Novell

Universal SmartCard Login Method

www.novell.com

QUICK START

Installing and Using the Universal SmartCard Method

The Universal SmartCard method provides user identification and authentication using a SmartCard and reader connected to a network.

Universal SmartCard User Identification and Authentication Options

The Universal SmartCard method provides three ways of identifying and authenticating users to the network:

- Identity and authentication, where the SmartCard provides both identification and authentication of the user to the network
- Identity only, where the SmartCard is used only to identify, with the user subsequently authenticating with a password or other similar means.
- Authenticate only, where user provides identity and the SmartCard authenticates the user to the network.

The first two ways require the method and the Universal SmartCard NMAS™ login ID snap-in; the third requires only the Universal SmartCard Login method.

Installing and Configuring the Login Method for Universal SmartCard

Information for installing and configuring the login method is provided here. For additional information, including how to create and authorize login sequences, see the NMAS Administration Guide at the Novell Documentation Web site (http://www.novell.com/documentation/lg/nmas20/index.html).

You must meet the following prerequisites before installing:

- ❑ Windows 98 or later on the workstation
- ❑ NMAS 2.02 or later on the server
- ❑ NMAS 2.1 or later client on the workstation if you are using the ID snap-ins

Novell®

- ❑ Universal SmartCard readers and vendor software on the workstation

Overview of SmartCard Login Method Installation

You must complete the following steps to make the Universal SmartCard login method available for use:

1. Installing the login method on the Server.
2. Creating the user certificate.
3. Authorizing login sequences for users.

   (This step is not necessary if installing only the ID snap-in.)
4. Set up any required workstation hardware.
5. Install the SmartCard Client Module on each workstation.

Installing the Login Method for Universal SmartCard

Run ConsoleOne® from a Windows* client workstation by using the ConsoleOne executable file located on the server at *server:*sys\public\mgmt\consoleone\1.2\consoleone.exe.

To install the login method on the server, you must perform the following proceedures:

- Install the SmartCard Method in eDirectory
- Create a Trusted Root Container
- Export a Trusted Root Certificate
- Install the Trusted Root Certificate into the Trusted Root Container
- Configure the Universal SmartCard Method to Use the Trusted Root Container

Install the SmartCard Method in eDirectory

1. In ConsoleOne, expand the Security container.
2. Right-click the Authorized Login Methods container.
3. Click New > Object.
4. Select SAS:NMAS Login Method.
5. Specify the login method configuration file, then click Next.

   The configuration file is located in the Universal SmartCard login method folder on the NMAS CD and is usually named config.txt.
6. (Conditional) If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne login method snap-ins.

Create a Trusted Root Container

1. Right-click the Security container.
2. Click New > Object.
3. Select the NDSPKI:Trusted Root Class, then click OK.
4. Name the new Trusted Root Container.

Export a Trusted Root Certificate

1. Obtain a self-signed certificate from the Certificate Authority.

   There are two sources for certificates: those created by Novell on the server and those delivered by a third-party certificate server. If you have a third-party certificate, skip to Install the Trusted Root Certificate into the Trusted Root Container; otherwise continue. (Third-part certificates must be in either DER or Base 64 format.)
2. Select the Security container.
3. Right-click the CA object, then select Properties.
4. Click the Certificates tab, then select the Self-signed Certificate.
5. Click Export to start the certificate export wizard.
6. Verify that the No button is selected (default), then click Next > Next.
7. Accept the defaults, then click Finish.

Install the Trusted Root Certificate into the Trusted Root Container

1. Right-click the Trusted Root container object, click New > Object, then select the NDSPKI:Trusted Root Object Class object.
2. Name the new Trusted Root Object, then click OK.
3. Click the Read from File button.
4. Scroll to select the Novell CA certificate or third-party certificate, then click Open > Finish.

Configure the Universal SmartCard Method to Use the Trusted Root Container

1. Select the Authorized Login Methods container, then select the Universal SmartCard Method object.
2. Right-click the SmartCard authentication object, then click Properties.
3. Select the Certificate tab, then click ADD.
4. Navigate to the Security container, then select the NDSPKI:Trusted Root container you created earlier.
5. Click OK > OK to finish configuring the server certificate.

Creating the User Certificate

You need a user certificate for each user loaded in the user's SmartCard, and the user's certificate subject name in eDirectory. The certificate on the SmartCard must also contain the user's private key. This can be done with either Novell created user certificates or third-party user certificates.

To create the user certificate with private key for use with the SmartCard method you will:

- Create a user certificate.

  You can use a third-party user certificate if it is provided.
- Configure the Certificate Subject Name from a user certificate
- Export the user certificate and private key

Create a User Certificate

If you want to use a third-party certificate, skip to "Use a Third-party Certificate for a User" on page 5. Otherwise, you must create a user certificate for each user as follows:

1. In ConsoleOne, double-click a User object.
2. Click Security > Certificate > Create.
3. Select the Custom radio button.
4. Create a Nickname for the certificate.
5. Click Next >Next.
6. Specify the key size.

   Most cards support up to 1024 bits (default is 2048). Check with your SmartCard vendor.
7. Accept the vendor values in the other fields, then click Next > Next.

   Normally you would accept the defaul values displayed.
8. Click Yes to clear the e-mail address warning message.
9. Click Finish to create the certificate.

