

# **Novell Privileged User Manager Evaluation Quick Start Guide**

---

## **2.2 Release**





## Table of Contents

<b>1.0 CONCEPTS AND OVERVIEW .....</b>	<b>3</b>
1.1 PREREQUISITES .....	3
1.2 OBTAINING EVALUATION INSTALLER .....	3
1.3 IMPORTANT INFORMATION – PLEASE READ BEFORE YOU START .....	4
2.1 INSTALL STD MANAGER PACKAGE .....	5
2.1.1 AIX MANAGER INSTALL .....	5
2.1.2 HP-UX FRAMEWORK MANAGER INSTALL.....	6
2.1.3 LINUX FRAMEWORK MANAGER INSTALL.....	7
2.1.4 SOLARIS FRAMEWORK MANAGER INSTALL.....	8
2.1.5 TRU64 FRAMEWORK MANAGER INSTALL .....	9
2.1.6 WINDOWS FRAMEWORK MANAGER INSTALL .....	10
2.2 LOG ON AND SET ADMINISTRATOR PASSWORD.....	11
2.3 LOAD AND INSTALL EVALUATION DATABASES.....	12
2.3.1 LOAD EVALUATION INSTALLER.....	12
2.3.2 INSTALL EVALUATION DATABASES TO HOST .....	12
<b>3.0 INITIAL ORIENTATION.....</b>	<b>14</b>
LOG ON TO THE NOVELL PRIVILEGED USER MANAGER ADMINISTRATION CONSOLE.....	14
CHANGE PASSWORD.....	14
ORIENTATION: HOME MENU .....	15
ORIENTATION: COMPLIANCE AUDITOR .....	16
ORIENTATION: REPORTING.....	17
ORIENTATION: HOSTS.....	18
ORIENTATION: PACKAGE MANAGER.....	19
ORIENTATION: COMMAND CONTROL.....	20
ORIENTATION: MANAGE USERS .....	21
<b>4.0 STEP BY STEP EXERCISES .....</b>	<b>22</b>
REVIEWING KEYSTROKE ACTIVITY PROACTIVELY .....	22
REVIEWING KEYSTROKE ACTIVITY FORENSICALLY .....	27
USE COMMAND CONTROL TO ACCESS A PRIVILEGED SHELL .....	31
REVIEW NOVELL PRIVILEGED USER MANAGER SYSTEM LOGS.....	32
DOWNLOAD NOVELL UPDATES AND DEPLOY TO YOUR HOST .....	33



## 1.0 Concepts and Overview

The Novell Privileged User Manager evaluation package is a collection of preconfigured databases that can be added to any standard manager installation to create an environment pre-populated with sample events and example configurations. Evaluation deployment steps involve:

1. Check prerequisites and download appropriate manager installer binaries (Section 1.1).
2. Obtain evaluation installer (Section 1.2).
- 3. Read and understand evaluation warnings (Section 1.3)**
4. Install standard manager package onto your supported platform (Section 2.1).
5. Log on to the administration console and set initial password (Section 2.2).
6. Install and load evaluation package to create pre-populated environment (Section 2.3)
7. Follow initial orientation to familiarize environment (Section 3).
8. Walk step by step through the example exercises (Section 4).

### 1.1 Prerequisites

- The administration console requires Adobe Flash to operate.
- Binaries for the standard Manager install can be obtained through [download.novell.com](http://download.novell.com)
- Please make sure that you read and understand the implications of installing the evaluation package onto an already configured system in Section 1.3.

#### SUSE Linux Enterprise Desktop and SUSE Linux Enterprise Server

1. You must make sure that the ksh shell is installed for the example exercises in Section 4 to work.
2. Edit `/etc/ksh.kshrc` as shown below to avoid the error below.

```
/bin/ls: cannot read symbolic link /proc/22154/exe: Permission denied
```

This is caused by the following line in `/etc/ksh.kshrc`

```
case "`/bin/ls --color=never -l /proc/$$/exe`" in
```

You can prevent this message by changing the line to the following:

```
case "`/bin/ls --color=never -l /proc/$$/exe 2>/dev/null`" in
```

### 1.2 Obtaining Evaluation Installer

The evaluation installer can be obtained through sales or technical support.

## 1.3 Important Information – Please Read Before You Start

### Note

We recommend that you apply the evaluation database package to a clean installation of the standard Manager. You should also uninstall the package when finished as per the instructions at the bottom of this page.

The evaluation database package consists of pre-population versions of the following databases:

Command Control audit database  
Compliance Auditor event database  
Command Control rules database

### Installing the evaluation package

Installing the evaluation database package will create a backup copy of your existing configuration and replace with the following:

- Sample log events, including keystrokes
- Sample Compliance Auditor events and rule
- Sample Command Control rule configuration
- Sample Command-Risk configuration

### Uninstalling the evaluation package

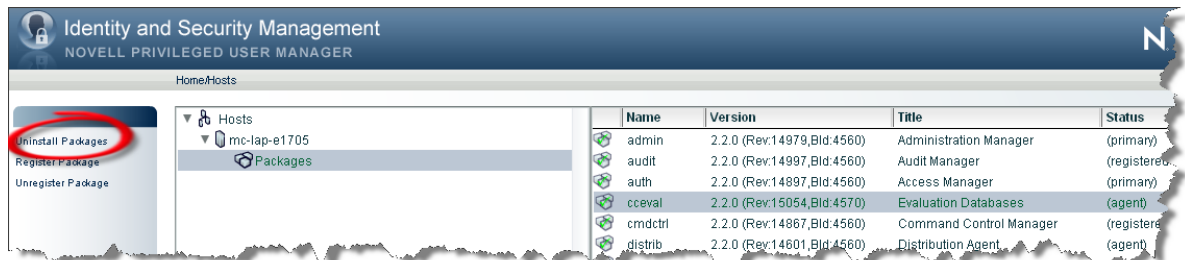
Uninstalling the evaluation database package will restore your previously backed up configuration. Please note that any configuration changes or captured events generated with the evaluation package installed will be permanently removed.

Note also that the evaluation environment can be 'refreshed' at any time simply by uninstalling and reinstalling the evaluation package.

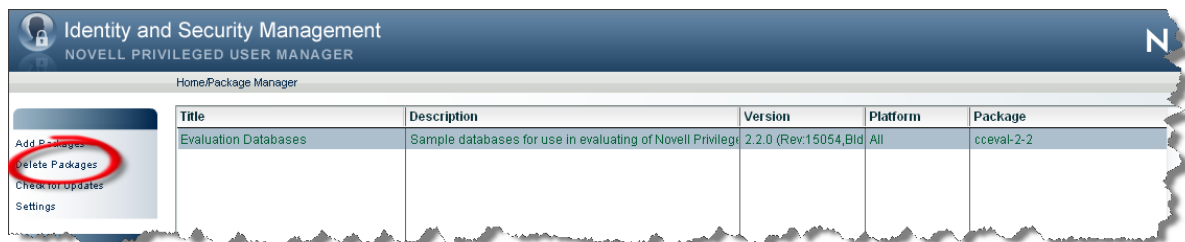
### Recommendation

When you have finished your evaluation, we strongly recommend that you perform the following steps:

Uninstall the evaluation and restore your original configuration through the host console by clicking the evaluation package, then selecting the 'Uninstall Package' option from the left-hand menu (as below).



