

NMAS Login Method and Login ID Snap-In for pcProx

June, 2009

Novell®

Installing and Using pcProx

The Novell Modular Authentication Services (NMAS) Login Method and Login ID snap-in for pcProx provides to you two ways to employ a proximity card as a means of authentication to the network. It enables you to set up a pcProx card ID to act like a conventional password to authenticate the user to the network. This method is similar to the login methods provided for use with NMAS.

IMPORTANT: pcProx should not be the only factor used for authentication, because this might pose security issues. It should be used with a second factor, such as a biometric device, a smart card, or a password.

The NMAS login ID snap-in enables the organizations to utilize their proximity cards to quickly and easily identify users. For example, instead of requiring user to specify their user IDs when they authenticate, you can require users to present their proximity cards for identification along with another form of authentication, such as a password or a biometric device to authenticate the users.

This login method supports two types of proximity cards:

- ♦ HID Cards
- ♦ AIR Cards

Software Requirements

Ensure that you have met the following requirements before installing the pcProx:

Client

One of the following operating systems:

- ♦ Microsoft* Windows* Vista*
- ♦ Microsoft Windows XP
- ♦ Microsoft Windows 2000
- ♦ NMAS Client 3.4 or later for Microsoft Windows 2000 or XP
- ♦ NMAS Client 3.4 for Microsoft Windows Vista
- ♦ The USB readers must have firmware 3.20 or above for standard cards (26-bit) and 6.30 or above for cards with the ID of length greater than 26-bits.

Server

Have the following software on the workstations that uses pcProx:

- ♦ Novell eDirectory™ 8.8.5, 8.8.4, or 8.8.3.
- ♦ NMAS Server 2.3.9

Novell iManager

- ♦ Novell® iManager 2.7.2 and 2.7.1

Mandatory Tasks

You must complete the following tasks to make the login method available for use:

1. "Setting Up the Hardware" on page 1
2. "Installing the Login Server Method for pcProx in eDirectory" on page 1
3. "Creating and Authorizing Login Sequences" on page 2
4. "Installing the Login Client Method for pcProx" on page 2
5. "Installing the iManager Plug-In for pcProx" on page 2
6. "Configuring the Login Method" on page 2

NOTE: Task 3 is not necessary for the ID snap-in.

SETTING UP THE HARDWARE

The login method for pcProx requires that each workstation that uses the method must have a pcProx card reader.

INSTALLING THE LOGIN SERVER METHOD FOR PCPROX IN EDIRECTORY

- 1 Launch and access iManager.

For detailed information on accessing iManager, see the [Novell Documentation Web site](http://www.novell.com/documentation/imanager20/imanager20/data/agrxn3.html). (<http://www.novell.com/documentation/imanager20/imanager20/data/agrxn3.html>)

- 2 Specify the username, password, and the eDirectory tree name, then login to eDirectory.

You can substitute the IP address of an eDirectory server for the tree name.

To have full access to all Novell iManager features, you must log in as a user with admin-equivalent rights to the tree.

- 3 Select *NMAS > NMAS Login Methods > New*. The New Login Method page opens.
- 4 Browse and locate the `pcprox.zip` found in `\Nmas\NmasMethods\Novell\pcProx\pcProx.zip` on the Novell SecureLogin installer package.

NOTE: The installation of NMAS Login Server Method for pcProx:

- ◆ Creates a login sequence called NMAS Proximity Card.
- ◆ Installs the iManager plug-in for pcProx.

CREATING AND AUTHORIZING LOGIN SEQUENCES

For information on 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). (<http://www.novell.com/documentation/lg/nmas20/index.html>)

INSTALLING THE LOGIN CLIENT METHOD FOR PCPROX

The pcProx client must be installed on each workstation that uses the pcprox login method.

To install the login client method:

1. Update the NMAS Client
2. Install the Login Client Method

Updating the NMAS Client

To update the NMAS Client:

- 1 Obtain and run the executable file for the operating system you are using.
 - ◆ For updating on Microsoft Windows Vista, NMAS is available in `\Nmas\NmasClient\Vista-x86\nmasclient_setup_v32.exe`, which is found on the Novell SecureLogin 6.1 installer package.
 - ◆ For updating on Microsoft Windows XP, 2000, and 2003, NMAS is available in `\Nmas\NmasClient\win32\nmasclient_setup.exe`, which is found on the Novell SecureLogin 6.1 installer package.
- 2 Follow the on-screen prompts to install the software.

