Entrust Login Method for NMAS™

2.2

Installing and Using Entrust

The Entrust login method for NMAS enables you to authenticate to Novell eDirectory™ using an Entrust trusted root certificate to verify the subject name and/or allowable subject name in a user certificate. This is similar to other login methods provided for use with NMAS.

Installing and Configuring the Login Method for Entrust

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/nmas22/index.html).

Prerequisites

You must meet the following prerequisites before installing Entrust:

- Windows* 98 or later
- NMAS 2.02 or later
- Each client being used must have Entrust/Entelligence* 5.x installed.
- Each user must have an Entrust profile set up on the client being used.

Steps

As with all login methods, you must complete the following steps to make the login method available for use:

1. Set up any required hardware.
2. Install the login method.
3. Configure the login method.
4. Create a login sequence.
5. Authorize login sequences for users.

Setting Up the Hardware

The Entrust login method does not require any additional hardware.

Installing the Login Method for Entrust

There are two steps in installing and setting up the login method for Entrust:

1. Set up the login method in eDirectory.

2. Install the Entrust login method client module on each workstation.

Setting Up the Login Method in eDirectory

There are three ways to set up the login method in eDirectory:

- The Login Method Installer (Windows workstation to any platform)

  The login method installer (methodinstaller.exe) is a standalone utility that installs login methods into eDirectory.

- nmasinst utility (UNIX* only)

  The nmasinst utility allows you to install login methods into eDirectory from a UNIX machine. The utility is located in the \usr\bin\nmasinst directory.

  For information on setting up a login method using the login method installer or the nmasinst utility, see the *NMAS Administration Guide* (http://www.novell.com/documentation/lg/nmas21/index.html).

- ConsoleOne® (Windows workstation to any platform)

IMPORTANT: 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*.

1. In ConsoleOne, expand the Security container.
2. Right-click the Authorized Login Methods container.
3. Select New > Object to start the New Object Wizard.
4. Select the SAS:NMAS Login Method class, then click OK.
5. Specify the configuration file, then click Open.

   The configuration file is located in the login method folder and is usually named config.txt.
6. In the license agreement page, click Accept, then click Next.
7. Accept the default method name or rename it, then click Next.
8. Review the available modules for this method, then click Next.
9. If you want to create a login sequence that uses only this login method, leave the check box checked, then click Finish. If you don't want to create a login sequence that uses only this login method, uncheck the check box, then click Finish.
10. Review the installation summary, then click OK.
11. If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne login method snap-ins. You can then configure the login method and enroll users to use it.

Installing the Entrust Login Method Client Module on Each Workstation

The client module must be installed on each workstation that will use the Entrust login method.

To install the client module, run clientsetup.exe in the entrustadv\client directory on each workstation that will use the login method. Follow the instructions of the installation wizard.

Configuring the Login Method for Entrust

After the login method for Entrust is installed, you can manage it using ConsoleOne. You will need to do two levels of configuration:

- General Method configuration
- User Object configuration

General Method Configuration

1. Obtain a self-signed trusted root certificate from the Entrust CA by running the ExtractEntrustCACert utility located in the entrustadv directory on the NMAS software build. It is a DOS command line utility. The syntax is ExtractEntrustCaCert c:\cacert.der. This file is then used when creating the trusted root object.
2. In ConsoleOne, expand the Security container.
3. If you have a trusted root container, skip to step 4. If not, create a trusted root container under the Security container by doing the following:
   - **3a** Right-click the Security container and selecting New > Object to start the New Object Wizard.
   - **3b** Select the NDSPKI:Trusted Root class, then click OK.
   - **3c** Specify a name for the trusted root container, then click OK.
4. Create a trusted root object in the trusted root container by doing the following:
   - **4a** Right-click the trusted root container and click New > Object to start the New Object Wizard..
   - **4b** Select the NDSPKI:Trusted Root Object class, then click OK.
   - **4c** Enter a name for the trusted root object, then click OK.
   - **4d** Click the Read from file button and browse for the trusted root certificate you exported in step 1, select it, then click Open, then click Finish.
5. Expand the Authorized Login Method, right-click the Entrust certificate object, then click Properties > Certificate tab.
6. Add the new trusted root container as a Certificate Search container by clicking Add. Browse for the trusted root container, select it, and click OK, then click OK again.

User Object Configuration

1. Double-click a User object.
2. Click the Security tab > Certificate Subject Names.

3 Click Add and type either the Entrust certificate's Issued To name or an allowable subject name. This must be the e-mail ID.

4 Click OK.

Creating a Login Sequence

When you set up the login method in eDirectory, you had the option to create a login sequence using only this login method. If you chose to do this, you already have a login sequence that uses this login method.

If you want to create other login sequences using this method, see Chapter 2 of the *NMAS Administration Guide* for information on creating a login sequence.

Authorizing Login Sequences for Users

By default, all login sequences are available to users. If you want to restrict a user from having access to a login sequence or if you want to set a default login sequence for a user, see Chapter 2 of the *NMAS Administration Guide* for information on authorizing a login sequence for users.