Remove the evaluation package from the Package Manager by clicking the package and selecting the 'Delete Packages' option from the left-hand menu (as below).





## 2.1 Install Std Manager Package

Copy the evaluation package appropriate for your platform to a temporary location on the machine that will be used for testing, and install according to the following instructions.

Note: By default the installation will install the software into /opt/novell.

### 2.1.1 AIX Manager Install

The AIX installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into /opt/novell. To change this, create a directory in the required part of the file system and create a symbolic link to /opt/novell.

To install the AIX manager:

1. Copy the installation package to a temporary location and use the following command to extract the installation files:

```
gunzip novell-npum-manager-X.X-aix-X.X-powerpc.bff.gz
```

2. After the AIX installation package is uncompressed, use one of the following methods to perform the installation.

- o The AIX smitty program
- o The following command:

```
installp -acgNQqwX -d <directory of .bff file> novellnpum
```

3. After installation is complete, check that the service is running by viewing the log file. The log file is located in /opt/novell/npum/logs/unifid.log, if the default install location was used.

You should see an output similar to the following:

```
=====
Version 2.2.0 (Rev:14967,Bld:4550) [aix-5.1-powerpc]
Database Version 3.5.7
[admin 2.2.0 (Rev:14979,Bld:4550) ] module loaded
[audit 2.2.0 (Rev:14937,Bld:4550) ] module loaded
[auth 2.2.0 (Rev:14897,Bld:4550) ] module loaded
[cmdctrl 2.2.0 (Rev:14867,Bld:4550) ] module loaded
[distrib 2.2.0 (Rev:14601,Bld:4550) ] module loaded
[msggagnt 2.2.0 (Rev:14842,Bld:4550) ] module loaded
[pkgman 2.2.0 (Rev:14972,Bld:4550) ] module loaded
[regclnt 2.2.0 (Rev:14845,Bld:4550) ] module loaded
[registry 2.2.0 (Rev:14926,Bld:4550) ] module loaded
[rexec 2.2.0 (Rev:14949,Bld:4550) ] module loaded
[secaudit 2.2.0 (Rev:14793,Bld:4550) ] module loaded
[strfwd 2.2.0 (Rev:14872,Bld:4550) ] module loaded
Service listening on 0.0.0.0:29120
Service listening on 0.0.0.0:443
Checking service registration for ussm-aixv1 (ussm-aixv1)
valid from Mon Mar 09 16:34:59 2009 to Mon Apr 06 17:34:59 2009 (registry offset 0 seconds)
```



## 2.1.2 HP-UX Framework Manager Install

The HP-UX installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into /opt/novell. To change this, create a directory in the required part of the file system and create a symbolic link to /opt/novell.

To install the HP-UX manager:

1. Copy the installation package to a temporary location and use the following command to extract the installation files:

For HP/PA:

```
gunzip novell-npum-manager-X.X-hpux-X.X-hppa.depot.gz
```

For ITA:

```
gunzip novell-npum-manager-X.X-hpux-X.X-ia64.depot.gz
```

2. After the HP-UX installation package is uncompressed, use the following command to install the manager:

For HP/PA:

```
swinstall -s /<directory of .depot file>/novell-npum-manager-X.X-hpux-X.X-hppa.depot \*
```

For ITA:

```
swinstall -s /<directory of .depot file>/novell-npum-manager-X.X-hpux-X.X-ia64.depot \*
```

3. After installation is complete, check that the service is running by viewing the log file. The log file is located in /opt/novell/npum/logs/unifid.log, if the default install location was used.

You should see an output similar to the following:

```
=====
Version 2.2.0 (Rev:14967,Bld:4552) [hpux-11.23-ia64]
Database Version 3.5.7
[admin 2.2.0 (Rev:14979,Bld:4552) ] module loaded
[audit 2.2.0 (Rev:14937,Bld:4552) ] module loaded
[auth 2.2.0 (Rev:14897,Bld:4552) ] module loaded
[cmdctrl 2.2.0 (Rev:14867,Bld:4552) ] module loaded
[distrib 2.2.0 (Rev:14601,Bld:4552) ] module loaded
[msgagnt 2.2.0 (Rev:14842,Bld:4552) ] module loaded
[pkgman 2.2.0 (Rev:14972,Bld:4552) ] module loaded
[regclnt 2.2.0 (Rev:14845,Bld:4552) ] module loaded
[registry 2.2.0 (Rev:14926,Bld:4552) ] module loaded
[rexec 2.2.0 (Rev:14949,Bld:4552) ] module loaded
[secaudit 2.2.0 (Rev:14793,Bld:4552) ] module loaded
[strfwd 2.2.0 (Rev:14872,Bld:4552) ] module loaded
Service listening on 0.0.0.0:29120
Service listening on 0.0.0.0:443
Checking service registration for ussm-hpuxv1 (ussm-hpuxv1)
valid from Mon Mar 09 16:31:49 2009 to Mon Apr 06 17:31:49 2009 (registry offset 0 seconds)
```



## 2.1.3 Linux Framework Manager Install

Linux hosts use the RPM packaging system for installation, upgrade, and removal.

By default, the installation program installs the software into /opt/novell. To change this, create a directory in the required part of the file system and create a symbolic link to /opt/novell.

To install the Linux manager:

1. Run the following command:

```
rpm -i novell-npum-manager-X.X-linux-X.X-intel.rpm
```

2. After installation is complete, check that the service is running by viewing the log file. The log file is located in /opt/novell/npum/logs/unifid.log, if the default install location was used.

You should see an output similar to the following:

```
=====  
Version 2.2.0 (Rev:14967,Bld:4552) [linux-2.6-intel]  
Database Version 3.5.7  
[admin 2.2.0 (Rev:14979,Bld:4552) ] module loaded  
[audit 2.2.0 (Rev:14937,Bld:4552) ] module loaded  
[auth 2.2.0 (Rev:14897,Bld:4552) ] module loaded  
[cmdctrl 2.2.0 (Rev:14867,Bld:4552) ] module loaded  
[distrib 2.2.0 (Rev:14601,Bld:4552) ] module loaded  
[msgagnt 2.2.0 (Rev:14842,Bld:4552) ] module loaded  
[pkgman 2.2.0 (Rev:14972,Bld:4552) ] module loaded  
[regclnt 2.2.0 (Rev:14845,Bld:4552) ] module loaded  
[registry 2.2.0 (Rev:14926,Bld:4552) ] module loaded  
[rexec 2.2.0 (Rev:14949,Bld:4552) ] module loaded  
[secaudit 2.2.0 (Rev:14793,Bld:4552) ] module loaded  
[strfwd 2.2.0 (Rev:14872,Bld:4552) ] module loaded  
Service listening on 0.0.0.0:29120  
Service listening on 0.0.0.0:443  
Checking service registration for ussm-lin1 (ussm-lin1)  
valid from Mon Mar 09 18:18:27 2009 to Mon Apr 06 19:18:27 2009 (registry offset 0 seconds)
```



## 2.1.4 Solaris Framework Manager Install

The Solaris installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into /opt/novell. To change this, create a directory in the required part of the file system and create a symbolic link to /opt/novell.