Installing the Login Client Method

- 1 Run the `pcprox.exe`, which is available at `Nmas\NmasMethods\Novell\pcProx\client` on your Novell SecureLogin 6.1 installer package.
- 2 Follow the onscreen prompts to complete the installation.

INSTALLING THE IMANAGER PLUG-IN FOR PCPROX

- 1 Launch and access iManager.

For detailed information on accessing iManager, see the [Novell Documentation Web site](http://www.novell.com/documentation/imanager27/imanager_admin_27/index.html?page=/documentation/imanager27/imanager_admin_27/data/bsxrjzp.html). (http://www.novell.com/documentation/imanager27/imanager_admin_27/index.html?page=/documentation/imanager27/imanager_admin_27/data/bsxrjzp.html)

- 2 Specify the username, password, and the eDirectory tree name, then login to eDirectory.

You can substitute the IP address of an eDirectory server for the tree name.

To have full access to all Novell iManager features, you must log in as a user with admin-equivalent rights to the tree.

- 3 Click the *Configure* tab.
- 4 Click *Plug-in Installation*, then select *Available Novell Plug-in Modules*.
- 5 Click *Add*. The Copy Plug-in File page is displayed.
- 6 Click *Browse* and locate the `pcprox.npm` file, which is available in `iManager\Snapin` folder of the Novell SecureLogin 6.1 installer package.
- 7 Select the pcprox plug-in you want to install and click *Install*. You see a confirmation message after the plug-in is successfully installed.
- 8 Click *Close*.
- 9 Restart Tomcat after the installation is complete. This might take several minutes.

For information on installation and Role Based Services (RBS) configuration, visit the [Novell Documentation Web page](http://www.novell.com/documentation/imanager27/index.html) (<http://www.novell.com/documentation/imanager27/index.html>)

NOTE: Scanning the pcProx card ID and associating it with the users for either identification or authentication works only with the iManager server running on Windows.

For enrolling the pcProx ID for the users, you can also use mobile iManager 2.6

CONFIGURING THE LOGIN METHOD

After you have successfully installed the login method for pcProx, you can manage it through iManager.

Manually Setting a pcProx Card for User

- 1 Launch and access iManager.

For detailed information on accessing iManager, see the [Novell Documentation Web site](http://www.novell.com/documentation/imanager20/imanager20/data/agrxn3.html). (<http://www.novell.com/documentation/imanager20/imanager20/data/agrxn3.html>)

- 2 Specify the username, password, and the eDirectory tree name, then login to eDirectory.

- 3 You can substitute the IP address of an eDirectory server for the tree name.

To have full access to all Novell iManager features, you must log in as a user with admin-equivalent rights to the tree.

- 4 From the left pane, select *NMAS > NMAS Users*.
- 5 In the *Username* field, specify the object name, then click *OK*.
- 6 Select the *PcProx* tab, then select *PcProx Authentication*.
- 7 From the task options, select *Set Card ID*.

If you want to scan the pcProx card ID, place the card on the card reader, then click *Scan ID*.

After the scanning is complete, the card's ID appears in the *Scan ID* field.

You can also manually specify the card ID number in the *Card ID* field.

- 8 Click *OK* or *Apply* to save your settings.

Removing a pcProx Card from a User

- 1 Log in to iManager.
- 2 From the left pane, select *NMAS > NMAS Users*.
- 3 In the *Username* field specify the object name, then click *OK*.
- 4 Select the *PcProx* tab, then select *PcProx Authentication*.
- 5 From the task options, select *Remove Card ID*.
- 6 Click *OK* or *Apply* to save the changes.

The selected card ID is removed.

Allowing a User to Self-Enroll the Card ID

- 1 Log in to iManager.
- 2 On the left pane, select *Directory Administration > Modify Object*.
- 3 Click the  icon adjacent to the Object name field.
- 4 Under the *Contents*, select *Security > Authorized Login Methods > NMAS Proximity Card*.
- 5 Click *OK*.
- 6 Click *PcProx* tab, then select *Enable Self Enrollment*.
- 7 Click *OK* or *Apply* to save the changes.

