both of these options.

The **Reset Account - Complete page** appears.
5 Securely record the reference number and authorization code. You need to provide these activation codes to the Smart Card Logon user so they can recover their certificate.

6 Provide the end-user with the details required to recover their certificate. This includes:
- The Administration Services URL for end users (User Registration Service application) provided to you by Entrust.
- The reference number and authorization code obtained in Step 4.
- The end-user guide for certificate enrollment to walk the user through a key recovery: Getting an end-user certificate using Entrust Authority Administration Services. This guide is available under the Resources tab at www.entrust.com/managed_services.
Smart Card Logon in Vista

Windows Vista is less restrictive than earlier versions of Windows in what it expects from smart cards. This means that, if your Smart Card Logon configuration worked on Windows XP, it should work on Vista.

The operations performed in Smart Card Logon in Vista are very similar to the ones performed in previous versions of Windows: except, in early versions of Windows the smart card operations used a call back into winlogon. Now, with the improved session handling in the Smart Card Resource Manager, CSP contexts are used directly in the Local Security Authority (LSA).


Before Windows Vista:

- A smart card could support only one certificate for logon.
- Only one container on the smart card could be marked default.
- Changing the PIN and unblocking a smart card were not natively supported or integrated. A user had to log on first with a standard user name and password to perform these tasks.

With Windows Vista:

- Logon is no longer triggered to smart card insertion. Users press Ctrl+Alt+Del to start the logon process.
- Depending on Group Policy, valid certificates are enumerated and displayed from all smart cards and presented to the user.
- Depending on Group Policy, keys are no longer restricted to being in the default container and certificates in different smart cards can be chosen.
- The CSP is opened in the both the logonUI.exe and lsass.exe. The CSP is never loaded into the winlogon process.

For more information, see the following sites:

Troubleshooting

- If a missing or wrong EKU is in the Domain Controller certificate or if the Domain Controller certificate is missing, end-users see the following error when attempting to log on to Windows using Windows Smart Card Logon:

  The System could not log you on. The server authenticating you reported an error (0xC00000BB). You can find further details in the Event Log. Please report this error to the System Administrator.

- If the CA that issued the Smart Card Logon certificate or the Domain Controller certificates is not properly added to the NTAuth store, the smart card logon process does not work. End-users see the following error:

  Unable to verify the credentials.

  Refer to “Distributing the CA certificate(s) to the trusted root store of all Domain Controllers” on page 26 for information on how to add the CA certificate to the NTAuth store.