To install the Solaris manager:

1. Copy the installation package to a temporary location and use the following command to extract the installation files:

For SPARC:

```
gunzip novell-npum-manager-X.X-solaris-X.X-sparc.pkg.gz
```

For Intel:

```
gunzip novell-npum-manager-X.X-solaris-X.X-intel.pkg.gz
```

2. After the Solaris installation package is uncompressed, use the following command to install the manager:

For SPARC:

```
pkgadd - d /<directory of .pkg file>/novell-npum-manager-X.X-solaris-X.X-sparc.pkg
```

For Intel:

```
pkgadd - d /<directory of .pkg file>/novell-npum-manager-X.X-solaris-X.X-intel.pkg
```

3. After installation is complete, check that the service is running by viewing the log file. The log file is located in /opt/novell/npum/logs/unifid.log, if the default install location was accepted.

You should see an output similar to the following:

```
=====
Version 2.2.0 (Rev:14967,Bld:4552) [solaris-2.10-sparc]
Database Version 3.5.7
[admin 2.2.0 (Rev:14979,Bld:4552) ] module loaded
[audit 2.2.0 (Rev:14937,Bld:4552) ] module loaded
[auth 2.2.0 (Rev:14897,Bld:4552) ] module loaded
[cmdctrl 2.2.0 (Rev:14867,Bld:4552) ] module loaded
[distrib 2.2.0 (Rev:14601,Bld:4552) ] module loaded
[msggagt 2.2.0 (Rev:14842,Bld:4552) ] module loaded
[pkgman 2.2.0 (Rev:14972,Bld:4552) ] module loaded
[regclnt 2.2.0 (Rev:14845,Bld:4552) ] module loaded
[registry 2.2.0 (Rev:14926,Bld:4552) ] module loaded
[rexec 2.2.0 (Rev:14949,Bld:4552) ] module loaded
[secaudit 2.2.0 (Rev:14793,Bld:4552) ] module loaded
[strfwd 2.2.0 (Rev:14872,Bld:4552) ] module loaded
Service listening on 0.0.0.0:29120
Service listening on 0.0.0.0:443
Checking service registration for ussm-solv1 (ussm-solv1)
valid from Mon Mar 09 17:24:28 2009 to Mon Apr 06 18:24:28 2009 (registry offset 0 seconds)
```





## 2.1.5 Tru64 Framework Manager Install

The Tru64 installation package is compressed through gzip. In order to install the package, you must unzip the package through gunzip.

By default, the installation program installs the software into /opt/novell. To change this, create a directory in the required part of the file system and create a symbolic link to /opt/novell.

To install the Tru64 manager:

1. Copy the installation package to a temporary location and use the following command to extract the installation files:

```
gunzip novell-npum-manager-X.X-tru64-X.X-alpha.tar.gz
tar -xvf novell-npum-manager-X.X-tru64-X.X-alpha.tar
```

2. After the Tru64 installation package is uncompressed, use the following command to install the manager:

```
setld -l NOVELLNPM/
```

3. After installation is complete, check that the service is running by viewing the log file. The log file is located in /opt/novell/npum/logs/unifid.log, if the default install location was used.

You should see an output similar to the following:

```
=====
Version 2.2.0 (Rev:14967,Bld:4551) [tru64-5.1-alpha]
Database Version 3.5.7
[admin 2.2.0 (Rev:14979,Bld:4551) ] module loaded
[audit 2.2.0 (Rev:14937,Bld:4551) ] module loaded
[auth 2.2.0 (Rev:14897,Bld:4551) ] module loaded
[cmdctrl 2.2.0 (Rev:14867,Bld:4551) ] module loaded
[distrib 2.2.0 (Rev:14601,Bld:4551) ] module loaded
[msgagnt 2.2.0 (Rev:0,Bld:4551) ] module loaded
[pkgman 2.2.0 (Rev:14972,Bld:4551) ] module loaded
[regclnt 2.2.0 (Rev:14845,Bld:4551) ] module loaded
[rexec 2.2.0 (Rev:14949,Bld:4551) ] module loaded
[registry 2.2.0 (Rev:14926,Bld:4551) ] module loaded
[secaudit 2.2.0 (Rev:0,Bld:4551) ] module loaded
[strfwd 2.2.0 (Rev:14872,Bld:4551) ] module loaded
Service listening on 0.0.0.0:29120
Service listening on 0.0.0.0:443
Checking service registration for ussm-truv1 (ussm-truv1)
valid from Mon Mar 09 16:42:59 2009 to Mon Apr 06 17:42:59 2009 (registry off
set 0 seconds)
```



## 2.1.6 Windows Framework Manager Install

1. Run the following install executable to start the installation:

```
novell-npum-manager-X.X-windows-5.0-intel.exe
```

2. Follow the steps in the install wizard.

The Framework Manager service can be installed on any part of the normal file system. It defaults to the C:\Program Files\Novell\npum folder.

3. After installation is complete, check that the service is running by viewing the log file. The log file is located in C:\Program Files\Novell\npum\logs\unifid.log, if the default install location was used.

You should see an output similar to the following:

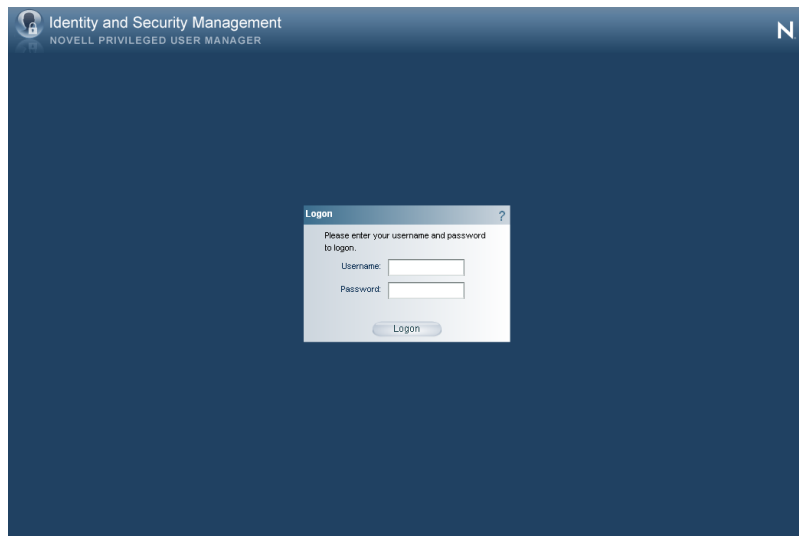
```
=====
Version 2.2.0 (Rev:14967,Bld:4554) [windows-5.0-intel]
Database Version 3.5.7
Parent (1508) starting child
=====
Version 2.2.0 (Rev:14967,Bld:4554) [windows-5.0-intel]
Database Version 3.5.7
Child (1520) main thread starting
[admin 2.2.0 (Rev:14979,Bld:4554) ] module loaded
[audit 2.2.0 (Rev:14937,Bld:4554) ] module loaded
[auth 2.2.0 (Rev:14897,Bld:4554) ] module loaded
[cmdctrl 2.2.0 (Rev:14867,Bld:4554) ] module loaded
[distrib 2.2.0 (Rev:14601,Bld:4554) ] module loaded
[msggagt 2.2.0 (Rev:14842,Bld:4554) ] module loaded
[pkgman 2.2.0 (Rev:14972,Bld:4554) ] module loaded
[regclnt 2.2.0 (Rev:14845,Bld:4554) ] module loaded
[registry 2.2.0 (Rev:14926,Bld:4554) ] module loaded
[secaudit 2.2.0 (Rev:14793,Bld:4554) ] module loaded
[strfwd 2.2.0 (Rev:14872,Bld:4554) ] module loaded
Service listening on 0.0.0.0:29120
Service listening on 0.0.0.0:443
Checking service registration for ussm-winv1 (ussm-winv1)
valid from Tue Mar 10 11:12:34 2009 to Tue Apr 07 12:12:34 2009 (registry offset 0 seconds)
```