   After the certificate is created, it appears in the Properties window listing.

Configure the User Certificate Subject Name from a User Certificate

1. In the User Properties window, click Details.
2. Click the X.509 tab, copy the certificate subject name to the Windows clipboard, then Close the dialog box.
3. Click Security Tab > Certificate Subject Names > Add.

4 Paste in the certificate subject name from the clipboard.

5 Click Apply > Close.

Export the User Certificate and Private Key

1 Shut down ConsoleOne, log in to NDS as the user you have just created a certificate for, then reopen ConsoleOne.

2 In ConsoleOne, right-click the User, then click Properties.

3 Click Security > Certificates.

4 Select the certificate, then click Export.

5 Verify that Yes button to Export with Private Key is selected, then click Next.

6 Type the password to encrypt the private key that will be placed on the SmartCard.

7 Accept or select a filename and destination for the file containing the user certificate and private key, then click Next > Finish to export it.

8 Close the Properties window and exit ConsoleOne.

Use a Third-party Certificate for a User

1 Create the user certificate using the vendor software.

2 Determine the subject name of the user certificate using the vendor software.

3 Log in to ConsoleOne as Admin.

4 Right-click the User object, then click Properties.

5 Click Security > Certificate Subject Names > Add.

6 Type the certificate subject name from step 2.

7 Click Apply > Close.

Authorizing the Login Sequence for Users

User objects can be configured to use one or more of the available login sequences defined in eDirectory. Users with no login restrictions are already authorized for the Universal SmartCard login sequence. If you have configured login sequence restrictions for your users, you will need to authorize the Universal SmartCard sequence for those users. To do so, complete the following authorization steps:

1 Log in to ConsoleOne as admin.

2 Right-click the User object, then click Properties.

3 On the Security tab, select Login Sequences.

4 Move the Universal SmarCard authorization sequence from the Available Sequences list to the Authorized Sequences list.

5 Click Apply > Close.

6 (Optional) Repeat the above steps for additional users.

7 Exit ConsoleOne.

Setting Up the Workstation Hardware

The reader and its software are provided by the reader manufacturer, and must be installed on the client workstation according to manufacturer instructions before installing the login method.

Installing the SmartCard Client Module on Each Workstation

The NMAS Client on the workstation must be updated to version 2.02 or later unless the ID snap-in will be used; in that case NMAS should be updated to version 2.1 or later. The SmartCard client module must be installed on each workstation that will use the SmartCard login method.

To install the client module:

1 To update the NMAS client on the workstation, run nmasinstall.exe (located at the root directory of the NMAS CD) on each workstation that will use the Universal SmartCard login method.

2 Select the NMAS Client, then click OK. (Requires NICI 2.4.1 Client)

3 Accept the agreement.

4 From the Select NMAS Clent Login panel, select Universal SmartCard and then click Next.

5 From the Select NMAS Post-Login Methods panel, do not select any method, click Next.

The wizard completes the NMAS upgrade and method selection. The SmartCard client module can be configured during setup to initiate a user login automatically with the insertion of the SmartCard in the reader, or to follow a manual login with the user presenting the SmartCard when prompted in the sequence.

6 At the PKCS#11 Library Selection panel, select the SmartCard vendor you are using from the list, or select User Specified. Then click Next.

(If you select User Specified you will need to provide the name of the vendor provided PKCS#11 library .DLL file.)

7 (Optionl) On the Select Options panel, you can choose to use the card reader to obtain the username of the SmartCard holder. NMAS restrictions allow only one method to automatically obtain the username at the workstation being configured.

If you select the option, the ID-snap-in will be configured to allow the SmartCard to provide both Identity and Authentication to the network for the user. To select, check the option and click Next. Otherwise, proceed to step 8.

7a Fill in the information if you want to specify which tree, server, and sequence are used for authentication. Otherwise, click Next

7b If the sequence field is left blank on the previous screen, the Sequence Options panel appears. In this case, select Use the Users Default Sequence if you have previously defined a sequence for your users. Otherwise, select the sequence last used on that workstation option, then click Next.

7c On the LDAP Servers panel, specify the name or IP Address of the LDAP server and any alternates, then click Next, > Next.

8 Complete the wizard to finish the installation.

9 (Conditional) If you have Secure Workstation installed, you will be required to restart the Secure Workstation service.

Preparing the SmartCard for the User

To initialize a SmartCard for use with this method, the SmartCard must have at least one private key and a user certificate corresponding to that private key. The private key must be enabled for signature generation. This is done preferably by using the vendor-supplied utility, or it can be done with the Novell supplied initsc.exe utility to upload the contents of a PKCS#12 (PFX) file into the Smart Card.

For example, if the name of the PFX file is MyKeys.pfx, its password is "Novell", and the SmartCard's PIN is 1234, then execute:

```
initsc -p 1234 -s Novell -f MyKeys.pfx -m pk2priv.dll
```

Note that “-m pk2priv.dll” is the name of the PKCS#11 provider library for GemSAFE. Other providers might have different names. In this example, it is a GemSAFE SmartCard and PKCS#11 provider. This utility does not accept Unicode* passwords and PINs, and it is tested with the GemSAFE SmartCard and library. The use of this library with other vendors might or might not work. Use it at your own risk.