Novell

Universal SmartCard Login Method

3.x

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 allows 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 to only 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 means 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/nmas30/index.html).

You must meet the following prerequisites before installing:

- ❑ NMAS 2.3.*x* or later on the server
- ❑ NMAS 2.7 or later client on the workstation (ships with Novell Client for Windows version 4.9)

Novell®

- ❑ Universal SmartCard readers and vendor software on the workstation

Overview of SmartCard Login Method installation

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

1. Install the login method on the Server.
2. Create the user certificate.
3. Authorize login sequences for users.
4. Set up any required workstation hardware.
5. Update the NMAS client on each workstation and install the SmartCard Client Module on Each Workstation.

NOTE: Step 3 is not necessary when installing only the ID snap-in.

Installing the Login Method for Universal SmartCard

Run ConsoleOne® from a Windows* client workstation by using the ConsoleOne executable located on the server at *server:SYS\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE*.

To install the login method on the server, you will perform the following processes:

- 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 to install the Login Server Method.
3. Select 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. 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. Select 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: created by Novell PKI on the server, or delivered by a third-party certificate server. If you have a third-party certificate, proceed to Install the Trusted Root Certificate into the Trusted Root Container, otherwise continue. (Third-part certificates must be in either a DER or Base 64 format.)
2. Select the Security container.
3. Right-click the CA object, then select Properties.
4. Select the Certificates tab, then the Self-signed Certificate.
5. Click the Export button to start the certificate export wizard.
6. Click the No button, then Next, then Next again.
7. Accept the defaults, then Finish the wizard.

Install the Trusted Root Certificate into the Trusted Root Container

1. Right-click the Security container > New > Object, Select NDSPKI:Trusted Root Object Class object.
2. Name the new Trusted Root Object, then click OK.
3. Enter a name for the new CA certificate.
4. Click the Read from File button.
5. Scroll to select the Novell CA certificate, or third-party certificate, click Open, then click 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 select Properties.
3. Select the Certificate tab, then click the ADD button.
4. Navigate to the Security container, then select the NDSPKI:Trusted Root container you created earlier.

5 Click OK, then click OK again to finish configuring the server certificate.

Creating the User Certificate

You need a PKI certificate for each user 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 certificates or third-party certificates.

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

- Create a Novell PKI Certificate for a user.

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

Creating a Novell PKI Certificate for a User

1 In ConsoleOne, double-click a User object.

2 Select the Security > Certificate.

3 Click the Create button.

4 Select the Custom radio button.

5 Create a Nickname for the certificate

6 Click Next, then Next again.

7 Specify the key size.

  Most cards support up to 1024 bits. Check with your SmartCard vendor.

8 Accept the vendor values on the other fields, then click Next.

9 Click Next again.

  (Normally you would accept the defaul values displayed.)

10 Click Yes to clear the e-mail address warning message.

11 Click Finish to create the certificate.

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

Configuring the Certificate Subject Name from a Novell Certificate

1 In the Propeties window, Click Details.

2 Select the X.509 tab, then copy the Subject Name to the Windows clipboard, then Close the dialog box.

3 Select Security Tab > Certificate Subject Names.

4 Click the Add button, then paste in the certificate subject name from the clipboard.

5 Click Apply, then Close.

Exporting the User Certificate and Private Key

1 Shut down ConsoleOne, login to NDS as the User you have just created a certificate for, then reopen ConsoleOne.

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

3 Select Security > Certificates.

4 Highlight the certificate, then click the Export button.

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

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

7 Select a filename and destination for the file containing the user certificate and private key, click Next, then Finish to export.

8 Close the Properties window and exit ConsoleOne.

Using a Third-party Certificate for a User

1 Create the PKI Certificate using the vendor software.

2 Determine the Subject Name of the user certificate using the vendor software.

3 Login as Admin to ConsoleOne.

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

5 Select Security Tab > Certificate Subject Names.

6 Click the Add button, then enter the certificate Subject Name from step 2.

7 Click Apply, then 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, perform the following authorization steps:

1 Login to ConsoleOne as admin.

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

3 On the Security tab, select Login Sequences.

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

5 Click Apply, then Close.

6 Repeat as needed 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 must be updated to level 2.7 or higher. The SmartCard client module must be installed on each workstation that will use the SmartCard login method.

Updating the NMAS Client and Installing The SmartCard Client Module

To install the client module:

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

2 Select the NMAS Client, then click OK.

3 Accept the agreement.

4 From the Select NMAS Clent Login panel, select Universal SmartCard, 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. (If you select User Specified you will need to provide the name of the vendor provided PKCS#11 library .DLL file.) then click Next.

7 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.)

8 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. Check the option and click Next. Otherwise, proceed to step 9.

8a Fill in the information if you want to specify which Tree, Server, and Sequence are used for authentication, otherwise, click Next

8b At the Sequence Options panel, select the 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.

8c On the LDAP Servers panel, supply the name or IP Address of the LDAP server and any alternates, click Next, then click Next again.

9 Complete the wizard to finish the installation.

10 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 also 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 may 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 is tested with GemSAFE SmartCard and library. The use of this library with other vendors may or may not work. Use it at your own risk.