## 2.2 Log on and Set Administrator Password

### Log on to the Novell Privileged User Manager Administration console

In a browser with access to test machine, enter: <https://testmachinename>

**Note:** When prompted, accept security certificate



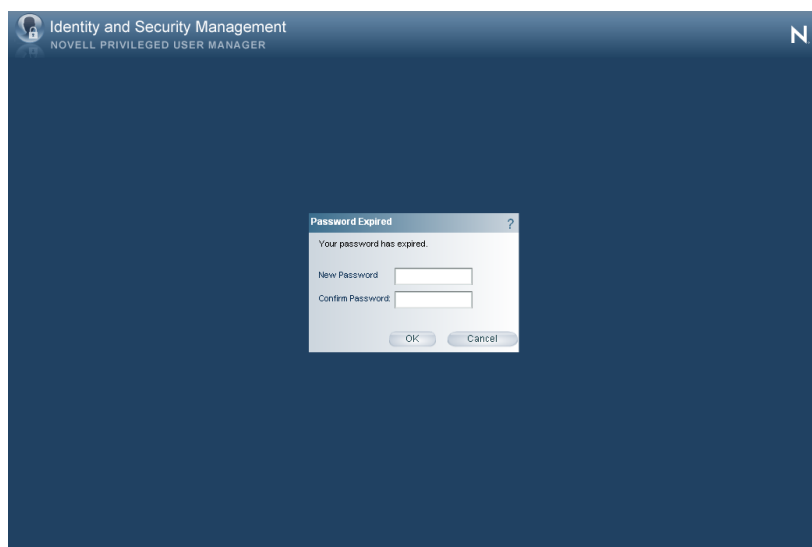
On first use, click through the license screen and enter the default credentials of:

Username: admin

Password: novell

### Change password

You will be prompted to change your password: (minimum of 6 characters, 1 alpha and 1 numeric)



## 2.3 Load and Install Evaluation Databases

### 2.3.1 Load Evaluation Installer

#### UNIX/Linux

Copy the evaluation installer file “cceval-2-2.pak” to a temporary location on your server.

Change to that directory and issue the following command to load the installer into your Framework Package Manager.

```
/opt/novell/npum/sbin/unifi -u admin distrib publish -f cceval-2-2.pak
```

Note: You will be prompted for the administration password you set in section 2.2

#### Windows

Copy the evaluation installer file “cceval-2-2.pak” to a temporary location on your server.

Change to that directory and issue the following command to load the installer into your Framework Package Manager.

```
“C:\Program Files\Novell\Npum\bin\unifi” -u admin distrib publish -f cceval-2-2.pak
```

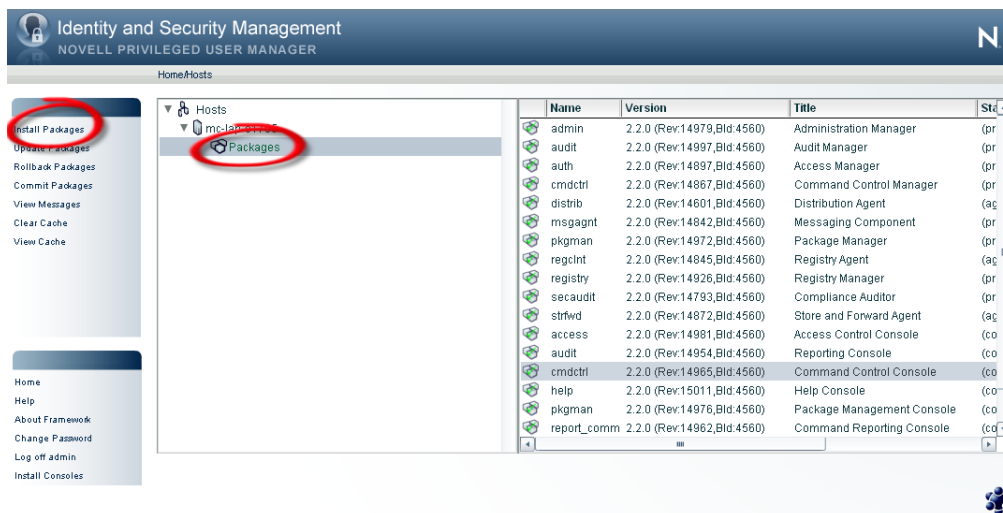
Note: You will be prompted for the administration password you set in section 2.2

### 2.3.2 Install Evaluation Databases to Host

Log onto the Administration Console and select the **Hosts** option.

Expand the hostname of your machine as shown below and then click on **Packages**.

Now select **Install Packages** from the left-hand menu



The screenshot shows the Administration Console interface for Identity and Security Management. The left-hand menu has "Install Packages" circled in red. The main area shows a tree view under "Hosts" with "Packages" circled in red. A table of installed packages is displayed on the right.

Name	Version	Title	Std
admin	2.2.0 (Rev:14979,Bld:4560)	Administration Manager	(pr
audit	2.2.0 (Rev:14997,Bld:4560)	Audit Manager	(pr
auth	2.2.0 (Rev:14897,Bld:4560)	Access Manager	(pr
cmdctrl	2.2.0 (Rev:14867,Bld:4560)	Command Control Manager	(pr
distrib	2.2.0 (Rev:14601,Bld:4560)	Distribution Agent	(ag
msgagnt	2.2.0 (Rev:14842,Bld:4560)	Messaging Component	(pr
pkgman	2.2.0 (Rev:14972,Bld:4560)	Package Manager	(pr
regclnt	2.2.0 (Rev:14845,Bld:4560)	Registry Agent	(ag
registry	2.2.0 (Rev:14926,Bld:4560)	Registry Manager	(pr
secaudit	2.2.0 (Rev:14793,Bld:4560)	Compliance Auditor	(pr
strfwd	2.2.0 (Rev:14872,Bld:4560)	Store and Forward Agent	(ag
access	2.2.0 (Rev:14981,Bld:4560)	Access Control Console	(co
audit	2.2.0 (Rev:14954,Bld:4560)	Reporting Console	(co
cmdctrl	2.2.0 (Rev:14965,Bld:4560)	Command Control Console	(co
help	2.2.0 (Rev:15011,Bld:4560)	Help Console	(co
pkgman	2.2.0 (Rev:14976,Bld:4560)	Package Management Console	(co
report_comm	2.2.0 (Rev:14962,Bld:4560)	Command Reporting Console	(co