Installing and Configuring the Login ID Snap-In for pcProx

After you have installed NMAS and the login method software, you need to install and configure the login ID snap-in.

SOFTWARE REQUIREMENTS

Ensure that you have met the following requirements before installing the pcProx:

Client

One of the following operating systems:

- ◆ Microsoft Windows Vista
- ◆ Microsoft Windows XP
- ◆ Microsoft Windows 2000
- ◆ NMAS Client 3.4 or later for Microsoft Windows 2000 or XP
- ◆ NMAS Client 3.4 for Microsoft Windows Vista
- ◆ The USB readers must have firmware 3.20 or above for standard cards (26-bit) and 6.30 or above for cards with the ID of length greater than 26-bits.

Server

Have the following software on the workstations that uses pcProx:

- ◆ Novell eDirectory 8.8.3, 8.8.4, and 8.8.5
- ◆ NMAS Server 2.3.9

Novell iManager

- ◆ Novell iManager 2.7.1 and 2.7.2

MANDATORY TASKS

Ensure that you complete the following tasks before making the login ID snap-in available for use:

1. [“Setting Up the Hardware” on page 3](#)
2. [“Installing the Login ID Snap-In for pcProx” on page 3](#)
3. [“Adding a pcProx Card as a Login ID” on page 4](#)

Setting Up the Hardware

- ◆ The login ID plug-in for pcProx requires that the workstation that uses the method must have a pcProx card reader.

NOTE: Specify the COM port number or USB during the method installation.

Installing the Login ID Snap-In for pcProx

- 1 Run `pcprox.exe`, which is available at `Nmas\NmasMethods\Novell\pcProx\client` on your Novell SecureLogin installer package.
- 2 Follow the onscreen prompts to complete the installation.

IMPORTANT: When you have to select the card reader options, you must select *Use the card reader* to obtain the username for login.

Adding a pcProx Card as a Login ID

You can add a pcProx card to be used as a login ID in two ways:

- ♦ Scanning the pcProx card
- ♦ Specifying the pcProx card ID manually.

To add the pcProx card ID by scanning the card:

- 1 Log in to iManager.
- 2 From the left pane, select *NMAS > NMAS Users*.
- 3 In the *Username* field specify the object name, then click *OK*.
- 4 Select the *PcProx* tab, then select *PcProx Identification*.
- 5 Place the card on the card reader and click *Scan & Add ID*. After the card is scanned, the card's ID appears in the *Card ID* field.
- 6 Click *Apply* to save the changes.
- 7 Click *OK* to exit.

To add the pcProx card manually:

- 1 Log in to iManager.
- 2 From the left pane, select *NMAS > NMAS Users*.
- 3 In the *Username* field specify the object name, then click *OK*.
- 4 Select the *PcProx* tab, then select *PcProx Identification*.
- 5 In the *Card ID* field, specify the pcProx card ID in hexadecimal format.
- 6 Click *Add ID* to add the ID.
- 7 Click *Apply* to save.
- 8 Click *OK* to exit.

Preventing the Login ID Plug-In from Executing

A user can prevent the ID plug-in from executing by holding the Ctrl key when the login dialog box is displayed. This is a useful feature for users who need to occasionally change their login information, for example, if a user needs to log in to a different tree or server, or use a different NMAS sequence.

Deleting a pcProx Card Used As A Login ID

- 1 Log in to iManager.
- 2 From the left pane, select *NMAS > NMAS Users*.
- 3 In the *Username* field specify the object name, then click *OK*.

- 4 Select the *PcProx* tab, then select *PcProx Identification*.
- 5 Select the ID to be removed from the pcProx ID list.
- 6 Select *Delete*.
- 7 Click *OK* or *Apply* to save the changes.

Using the pcProx ID for Authentication and User Identification and Secure Workstation

The assignment of the pcProx ID for authentication and user identification must be made in two different places in iManager. To assign the pcProx ID for authentication, use the *PcProx Authentication* tab. To assign the pcProx ID for identification, use the *PcProx Identification* tab.

To use the card for identification, the assignment must be made public in the directory because no user is logged in. If you choose to use the pcProx method for authentication, we recommend that a second factor of authentication also be used.

