AUTHORIZED DOCUMENTATION

pcProx Guide

Novell® SecureLogin

7.0 SP1 HF2

July 20, 2010

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide contains the following section:

Audience

This guide is intended for administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *pcProx Guide*, visit the Novell SecureLogin Documentation Web site (http://www.novell.com/documentation/securelogin70).

Additional Documentation

For documentation on other Novell SecureLogin documentation, see the Novell SecureLogin Documentation Web site (http://www.novell.com/documentation/securelogin70).

The other documents available with this release of Novell SecureLogin are:

- *Getting Started*
  - “Novell SecureLogin Readme 7.0 SP1Hot Fix 2”
  - “Novell SecureLogin Quick Start Guide”
  - *Novell SecureLogin Overview Guide*
- *Installation*
  - *Novell SecureLogin Installation Guide*
- *Administration*
  - *Novell SecureLogin Administration Guide*
  - *Novell SecureLogin Application Definition Wizard Administration Guide*
  - *Novell SecureLogin Citrix and Terminal Services Guide*
- *End User*
  - *Novell SecureLogin User Guide*

- *Reference*
  - *Novell SecureLogin Application Definition Guide*

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Installing and Using pcProx

1

The NMAS™ Login Method and Login ID plug-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 plug-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

1.1 Software Requirements

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

1.1.1 Client

- Microsoft* Windows* Vista* SP1, 32-bit and 64 bit.
  - Microsoft Vista Ultimate
  - Microsoft Vista Enterprise
  - Microsoft Vista Business
- Microsoft Windows Server* 2003, 32-bit.
- Microsoft Windows Server 2008, 32-bit and 64-bit.
- Microsoft Windows XP Professional SP2 and SP3, 32-bit
- NMAS Client 3.4 or later for Microsoft Windows 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.

1.1.2 Server

Have the following server on the workstations that uses pcProx:

- Novell eDirectory™ 8.8.5, 8.8.4, or 8.8.3.
- NMAS Server - the version bundled with the eDirectory version you are using.

1.1.3 Novell iManager

- Novell® iManager 2.7.2 and 2.7.1

1.2 Installing PcProx NMAS Login Server Method

NOTE: Installing the NMAS Login Server Method for pcProx by using the iManager plug-in for NMAS with iManager 2.6 fails to extend the schema definition of the User object class with the sasPcProxID attribute. This means that you are unable to associate the pcProx card ID with the User object for identification.

To resolve the issue, you must manually add the sasPcProxID attribute to the user object class by using the iManager schema plug-in.

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/agrxfn3.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.

1.3 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)
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\2.7* folder of the Novell SecureLogin 7.0 SP1 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)

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 2.7

Configuring pcProx for Identification (Login ID)

2

After you have installed NMAS and the login method software, configure pcProx for identification, that is, configure as a login ID.

2.1 Setting Up the Hardware

- The workstation that uses the pcProx login method must have a pcProx card reader.

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

2.2 Configuring the Workstation to Scan the pcProx Card Through Plug-In

1. Run `pcprox.reg` available in the `iManager` folder in the Novell SecureLogin 7.0 SP1 installer package.

2.3 Configuring pcProx card format

To configure pcProx card to supports different card format:

1. On the Windows Start menu, click *Start* > *Run* to display the Run dialog box.
2. Type regedit then click `OK` to open the Registry Editor.
3. Browse to the `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NMAS\MethodData\pcProx.`
4. Create a registry string value `FilterMask`.
5. Use the PFIP (P - Leading Parity F- Facility Code I -Card Id P-Trailing Parity) format to set the value of the `FilterMask`.

   Example: PFFFFFFFFIIIIIIIIIIIIIIIP. In this example the 26 bit card format consists of:

   - 1 - Leading Parity
   - 8 - Facility Code

- 16 - Card ID
- 1 - Trailing Parity

6 Exit the Registry Editor.

NOTE: Default behavior will be applied if the card format is not set. The default behaviour is to assign all the bits as Card ID.

For information on different pcProx card format see pcProx Card Formats (http://www.rfideas.com/support/learning_center/proximity_card_formats.php).

2.4 Adding a pcProx Card as a Login ID

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

- Section 2.4.1, “Adding by Scanning the Card,” on page 14
- Section 2.4.2, “Adding Manually,” on page 14

NOTE: ◆pcProx identification fails in LDAP Credential Provider mode because pcProx caches the certificate in the registry to identify the card on the server (that is, eDirectory) it is registered. If you change the server, pcProx does not have the logic to verify if the certificate is valid or not. pcProx treats the certificate from the new server as invalid. It tries to identify with this certificate and so, the identification fails.

To resolve this issue, you must delete the certificate registry value whenever you change the identification server (eDirectory).

You must delete the *TrustedCertificate0*, which is located in the `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NMAS\MethodData\pcProx\ID\LDAPServers`

- Identification might also fail if the certificate is corrupted. In such a scenario, delete the old cached certificate from the registry and add new certificate.

2.4.1 Adding 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.

2.4.2 Adding 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.

2.5 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.

2.6 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.

Configuring pcProx for Authentication

3

3.1 Setting Up the Hardware

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

3.2 Installing the Login Server Method for pcProx in eDirectory

See Section 1.2, “Installing PcProx NMAS Login Server Method,” on page 10

3.3 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)

NOTE: This task is not necessary for the ID plug-in

3.4 Configuring the Workstation to Scan the pcProx Card Through Plug-In

1 Run `pcprox.reg` available in the `iManager` folder in the Novell SecureLogin 7.0 SP1 installer package.

3.5 Configuring the Login Method

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

Refer the following sections to manage the login method for pcProx through iManager:

- Section 3.5.3, “Removing a pcProx Card from a User,” on page 19
- Section 3.5.4, “Allowing a User to Self-Enroll the Card ID,” on page 19

3.5.1 Adding a Certificate

After you have installed the pcProx plug-in on the server sunning iManager, you must import certificates to the workstation running iManager. Importing the certificate associates the proximity card to the user for authentication.

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

3.5.2 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/agrxfn3.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.

3.5.3 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.

3.5.4 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.

Registry Keys and Values for the pcProx Method

4

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.

4.1 Registry Keys and Values for the pcProx Plug-In

Key: `HKLM\SOFTWARE\Novell\NMAS\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\NMAS\<<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`.