Now select the **Evaluation Databases** package as shown below and click **Next**

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Install Package

Title	Description	Version	Package
Evaluation Databases	Sample databases for use in evaluating of Novell Privileged User	2.2.0 (Rev:15054,Bld:4570)	cceval-2-2

Next > Cancel

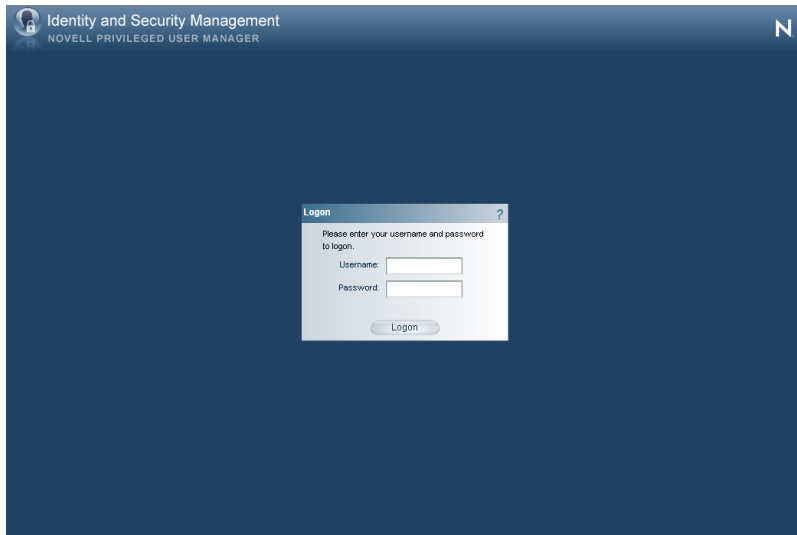
When the install is complete, return to the main menu by clicking **Home** in the breadcrumb trail, (underneath the title-bar at the top) to complete the remaining exercises in this guide.

## 3.0 Initial Orientation

### Log on to the Novell Privileged User Manager administration console

In a browser with access to test machine, enter: <https://testmachinename>

**Note:** When prompted, accept security certificate



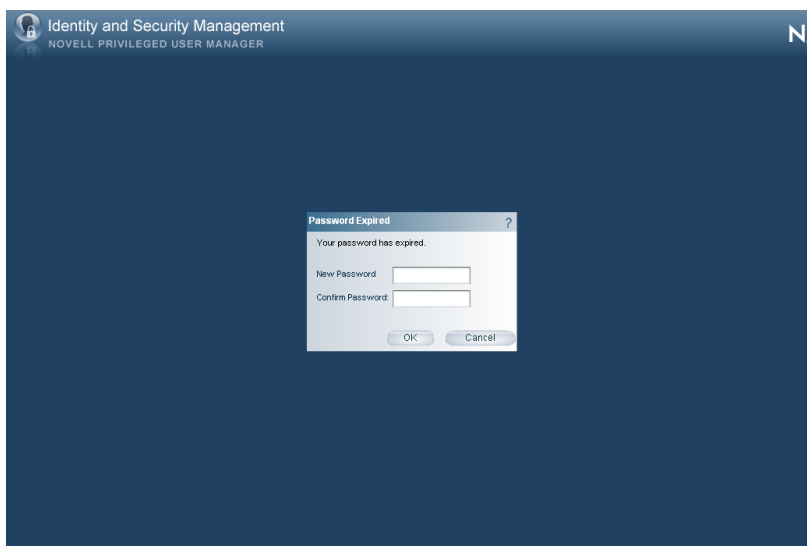
If first use, click through the license screen and enter the default credentials of:

Username: admin

Password: novell

### Change password

If first use, you will be prompted to change your password.





**Orientation: Home Menu**

The Home menu is where you are able to access the individual administrative ‘consoles’ that are installed as part of your solution.

The screenshot shows the 'Identity and Security Management' interface for 'NOVELL PRIVILEGED USER MANAGER'. The main menu includes 'Home', 'Reporting', 'Compliance Auditor', 'Hosts', 'Package Manager', 'Command Control', and 'Framework User Manager'. A left sidebar contains 'Home', 'Help', 'About Framework', 'Change Password', 'Log off admin', and 'Install Consoles'. Six yellow callout boxes provide details:

- Compliance Auditor:** Proactive auditing tool that pulls events from the event logs, according to predefined rules, for analysis.
- Hosts:** Centrally manage application installation and update, load-balancing / redundancy of resources, and host alerting.
- Command Control:** Manage security policies for privilege management using an intuitive GUI interface.
- Framework User Manager:** Manage users that will log onto the admin console using role-based grouping.
- Reporting:** Easily access and search event logs, review user keystroke activity, color-coded through our unique Command-Risk Analysis Engine.
- Package Manager:** Any module can be easily updated via connection to an online update server and pushed out to hosts.

**NOTE**

The administration console is Adobe Flash-driven and requires only a single click to select menu options.

**IMPORTANT:**

To navigate when in the administration console, DO NOT use your browsers' forward or back buttons; use the 'breadcrumb trail' at the top of each page, for example:

“Home / Compliance Auditor” – click on **Home** to return to main console menu



**Orientation: Compliance Auditor**

From the Home menu, select the Compliance Auditor console

Each event record is color-coded according to the highest rated command risk (see below).

New: Events have not been examined  
Pending: Examination in progress  
Authorized: Activity has been signed off as okay  
Unauthorized: Activity not acceptable

Filters can be set on combination of date range and event status.

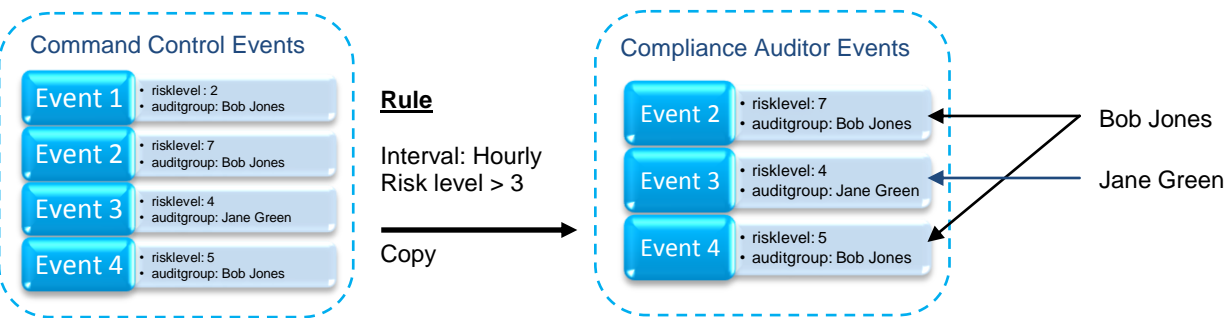
Level	Status	Time	Event	Note
0	New	10 Jun 2008 10:08:40	cusr1@fedvm3 /usr/bin/ksh as cusr1@fedvm3	
0	New	10 Jun 2008 10:11:13	tusr1@fedvm1 id as root@fedvm1	
0	New	10 Jun 2008 10:11:20	tusr1@fedvm1 ls -l as tusr1@fedvm1	
0	New	10 Jun 2008 10:12:14	tusr1@fedvm3 id as root@fedvm3	
0	New	10 Jun 2008 10:12:18	tusr1@fedvm3 ls -l as tusr1@fedvm3	
0	New	10 Jun 2008 10:12:27	tusr2@fedvm1 id as tusr2@fedvm1	
0	New	10 Jun 2008 10:12:31	tusr2@fedvm1 ls -l as root@fedvm1	
0	New	10 Jun 2008 10:12:40	tusr2@fedvm3 id as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:43	tusr2@fedvm3 ls -l as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:59	rusr1@fedvm1 /usr/bin/rush -o audit 1 as root@fedvm1	

Note: Events containing keystroke activity through the 'rush' shell are colored according to risk, ranging from Green (low) to Red (high).