You can also set up pcProx as an event that is monitored by Secure Workstation. When a user logs in with pcProx and a proximity card, Secure Workstation will monitor that card as an event to watch. If the user logs in using some other means of authentication, but Secure Workstation knows there is a card associated with that user, Secure Workstation will prompt the user to identify their card number.

pcProx and Citrix: When using pcProx with Citrix, you can set up a virtual channel between the Citrix box and the ICA box with a card reader. This will work properly as long as the pcProx client module is installed on both the ICA box and the Citrix box.

Registry Keys and Values for the pcProx Method

Key: HKLM\SOFTWARE\Novell\NMAS\MethodData\pcProx

Value: comid

Type: DWORD

Data: The com port that the reader is attached to. A value of -1 (0xffffffff) signifies USB.

Value: retries

Type: DWORD

Data: Specifies the number of consecutive failures that the reader must get before reporting a Device Removal Event to Secure Workstation. This is most useful when the AIR ID readers are used in areas with considerable interference.

Registry Keys and Values for the pcProx Snap-In

Key: HKLM\SOFTWARE\Novell\NMA\pcProx\ID

Value: Sequence

Type: String

Data: The name of the sequence to be used when a user ID is obtained from the device. If this value exists but has no data, then the user's default sequence is used.

Value: Tree

Type: String

Data: The tree name to be used when a user ID is obtained from the device.

Value: Server

Type: String

Data: The server to be used for login when a user ID is obtained from the device.

Key: HKLM\SOFTWARE\Novell\NMA\<<Method Name>>\ID\LDAPServers

This key contains an ordered list of LDAP servers that is queried for the user name when data is read from the device.

Corresponding to each of the LDAP servers in the list, the administrators can specify the full path of the trusted root certificate file as the data for the value with the prefix `TrustedCertificateFile` and the server number as the suffix. For example, a value `TrustedCertificateFile0` can have `C:\Certificates\TrustedRoot-acme.com.der` as the data.

If these values are not present, pcProx LCM automatically imports and writes contents of the trusted root certificate under this key with a prefix of `TrustedCertificate` and a suffix of the corresponding server number. For example, the contents of the trusted root certificate of the server with the number 0 has the value as `TrustedCertificate0`.

ADDING A CERTIFICATE

- 1 Export the certificate from eDirectory using iManager
 - 1a Log in to iManager.
 - 1b In Roles and Tasks, click *Directory Administration* > *Modify Object*.
 - 1c Use the Object Selector to select the SSL CertificateDNS certificate.
 - 1d Click *OK*.

1e Verify if *Novell Certificate Server Plug-ins* for iManager is installed or not. If it is not installed it, install it.

1f In Roles and Tasks, click *Novell Certificate Access* > *Server Certificates*.

1g Select *SSL CertificateDNS* > *Export*.

1h From the *Certificate* drop-down list, select *SSL CertificateDNS*.

1i If *Export private key* is selected, deselect it and select the export format as `.DER`

1j Click *Next* and specify the path to save the file.

2 Importing the certificate to JRE keystore used by iManager

2a Run the command prompt and change the directory to JRE path that is used by iManager.

2b Navigate to bin directory under JRE directory.

- ◆ The JRE path for workstation iManager running on,
 - ◆ **Windows:** <iManager extracted directory>\bin\windows\java\jre
 - ◆ **Linux:** <iManager extracted directory>/bin/linux/java/jre
- ◆ The default path for iManager server installation is,
 - ◆ **Windows:** C:\Program Files\novell\jre
 - ◆ **Linux:** opt\novell\jdk\jre

2c Run following command.

```
<Prompt>keytool -import -file <imported certificate file path> -alias <alias to identify the server> -keystore..\lib\security\cacerts -storepass changeit
```

NOTE: alias is optional.

Example

Use the following command to import the certificate (`cert.der`) from C:\, under the `NSL611TREE` tree,

```
C:\Program Files\novell\jre\bin>keytool -import -file c:\cert.der -alias NSL611TREECERT -keystore ..\lib\security\cacerts-storepass changeit
```

2d If the import is correct, press *Y*.

2e Restart iManager.

Legal Notice

Copyright © 2007 - 2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher. For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmliist.html\)](http://www.novell.com/company/legal/trademarks/tmliist.html). All third-party trademarks are the property of their respective owners. A trademark symbol (®, ™, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark.