

Setup Instructions for Digipass Method

Novell.



| | |
|--|-----------|
| Market Overview | 3 |
| Product Overview | 3 |
| Authentication Features | 3 |
| NMAS Enterprise Edition | 3 |
| Product Tour | 4 |
| Requirements..... | 5 |
| Procedures | 5 |
| Check Version of Server NCI and Novell Certificate Server | 5 |
| Create NSS Volumes..... | 6 |
| Install ConsoleOne | 8 |
| Install NMAS Enterprise Edition | 8 |
| Create a New User..... | 10 |
| Install Client Login Method Components (Client) | 10 |
| Install Server Login Method Components (Server)..... | 11 |
| Create the VASCO Container and Assign Users for VASCO Token | 12 |
| Define Login Sequence | 15 |
| Establish Clearances for Users | 17 |
| Make User Admin a Multi-Level Administrator..... | 18 |
| Set the Administrator’s Default Login Sequence | 19 |
| Set Up Volume Trustees | 19 |
| Set Up Volume Clearances..... | 20 |
| Observe Multi-Factor Authentication and Graded Authentication | 22 |
| Conclusion..... | 24 |

Market Overview

In an age of ubiquitous electronic connectivity where hackers, viruses, electronic eavesdropping and fraud can threaten the communication, productivity, and prosperity of businesses and individuals, advanced network authentication-based solutions are becoming a necessary component in corporate security policies.

Advanced network authentication lessens the threat of intrusion by requiring users to provide stronger authentication credentials and by allowing for the creation of multi-factor login sequences.

Ideally, advanced authentication methods should be managed in a complementary advanced authentication framework that supports the access of network resources. In addition, the framework should be secure enough so that information accessed through one form of authentication cannot be moved to a network area requiring a different form of authentication.

Product Overview



NMAS Enterprise Edition provides the advanced authentication methods and framework needed for implementing and managing a stronger authentication policy.

Novell's "Graded Authentication" provides the means to set network access at the NDS volume level, based on the authentication sequence used. In addition, Graded Authentication keeps information secure by preventing users from copying or moving information from one secure location to another location requiring a lesser "grade" of authentication credential for access.

Authentication Features

Support for new Novell-developed authentication methods

- NDS password authentication
- X.509 certificate authentication (via Novell Certificate Server 2.0)
- Simple password authentication
- Support for third-party authentication methods
- VASCO Digipass authentication
- Multi-factor authentication
- Graded Authentication

NMAS Enterprise Edition

The NMAS framework extends the options for user login from NDS password only, to a variety of Novell methods. These methods are managed on an individual user basis through ConsoleOne.

For each method, including the traditional NDS password method, there is an associated Login Client Module (LCM) and a Novell digitally signed Login Server Module (LSM). Novell distributes the LSMs on the Enterprise Edition CD.

NMAS is managed through an easy-to-install ConsoleOne snap-in module. Specific ConsoleOne property pages let the administrator manage authentication methods, the sequence of those methods, and the security grade associated with those methods.

During the installation of the snap-in module, NMAS extends the NDS schema and creates two new containers in the Security container. These containers are the Authorized Login Methods and Login Policy objects. All authentication modules are stored and managed in the Login Method container.

Assigning how a user authenticates using NMAS is done by assigning a login sequence. Sequences incorporate one or more authentication methods and are stored in the new Login Policy object in the Security container. A sequence includes the methods and the order that those methods execute during user authentication.

The NMAS framework lets administrators easily chain both Novell and Digipass authentication methods as part of a login sequence. No collaborative engineering work between different companies is needed. The NMAS framework does the collaboration. This makes it possible to create a sequence using a VASCO Digipass and a standard NDS password.

Graded Authentication lets administrators determine a scale or grade for the authentication methods supported and grant access rights accordingly. For example, the organization's security policy might specify that using a One Time Password generated by a Digipass token in tandem with an NDS password is a stronger form of authentication than using an NDS password alone. As a result, a user successfully authenticated with a Digipass and NDS password might receive a very wide set of access rights since the administrator has greater confidence in that form of authentication and is assured that the user is not an intruder. Conversely, a user authenticating to the network with just a password might be granted a limited set of access rights. Therefore, Graded Authentication allows the administration of network access rights to be more finely controlled.

Product Tour



This document provides step-by-step procedures for setting up and using VASCO Digipass with NMAS graded authentication features.

Along with the necessary Novell software components, VASCO Data Security provides two-factor tokens and the VASCO method. It should be noted that VASCO tokens are set at the "demo" mode for this exercise.

In this exercise, you will create a new user named "Edward" and create three different login sequences for him. You will then see how Edward will be able to access certain NetWare volumes (specifically, the "Payroll," "Research," and "Sales" volumes) only when he authenticates using the correct authentication sequence.

In addition, you will see how Edward's rights change based on the authentication method used, and how Graded Authentication prevents Edward from moving secure information from the "Payroll" and "Research" volumes to the "Sales" volume.

This exercise also provides procedures for assigning the administrator to be a Multi-Level Administrator, and how having this classification, once authenticated, allows the administrator to have Read and Write rights to all three volumes.

Requirements

- NetWare 5.1 server minimum
- **Note:** NMAS works in a NetWare 5.x environment. For this exercise, we have written the procedures as if you were using a NetWare 5.1 server.
- Windows client workstation connected to server with Novell Client software installed.
- NDS Supervisor rights to the [Root] of the NDS tree.

Procedures

This document describes the following procedures:

1. Check the version of Novell International Cryptographic Infrastructure (NICI) and Novell Certificate Server.
2. Create Novell Storage Services (NSS) volumes.
3. Install ConsoleOne.
4. Install NMAS Enterprise Edition.
5. Create a new user.
6. Install client login method components.
7. Install server login method components.
8. Create the VASCO container and assign users for VASCO tokens.
9. Define login sequences.
10. Establish clearances for users.
11. Make user Admin a multi-level administrator.
12. Set the default login sequence for user Admin.
13. Set up volume trustees.
14. Set up volume clearances.
15. Observe multi-level authentication and Graded Authentication.

Check Version of Server NICI and Novell Certificate Server

If the server version of Novell International Cryptographic Infrastructure (NICI) is below 1.5 or the version of Novell Certificate Server is below 2.02, you will need to install newer versions.

1. At the NetWare server console, type NWCONFIG.
2. From the Configuration Options menu, select Product Options.
3. From the Other Installation Actions menu, select View/Configure/Remove Installed Products.
4. View the version of NICI and Novell Certificate Server (listed as PKIS) in the Currently Installed Products list.

Install newer version of server NICI (Conditional)

1. At the NetWare server, insert the NMAS Enterprise Edition CD.

2. At the server console, type CDROM.
Wait for the volume to mount.
3. Type NWCONFIG
4. From the Configuration Options menu, select Product Options.
5. From the Other Installation Actions menu, select Install a Product Not Listed.
6. Read the message.
7. Type <F3> to specify a new location.
8. Specify the path to the NICI module.
This will be NMAS_EE:NICI_1.5\NWSERVER
9. Read the license agreement and then press <Esc> to continue.
10. Press <Enter> to accept the license agreement.
11. When prompted on whether you want to view the readme file, select Yes or No.
If you select No, the installation begins.
12. When the installation is complete, press <Enter> to continue.
13. Exit NWCONFIG.
14. At the server console type DOWN to shut down the server.
15. Reboot the server.
16. Start the server up again.

The server reboots with the new NICI version.

Install newer version of Novell Certificate Server (Conditional)

1. From the Windows client workstation, log in to the NetWare 5 server as Admin or the user that has NDS Supervisor rights to the [Root] of your NDS tree.
2. Insert the NMAS Enterprise Edition CD.
3. Exit the NMAS installation auto-start screen.
4. Run the Windows Explorer application, locate and open the CERTSERV folder and launch the INSTALL.EXE.
5. Follow the prompts in the installation wizard.

Create NSS Volumes

You will now create three Novell Storage System (NSS) volumes named "Payroll," "Research," and "Sales," where the features of NMAS can be easily observed and understood.

You must have available disk space on the NetWare server that is not currently allocated to a volume.

1. At the NetWare server console, type NWCONFIG.
2. From the Configuration Options menu, select NSS Disk Options.
3. Select Storage.
4. Select the following options in order:
 - **Update Provider Information** scans your storage for free space. Choose a provider from the list.
 - **Assign Ownership** assigns a consumer to the free space storage deposit you select and creates an NSS partition. NSS needs to own the free space before an NSS volume can be created.
 - **View Free Space** (optional).
5. From the Available NSS Options menu, select NSS Volume Options.
6. Authenticate the NDS admin by entering the full context and password.
7. From the Available NSS Volume Options menu, select Create.
8. Select Storage Group.
9. Select a managed object. If you have more than one managed object, a list will appear.
10. Confirm your choice.
11. Select NSS Volume.
12. Select the managed object.
13. When prompted, enter the size in megabytes of the first of the three new volumes you will create.

NOTE: 10 MB will be more than adequate for this exercise.
14. Enter PAYROLL as the name for the volume.
15. Confirm your choice.
16. Create volumes named RESEARCH and SALES.

Again, 10 MB for each volume will be more than adequate for this exercise.
17. Exit NWCONFIG.

18. At the NetWare 5.1 server console, mount all three NSS volumes by typing MOUNT <volume name> at the server console. Make sure to mount all three volumes created (Payroll, Research, and Sales).

Install ConsoleOne

1. From the Windows client workstation, verify that you have a mapped drive to SYS:PUBLIC on the NetWare 5.1 server.
2. At the same workstation, insert the NMAS Enterprise Edition CD.
3. If the NMAS installation auto-start screen appears, exit from it.
4. Run the Windows Explorer application, locate and open the CONSOLEONE12C folder and launch the SETUP.EXE.
5. When prompted, select the language version to install.
6. When prompted, indicate the server volume where you want ConsoleOne installed.
7. Use the Browse button to locate the mapped drive to SYS:PUBLIC.
8. Follow the remaining prompts in the installation wizard.
9. When finished, reboot the client workstation and the NetWare server.

Install NMAS Enterprise Edition

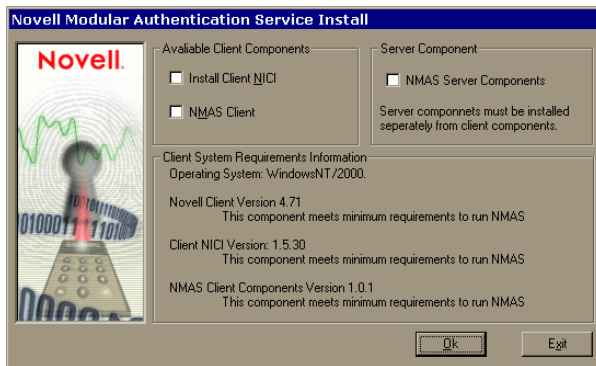
Prior to following the installation procedures below, refer to the README.TXT file on the NMAS Enterprise Edition CD for any installation issues.

1. From the Windows client workstation, log in to the NetWare server as Admin or the user that has NDS Supervisor rights to the [Root] of your NDS tree.
2. Insert the NMAS Enterprise Edition CD.
3. Follow the installation prompts.

If the installation utility determines that you need to update your client software, you must do so before installing NMAS Enterprise Edition. You will be exited from the installation utility.

Insert the Novell Client CD, select the appropriate Novell Client for your workstation platform, and follow the installation prompts. Reboot the workstation when finished. Begin Step 1 again.

4. The following screen appears.

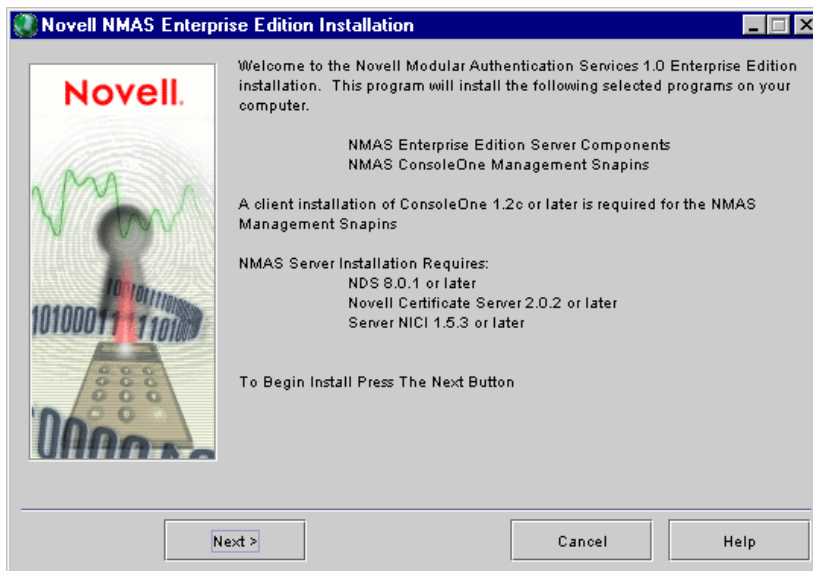


The installation screen autodetects the needed client components by checking applicable checkboxes.

We recommend that you install the server components first, then restart the server. While the server is restarting we recommend that you then install the client components. The procedures below are written in that order.

5. Check the NMA Server Components check box in the Server Component area of the screen and click OK.

The following wizard page appears.



6. Click Next and follow the prompts in the installation wizard.
7. When prompted, restart the server. During the restart, install the client components by following the procedures below.
8. From the Windows client workstation, run the Windows Explorer application, locate and run NMAINSTALL.EXE from the root of the NMA-EE CD.

The NMA installation screen appears.

9. In the Available Client Components area, leave the checkbox settings as they are currently set.
10. Click OK.
11. Review the license text and click Accept.
12. Follow the installation procedures in the installation wizard as prompted.
13. Restart the Windows client workstation when the installation is complete.

Create a New User

In this section you will create a new user and assign multiple NMAS clearances so that you can see how multi-factor authentication and Graded Authentication work.

1. From the Windows client workstation, log in to the NetWare 5 server as Admin or the user that has NDS Supervisor rights to the [Root] of your NDS tree.
2. From the Windows client workstation, start the version of ConsoleOne installed on the NetWare server (<server_name>:SYS:PUBLIC\MGMT\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE).

3. Create a new user.

In this example, the user will be referred to as "Edward."

4. Leave the Assign NDS Password check box checked.
5. Click OK.
6. When prompted, create a user password for Edward.
7. Close ConsoleOne.

Install Client Login Method Components (Client)

You'll now use ConsoleOne to install the VASCO client method components.

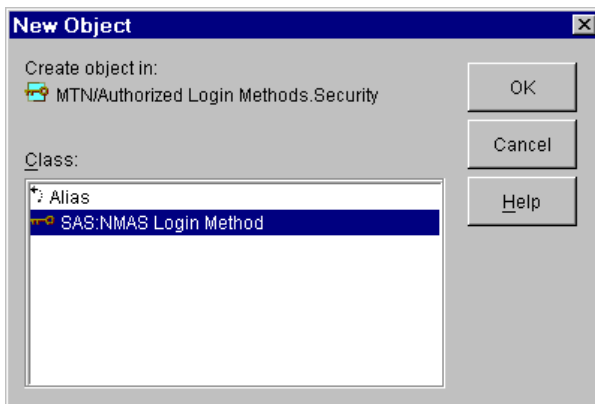
1. At the Windows client workstation, insert the NMAS Enterprise Edition CD.
2. If the NMAS installation auto-start screen appears, exit from it.
3. Run SETUP.EXE from the following path:
NMAS-EE\METHODS\VASCO\DIGIPASS\CLIENT
4. Select the default option
5. Press Finish
6. Restart your workstation following the installation.

Install Server Login Method Components (Server)

You'll now install the VASCO server method components through ConsoleOne.

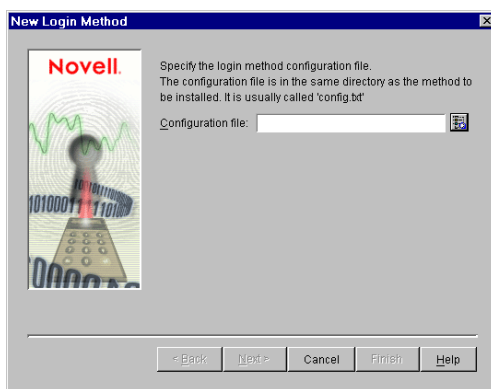
1. Launch ConsoleOne.
2. Expand the Tree object where the NetWare server is located.
3. Expand the Security object below the Tree object.
4. Highlight the Authorized Login Methods, right-click and select New > Object.

The following dialog appears.



5. Select the SAS: NMAS Login Method and click OK.

The following dialog appears.



6. Browse for the VASCO method CONFIG.TXT file using the following path:

NMAS-EE\METHODS\VASCO\DIGIPASS

7. Follow the remaining prompts in the installation wizard. Leave the Create Login Sequence check box checked so that a login sequence for this method is created.

8. Close the installation wizard when finished.
9. Exit from ConsoleOne.

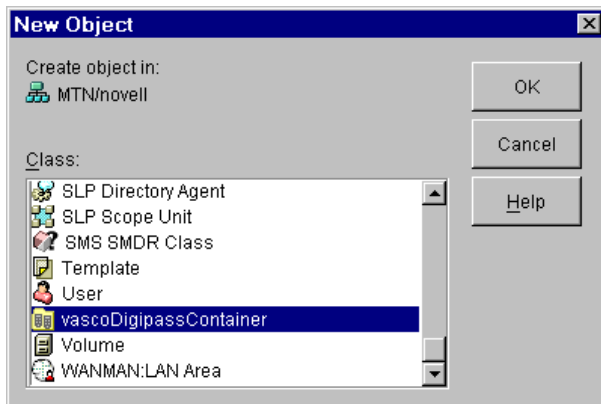
Note: You must exit and restart ConsoleOne before the installed NMAS methods are available for use.

Create the VASCO Container and Assign Users for VASCO Token

In this section you will create the necessary VASCO containers and then assign Edward so that he can use a VASCO Digipass token.

1. Launch ConsoleOne.
2. Highlight the Organization or Organizational Unit object where Edward resides, right-click and select New > Object.

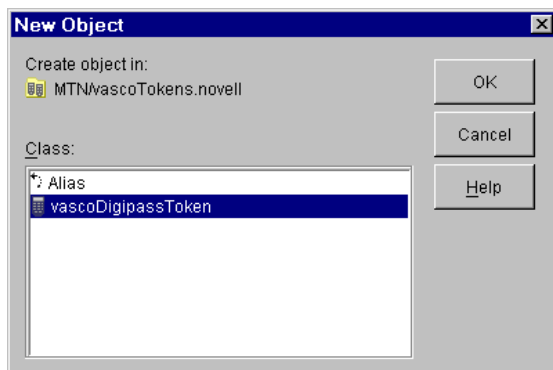
The following dialog appears.



3. Select the VASCO Digipass Container and click OK.
4. When prompted for a container name, give it something descriptive such as "Digipass".
5. Highlight the new VASCO container, right-click and select

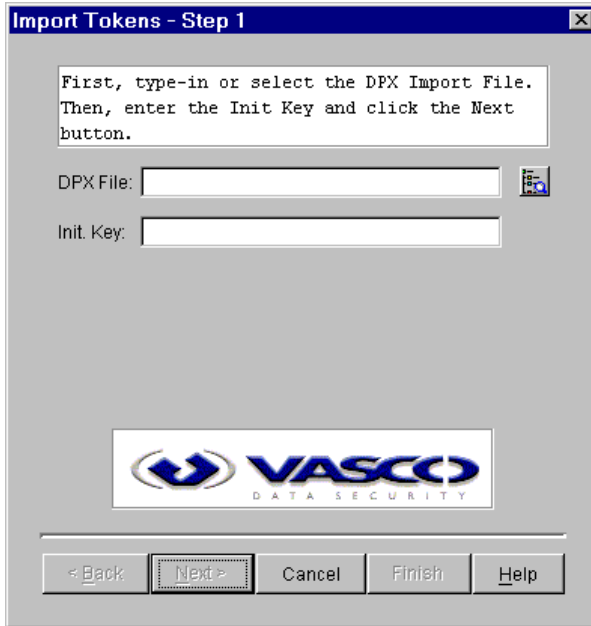
New > Object.

The following dialog appears.



6. Highlight the Digipass token and click OK.

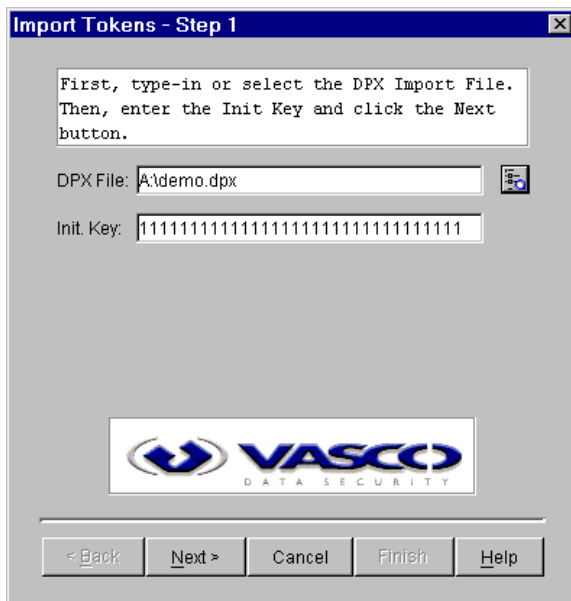
The Import Tokens dialog appears.



7. Insert the VASCO floppy diskette, then click the Browse button to locate the DEMO.DPX file located in the following path:

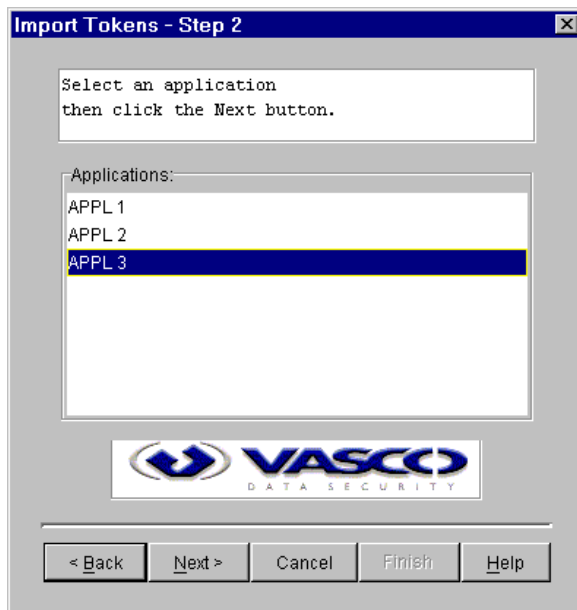
A:DEMO.DPX

8. In the Browse dialog, select Import.
9. Open the INSTRUCT.TXT file from the floppy diskette and copy and paste the Init. Key numbers in the Init Key field.



10. Click Next.

The following dialog appears.



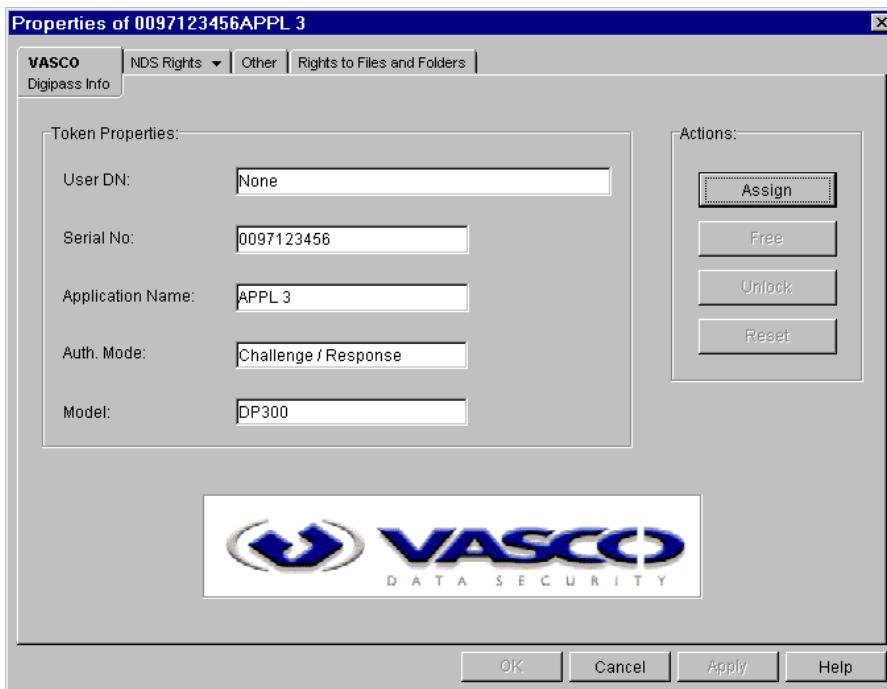
11. Select "APPL 3" (which is the designation for the VASCO challenge-response mode) and click Next.

A dialog appears with a summary of the assigned application and token.

12. Click Finish.

13. In the VASCO Digipass Container object in ConsoleOne, right-click the newly-created VASCO Digipass Token object and select Properties.

The following property page appears.



14. Click the Assign button and locate the user Edward to assign him to use the VASCO Digipass token.

Edward has now been enabled to use the VASCO Digipass token in challenge-response mode.

15. Repeat Steps 5-10. In the Import Tokens – Step 2 dialog, select “APPL 1” (which is the designation for the VASCO Digipass response-only mode) and click Next.

NOTE: IF USING DIGIPASS GO1 OR GO3, IT IS NECESSARY TO USE APPL 1

16. Click Finish

17. Right-click the newly-assigned VASCO Digipass token object and select Properties.

18. Click the Assign button and locate the user Admin to assign him to use the VASCO Digipass token.

User Admin has now been enabled to use the VASCO Digipass token in response-only mode.

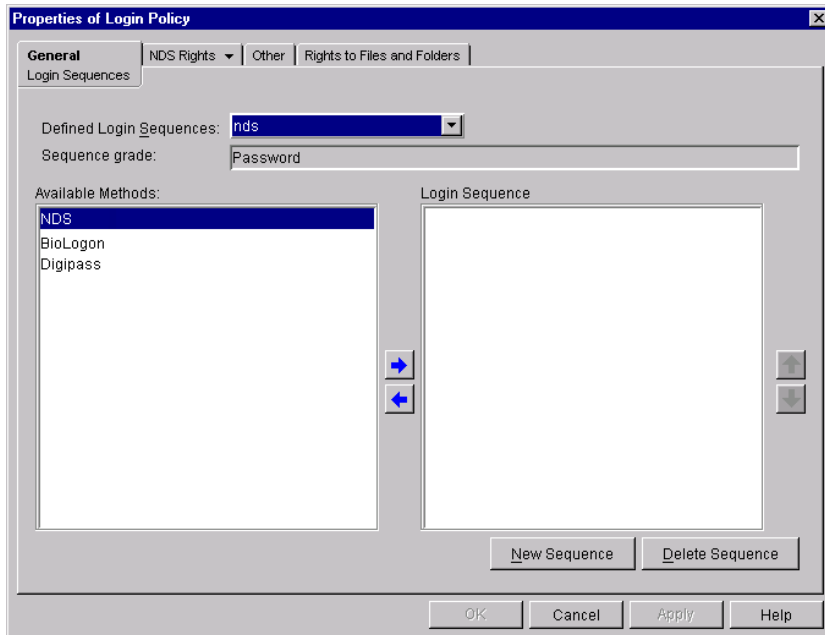
19. Close and restart ConsoleOne.

Define Login Sequence

In this section you define the sequences needed for access to the Payroll, Research, and Sales volumes that you created earlier. Keep in mind that NMAS allows you to set login sequences for access to NDS tree partitions as well. For simplicity, this exercise is at the volume level only.

1. In ConsoleOne, select the Security container, right-click the Login Policy object and select Properties.

The Login Sequences property page appears.



2. Click the New Sequence button.

The New Login Sequence dialog appears.

3. Name the sequence "Sales" and click OK.

This places the new Sales login sequence in the Defined Login Sequences field where you can add methods to the sequence.

4. Move the NDS login method to the Login Sequence window.

5. Click Apply.

6. Repeat Step 2.

7. Name the new sequence "Payroll" and click OK.

8. Repeat Step 2.

9. Name the new sequence "Research" and click OK.

10. Move the Digipass method to the Login Sequence window.

11. Move the NDS login method to the Login Sequence window.

Verify that the Digipass method is above the NDS password method.

12. Click Apply.

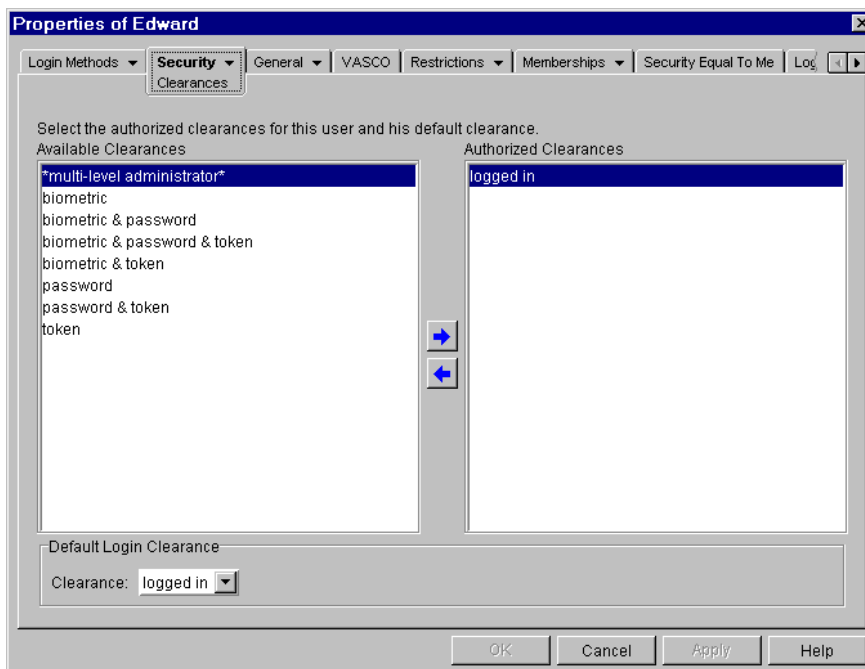
13. Repeat Step 2.
14. Name the new sequence "Admin" and click OK.
15. Move the Digipass and NDS methods to the Login Sequence window.
16. Click Apply.
17. Click Close to close the property page.

Establish Clearances for Users

In this section you set multiple clearances for Edward and the Admin. This will allow you to see the effects of Graded Authentication.

1. In ConsoleOne, right-click Edward and select Properties.
2. Click the Security tab and select Clearances.

The following property page appears.



3. Move the following clearances to the Authorized Clearances window:
 - password & token
 - password
4. From the Clearance drop-down menu, select "password & token" as the default login clearance.
5. Click OK.

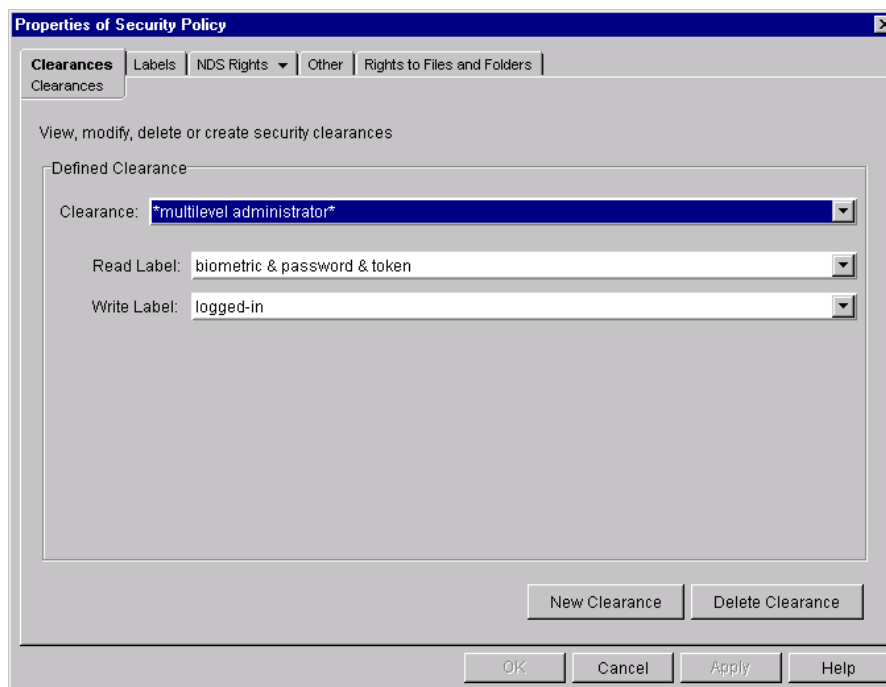
6. Repeat these steps for the Admin, but only give the Admin the “multi-level administrator” clearance.

Make User Admin a Multi-Level Administrator

In this section you will make the Admin a Multi-Level Administrator so that he can have Read and Write rights to all of the volumes.

1. In ConsoleOne, select the Security container, right-click the Security Policy object and select Properties.

The following property page appears



2. In order to have Multi-Level Administrator clearance, the Admin needs to authenticate using these factors.
3. Close the property page.
4. In ConsoleOne, highlight the Admin, right-click and select Properties.
5. Set the default login clearance for the Admin by choosing Multi-Level Administrator from the Security Clearance drop-down menu.
6. Click OK.

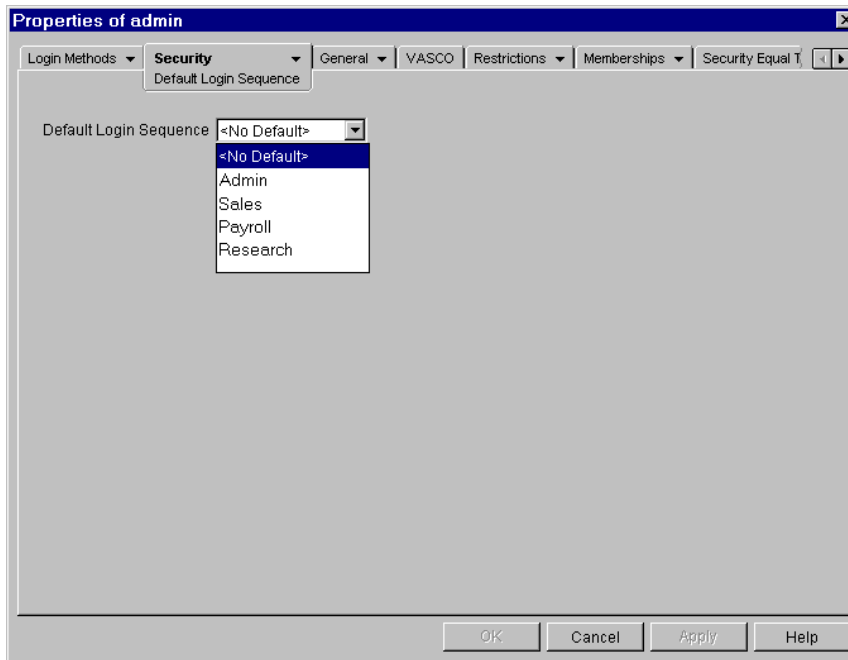
Now every time user Admin logs in, his default clearance will be Multi-Level Administrator.

Set the Administrator's Default Login Sequence

In this section you will set the default login sequence for the administrator.

1. In ConsoleOne, right-click the Admin object and select Properties.
2. Under the Security tab, select Default Login Sequences.

The following property page appears.



3. Select Admin and click OK.

Set Up Volume Trustees

In this section you will make Admin and Edward trustees of the Payroll, Research, and Sales volumes.

1. In ConsoleOne, right-click the Payroll volume and select Properties.

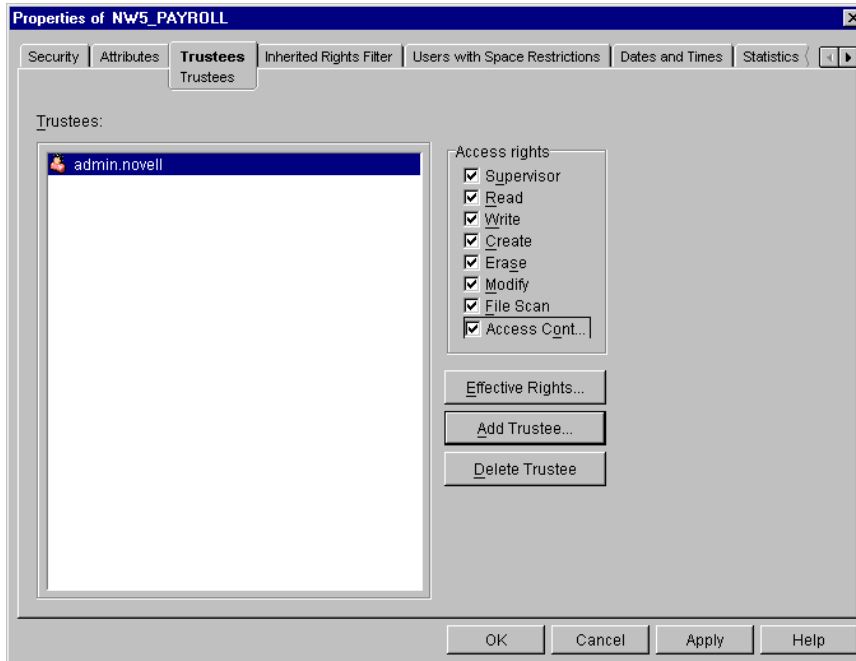
The Volume Security Label property page appears.

2. Click the Trustees tab.

The Trustees property page appears.

3. Click the Add Trustee button.
4. When the browse dialog appears, click the folder icon to go up a level.
5. Select the Admin object and click OK.


6. Make user Admin a supervisor of the volume with all rights.



7. Click the Add Trustee button again and add Edward.
8. Give Edward the Read, Write, Create, Erase, Modify, and File Scan rights.
9. Click OK.
10. Repeat these steps for the Research and Sales volumes.

Set Up Volume Clearances

In this section you will set the clearances needed to access the Payroll, Research, and Sales volumes.

1. Reboot the Windows client workstation.
2. Log in as user Admin and select the Admin login sequence.
Follow the enrollment procedures as prompted.
3. When prompted for the VASCO password (this is the response-only mode), press the  button and enter your PIN if using a Digipass 300 or 250 model

Digipass 250



NOTE: The VASCO Digipass demo token pins are normally 1234.

4. When the APPLI prompt appears on the token, press 1 (for application 1 or response-only mode).

Digipass Go1

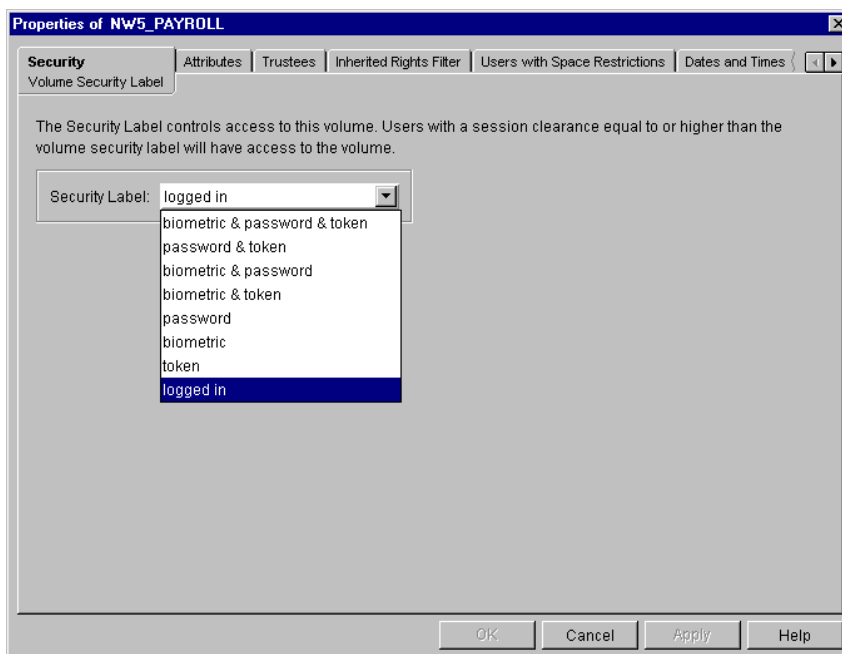
A one-time password (series of numbers) appears on the VASCO Digipass token.



NOTE: If using a DP Go1 or Go3, you only need to open the token or press the button on the token

5. In the dialog, enter the one-time password displayed on the token.
6. Enter the NDS password for the Admin when prompted.
7. Start ConsoleOne.
8. Right-click the Payroll volume and select Properties.

The Volume Security Label property page appears.



9. Observe the security label default for the volume ("logged in").
10. Change the security label to "password.& token"

This means that Edward will only be able to access this volume with a token and NDS password clearance or higher.

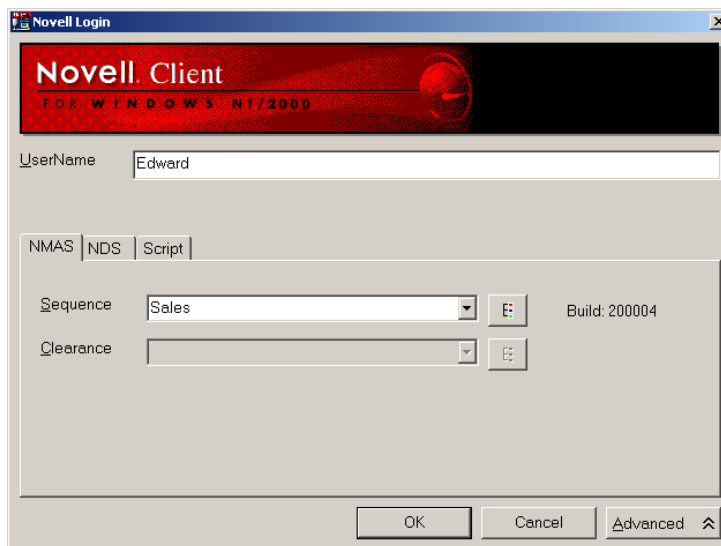
11. Click OK.
12. For the Research volume, repeat Steps 1-4, and make the clearance "password & token."
13. Click OK.

14. For the Sales volume, repeat Steps 1-4, but make the clearance "password."
15. Click OK.

Observe Multi-Factor Authentication and Graded Authentication

In this section you will use the sequences needed to access the Payroll, Research, and Sales volumes.

1. From the client that you upgraded with NMAS, log in to the NetWare 5 server as Edward, select the Sales sequence.



2. From the workstation desktop, right-click the Network Neighborhood icon and select Novell Map Network Drive.

The Map Drive dialog appears.

3. In the Enter the Network Path to the Resource field, enter

`\\server_name\sales`

4. Click Map.
5. Verify that you can create documents in the Sales volume.

6. From the workstation desktop, right-click the Network Neighborhood icon and select Novell Map Network Drive.

The Map Drive dialog appears.

7. In the Enter the Network Path to the Resource field, enter

`\\server_name\payroll`

8. Click Map.

You are denied access to that volume because it requires a stronger clearance.

9. Right click the NetWare Services red "N" on the bottom right-hand corner of your desktop and select NetWare Login.

10. In the Novell Login dialog box, change the sequence to Payroll and click OK.

11. When prompted, enter the VASCO Digipass One Time Password

12. When prompted, enter Edward's NDS password.

13. Now map a drive to the Payroll volume and create a new folder and name it "Salaries."

14. Map another drive to the Sales volume.

15. Attempt to copy the Salaries folder to the Sales volume. Observe that you are prohibited from doing so.

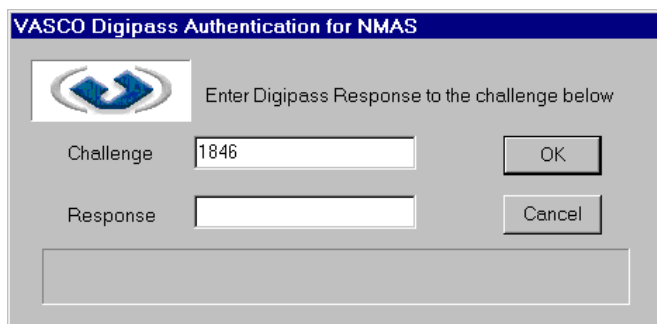
Graded Authentication not only restricts user access via authentication methods used, but prevents users from moving information from a high security area to a less secure area.

16. Now attempt to map a drive to the Research volume.

You are prevented from doing so, because the authentication clearance is "password & token."

17. Log in again, but this time, use the Research sequence.

18. The VASCO Digipass method prompts you with a challenge.



This is a variable number that is generated by the VASCO NLM.

19. If using a VASCO Digipass 300 or 250 token, press the ◀ button and enter your PIN.

Again, the VASCO Digipass demo token pins are normally 1234.

20. When the APPLI prompt appears on the token, press 3 (for application 3 or challenge-response mode).

21. On the VASCO token, enter the VASCO challenge number that is currently displayed in the Challenge field on your workstation.
22. In the Response field, enter the response number that is generated on your VASCO token.
23. When prompted, enter Edward's NDS password.
24. Once you are logged in, map a drive to the Research volume and create a folder and name it "Confidential."
25. Map a drive to the Sales volume.
26. While in the Sales volume, attempt to create a new folder. Observe that you cannot. This is because you only have Read rights to that volume at your current clearance.
27. Attempt to copy the Confidential folder to the Sales volume.

Again, Graded Authentication restricts you from doing so.
28. Log in as the Admin using the multi-level administrator sequence.
29. When prompted for the VASCO password (this is the response-only mode), press the \blacktriangleleft button and enter your PIN.
30. When the APPLI prompt appears on the token, press 1 (for application 1 or response-only mode).

A one-time password (series of numbers) appears on the VASCO Digipass token.
31. In the dialog, enter the one-time password displayed on the token.
32. Enter the NDS password for the Admin when prompted.
33. Map drives to the Sales, Payroll and Research volumes.
34. Observe how you can, with this clearance, copy the Confidential and Salaries folders between volumes.

As you can see, the Multi-Level Administrator designation lets you use the security policies of Graded Authentication. Granting the multi-level administrator clearance should therefore be strictly limited.

Conclusion

We hope that this exercise adequately demonstrates both the flexibility and enhanced security that NMAS Enterprise Edition and VASCO Digipass provides. The VASCO and Novell partnership provides some key differentiators that are not available when dealing with other authentication vendors.

Native Integration

The VASCO solution does not require the acquisition and management of an additional authentication server, reducing both cost and complexity of deployment.

Full Interoperability with all Digipass Products

Novell supports Digipass response-only and challenge-response authentication modes as well as all major Digipass management functions (reset, test, and unlock)



Novell Certified

VASCO has obtained Yes, Tested and Approved certification through third-party testing facilities to insure the reliability and functionality of the integration.

About VASCO

VASCO secures the enterprise from the mainframe to the Internet with authentication solutions that enable secure e-business and e-commerce, protect sensitive information, and safeguard the identity of users. VASCO's customers include hundreds of financial institutions, blue-chip corporations, and government agencies in more than 50 countries. More information is available at www.vasco.com or call +1 630-932-8844 for additional information.