Event escalation level (manually set)

Context sensitive menus provide access to the rules that pull events into the Compliance Auditor, and to automated workflow email management.

The Compliance Auditor makes copies of events according to predefined rules. Command Control events can be tagged with an 'Audit Group' to ensure that users can only view events appropriate to their role. In the example below, only events with a risk rating greater than 3 are copied over each hour. When logged in, Bob Jones can only see events in his Audit Group, likewise with Jane Green.








## Orientation: Reporting

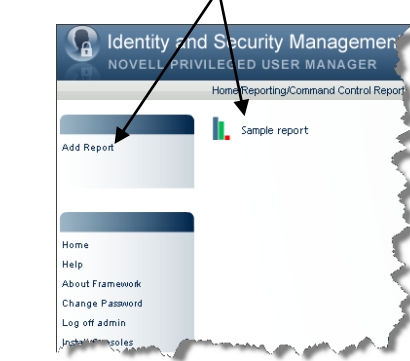
From the Home Menu, select the Reporting Console

**Global settings such as log file rollover and encryption settings.**



**Icon is shown for accessing Command Control activity logs**

**Many reports with custom filters can be created and stored for reuse.**



**Select log files to be used for the report**

**Create custom filters based on submituser, runuser, host, command string or date**

**Change name or description of report**

**Delete Report**

**Activity Report**

Keystroke Replay

---

Home

Help

About Framework

Change Password

Log off admin

Install Consoles

Home/Reporting/Command Control Reports/Sample report

Report Data
LogFiles
Filter
General

Time	User	Host	RunAs	RunHost	Command	Authorized	Capture	Audit Status	Audit ID
Tue Jun 10 10:08:40	cust1	fedvm3	cust1	fedvm3	/usr/bin/ksh	yes	yes		7492888
Tue Jun 10 10:11:13	tusr1	fedvm1	root	fedvm1	id	yes	no		760b158
Tue Jun 10 10:11:20	tusr1	fedvm1	tusr1	fedvm1	ls -l	no	no		4bd266c
Tue Jun 10 10:12:14	tusr1	fedvm3	root	fedvm3	id	yes	no		ba8df33c
Tue Jun 10 10:12:18	tusr1	fedvm3	tusr1	fedvm3	ls -l	no	no		270e87fe
Tue Jun 10 10:12:27	tusr2	fedvm1	tusr2	fedvm1	id	no	no		8e55d9d
Tue Jun 10 10:12:31	tusr2	fedvm1	root	fedvm1	ls -l	yes	yes		7ab0b65
Tue Jun 10 10:12:40	tusr2	fedvm3	tusr2	fedvm3	id	no	no		ac79ef3b
Tue Jun 10 10:12:43	tusr2	fedvm3	tusr2	fedvm3	ls -l	no	no		98b6312
Tue Jun 10 10:12:59	tusr1	fedvm1	root	fedvm1	/usr/bin/rush -	yes	yes		a7610cf5

Apply
Reset

**If an event is highlighted that contains a keystroke report, the keystroke player can be launched.**



**Orientation: Hosts**

From the Home Menu, select the Hosts Console

Context sensitive menu provides options for module updates and maintenance on a single host, or group

When a host is selected, its status is displayed in the right-hand pane.

Name	Value
Agent name	usma-vfc1
Host name	usma-vfc1
Host port	29120
Platform	linux
Processor	intel
OS Version	2.6
Agent version	2.2.0 (Rev:14967,Bld:4555)
System time	Sun Mar 15 21:35:21 2009 UTC
Service uptime	55 mins 25 secs
Active sessions	1
Active tasks	1
Installation path	/opt/novell/npum
Disk space	Total size: 3.24GB Available: 1.77GB Capacity: 45.25%
Memory (approx)	7.20MB
Registration	Unlicensed (usma-vfc1) from: Sun Mar 15 17:21:17 2009
Status	online

Clicking on Packages, displays the application modules installed on the host.

Name	Version	Title
admin	2.2.0 (Rev:14979,Bld:4555)	Administration Manager
audit	2.2.0 (Rev:14937,Bld:4555)	Audit Manager
auth	2.2.0 (Rev:14897,Bld:4555)	Access Manager
cmdctrl	2.2.0 (Rev:14867,Bld:4555)	Command Control Mana
distrib	2.2.0 (Rev:14601,Bld:4555)	Distribution Agent
msgagnt	2.2.0 (Rev:14842,Bld:4555)	Messaging Component
pkgman	2.2.0 (Rev:14972,Bld:4555)	Package Manager
regclnt	2.2.0 (Rev:14845,Bld:4555)	Registry Agent
registry	2.2.0 (Rev:14926,Bld:4555)	Registry Manager
rexc	2.2.0 (Rev:14949,Bld:4555)	Command Control Agent
secaudit	2.2.0 (Rev:14793,Bld:4555)	Compliance Auditor
strfwd	2.2.0 (Rev:14872,Bld:4555)	Store and Forward Agent
cmdctrl	2.2.0 (Rev:14965,Bld:4555)	Command Control Cons
secaudit	2.2.0 (Rev:14954,Bld:4555)	Compliance Auditor Con
report_comm	2.2.0 (Rev:14962,Bld:4555)	Command Reporting Co
access	2.2.0 (Rev:14981,Bld:4555)	Access Control Console
pkgman	2.2.0 (Rev:14976,Bld:4555)	Package Management C

New packages can be installed to the host when you click on Packages, or deleted if a module is selected in the right-hand pane.

Each application module's status and version information can be reviewed in the right-hand pane.



**Orientation: Package Manager**

From the Home Menu, select the Package Manager Console

New packages can be downloaded directly into the local Package Manager if the host is capable of supporting an http internet connection.

Once applications have been downloaded and deployed, a single click checks for available updates.

The screenshot shows the 'Identity and Security Management' console for 'NOVELL PRIVILEGED USER MANAGER'. The breadcrumb path is 'Home/Package Manager'. On the left, there is a navigation menu with options: Add Packages, Delete Packages, Check for Updates, Settings, Home, Help, About Framework, Change Password, Log off admin, and Install Consoles. The main area displays a table of installed packages.

Title	Description	Version	Platform	Pack
Access Control Console	Novell Privileged User Manager Access Control	2.2.0 (Rev:14981,Bld	All	acce
Agent Console	Novell Privileged User Manager Agent Management	2.2.0 (Rev:14964,Bld	All	serv
Command Control Console	Provides access to commands without giving full root acc	2.2.0 (Rev:14965,Bld	All	cmd
Command Reporting Console	Novell Privileged User Manager Command Reporting Cor	2.2.0 (Rev:14962,Bld	All	repo
Compliance Auditor Console	Provides compliance auditing	2.2.0 (Rev:14954,Bld	All	secc
Help Console	Provides help for the Novell Privileged User Manager prod	2.2.0 (Rev:15007,Bld	All	help
Package Management Console	Novell Privileged User Manager Package Management	2.2.0 (Rev:14976,Bld	All	pkgr
Reporting Console	Novell Privileged User Manager Audit Reporting	2.2.0 (Rev:14954,Bld	All	audi
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	windows	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	hpux [ia64] (11.23	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	aix [powerpc] (4.3	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	linux [intel] (2.4)	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	hpux [hppa] (11.0	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	tru64 [alpha] (5.0)	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	solaris [sparc] (2.	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	aix [powerpc] (5.1	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	solaris [sparc] (2.	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	tru64 [alpha] (4.0)	auth
Access Manager	Provides Framework authentication	2.2.0 (Rev:14897,Bld	solaris [intel] (2.0)	auth

An account is required to connect to Novell's update servers, these credentials together with optional proxy server information are entered under Settings.

All packages available for deployment are listed together with platform and version information.

**Note**

When first accessing the Package Manager console, the application module list will be blank. This special evaluation version of the product has application modules preinstalled for your test host. You have the option of downloading additional modules as an exercise later in this guide.

**Orientation: Command Control**

From the Home Menu, select the Command Control Console

Privilege management policies are created by dragging 'trigger' objects such as user groups and commands into rules that determine whether a submitted command is authorized to run and with what parameters, such as runuser account, keystroke logging etc.

Home/Command Control

Command Control

Import Samples  
Import Settings  
Export Settings  
Test Suites  
Commit Transaction  
Cancel Transaction  
Transaction Settings  
Audit Settings

Home  
Help  
About Framework  
Change Password  
Log off admin  
Install Consoles

Rules  
Account Groups  
Commands  
Scripts  
Access Times  
Reports

Import or export your configuration settings, organize and run test suites, and configure built-in change management functions for audit of administrative activities.

Clicking on each group in the tree displays member objects in the right-hand pane.

Home/Command Control

Add Rule  
Modify Rule  
Find Rule  
Delete Rules  
Script Arguments  
Pseudocode

Home  
Help  
About Framework  
Change Password  
Log off admin  
Install Consoles

Rules  
Allow id command as Root  
Allow Is -l command as Root  
Crush shell login with Session Capture  
Full root session with rush

Account Groups  
Commands  
Scripts  
Access Times  
Reports

IF (user IN Is -l command user group AND host IN Is -l commar)

- Authorize: yes
- Session Capture: yes
- runUser = "root"
- Stop if authorized

When the rule is executed, these are the parameters under which the command will be run.

When a rule is selected in the tree, current options are displayed in the right-hand pane. Double-clicking the rule name allows settings such as runuser and session capture to be set.

Command Control Manager: usma-vfc1

Clicking Pseudocode displays rule logic in a clear color-coded Boolean format.



**Orientation: Manage Users**

From the Home Menu, select the Framework User Manager Console

Specific account information can be set for individual users or globally for all users.

## 4.0 Step by Step Exercises

### Reviewing keystroke activity proactively

- a) Select the Compliance Auditor Console from the Home Menu



- b) Notice the events that have been pulled from the Command Control event logs.

Level	Status	Time	Event	Note
0	New	10 Jun 2008 10:08:40	cusr1@fedvm3 /usr/bin/ksh as cusr1@fedvm3	
0	New	10 Jun 2008 10:11:13	tusr1@fedvm1 id as root@fedvm1	
0	New	10 Jun 2008 10:11:20	tusr1@fedvm1 ls -l as tusr1@fedvm1	
0	New	10 Jun 2008 10:12:14	tusr1@fedvm3 id as root@fedvm3	
0	New	10 Jun 2008 10:12:18	tusr1@fedvm3 ls -l as tusr1@fedvm3	
0	New	10 Jun 2008 10:12:27	tusr2@fedvm1 id as tusr2@fedvm1	
0	New	10 Jun 2008 10:12:31	tusr2@fedvm1 ls -l as root@fedvm1	
0	New	10 Jun 2008 10:12:40	tusr2@fedvm3 id as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:43	tusr2@fedvm3 ls -l as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:59	tusr1@fedvm1 /usr/bin/rush -o audit 1 as root@fedvm1	

Note: The color coding comes from Privilege User Managers' unique Command-Risk Analysis engine, each command typed and associated session event is colored according to the following matrix:

Risk	Regex	Command
9	Yes	(^/)/reboot\$
9	Yes	(^/)/shutdown([[:space:]] \$)
8	Yes	(^/)/kill([[:space:]] )
8	Yes	(^/)/rm([[:space:]] )
7	Yes	(^/)/vi([[:space:]] \$)
6	Yes	(^/)/passwd([[:space:]] \$)
6	Yes	(^/)/usvi([[:space:]] \$)
5	Yes	(^/)/chown([[:space:]] )
5	Yes	(^/)/cp([[:space:]] )
5	Yes	(^/)/chmod([[:space:]] )
4	Yes	(^/)/mv([[:space:]] )



c) Double-click the record colored red

The screenshot shows the 'Identity and Security Management' interface for 'NOVELL PRIVILEGED USER MANAGER'. The page title is 'Home/Compliance Auditor'. There are filters for 'New', 'Pending', 'Authorized', and 'Unauthorized'. The date range is set to '15 Mar 2009 19:25' to '15 Mar 2009 19:25'. A table of records is displayed with columns: Level, Status, Time, Event, and Note. The last record is highlighted in red and has a red box around it with the text 'Click Here' and a mouse cursor pointing to it.

Level	Status	Time	Event	Note
0	New	10 Jun 2008 10:08:40	cusr1@fedvm3 /usr/bin/ksh as cusr1@fedvr	
0	New	10 Jun 2008 10:11:13	tusr1@fedvm1 id as root@fedvm1	
0	New	10 Jun 2008 10:11:20	tusr1@fedvm1 ls -l as tusr1@fedvm1	
0	New	10 Jun 2008 10:12:14	tusr1@fedvm3 id as root@fedvm3	
0	New	10 Jun 2008 10:12:18	tusr1@fedvm3 ls -l as tusr1@fedvm3	
0	New	10 Jun 2008 10:12:27	tusr2@fedvm1 id as tusr2@fedvm1	
0	New	10 Jun 2008 10:12:31	tusr2@fedvm1 ls -l as root@fedvm1	
0	New	10 Jun 2008 10:12:40	tusr2@fedvm3 id as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:43	tusr2@fedvm3 ls -l as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:59	rusr1@fedvm1 /usr/bin/rush -o audit 1 as root	

You will see that it is not currently possible to edit the record and that icon bottom right is grayed out.

The screenshot shows the 'View Record' page for the selected record. The page title is 'Home/Compliance Auditor/View Record'. The record details are as follows:

Time	10 Jun 2008 10:12:59	Event ID	a7610cf5-7952-47fd-906c-27882452b61f
User	rusr1	Host	fedvm1
RunAs	root	RunHost	fedvm1
Command	/usr/bin/rush -o audit 1		
Authorized	Yes	Captured	Yes
Status	<input type="radio"/> New	Assigned To	
Note			
History			

At the bottom right, there are two icons: 'Keystroke' and 'Edit Record'. The 'Edit Record' icon is circled in red.

d) Please double-click the icon marked Keystroke (or 'View Keystroke Report' in menu).

The keystroke replay is displayed for the event, please see below for descriptions.

Each line is color-coded according to command risk.

Stdin

Stdout

Identity and Security Management

NOVELL PRIVILEGED USER MANAGER

N

Command Control Keystroke Report

Input
  Output

Time	Standard Input
10 Jun 2008 10:13:02	id[CR]
10 Jun 2008 10:13:13	uname -a[CR]
10 Jun 2008 10:13:16	whoami[CR]
10 Jun 2008 10:13:22	passwd[CR]
10 Jun 2008 10:13:33	cd /etc[CR]
10 Jun 2008 10:13:38	more passwd[CR]
10 Jun 2008 10:13:51	cp /etc/passwd /tmp/file1 [CR]
10 Jun 2008 10:13:55	cd /tmp[CR]
10 Jun 2008 10:14:00	ls -l[CR]
10 Jun 2008 10:14:10	ksh[CR]
10 Jun 2008 10:14:16	vi file1[CR]
10 Jun 2008 10:14:34	[KCUD1][KCUD1][KCUD1]dddddddddoohis is a test[ESC]Zzm -rf file1[CR]
10 Jun 2008 10:14:38	ls -l[CR]
10 Jun 2008 10:14:41	cd /[CR]
10 Jun 2008 10:14:50	telnet □□□□□□ssh fedvm3[CR]
10 Jun 2008 10:14:52	yes[CR]
10 Jun 2008 10:14:54	xxxxxx[CR]
10 Jun 2008 10:15:00	id[CR]
10 Jun 2008 10:15:03	exit[CR]
10 Jun 2008 10:15:14	reboot[CR]

Terminal Type: vt100

Audit Manager: usma-vc1

vt100

Find

Show control characters  
 Show audited commands  
 Show profile commands

Refresh

Cancel

Decryption key

Terminal type is auto selected but can be manually overridden from a list

Any string can be searched for within the keystroke log

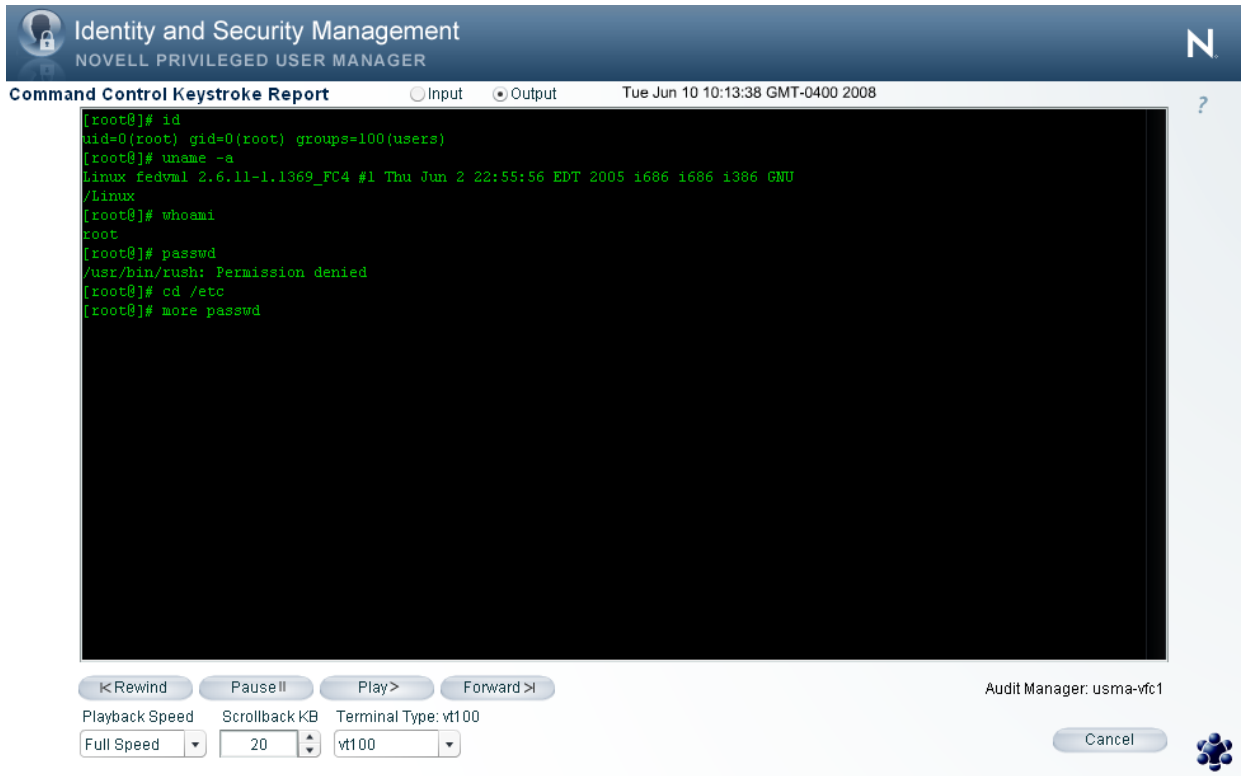
Please toggle the checkboxes for 'Show control characters' and 'Show audited commands' and observe how this simplifies the presentation of data to the person auditing activity.

e) Click the 'Output' radio button at the top of the screen to display stdout



The Output screen allows the auditor to replay every keystroke typed by the user using the navigation buttons at the bottom. The playback speed can be varied accordingly and the terminal type manually adjusted if required.

Click the 'Play' button to watch a playback of session activity.



Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Command Control Keystroke Report  Input  Output Tue Jun 10 10:13:38 GMT-0400 2008

```
[root@]# id
uid=0(root) gid=0(root) groups=100(users)
[root@]# uname -a
Linux fedvml 2.6.11-1.1369_FC4 #1 Thu Jun 2 22:55:56 EDT 2005 i686 i686 i386 GNU
/Linux
[root@]# whoami
root
[root@]# passwd
/usr/bin/rush: Permission denied
[root@]# cd /etc
[root@]# more passwd
```

<Rewind Pause Play Forward>

Playback Speed: Full Speed Scrollback KB: 20 Terminal Type: vt100

Audit Manager: usma-vfc1

Cancel

If a specific part of the session needs to be played back, simply switch to the 'input' view by clicking the **Input** radio button at the top of the screen, then click the stdin line where you want play back to commence, and then click the **Output** radio button again. You will find that the stdout playback is now at the direct point you just selected and you can commence playback.

f) Click **Cancel** when you have finished viewing the record.

Notice how the **Edit Record** icon is now available, and that a record has been made in the event audit trail noting that the keystroke activity has been viewed.



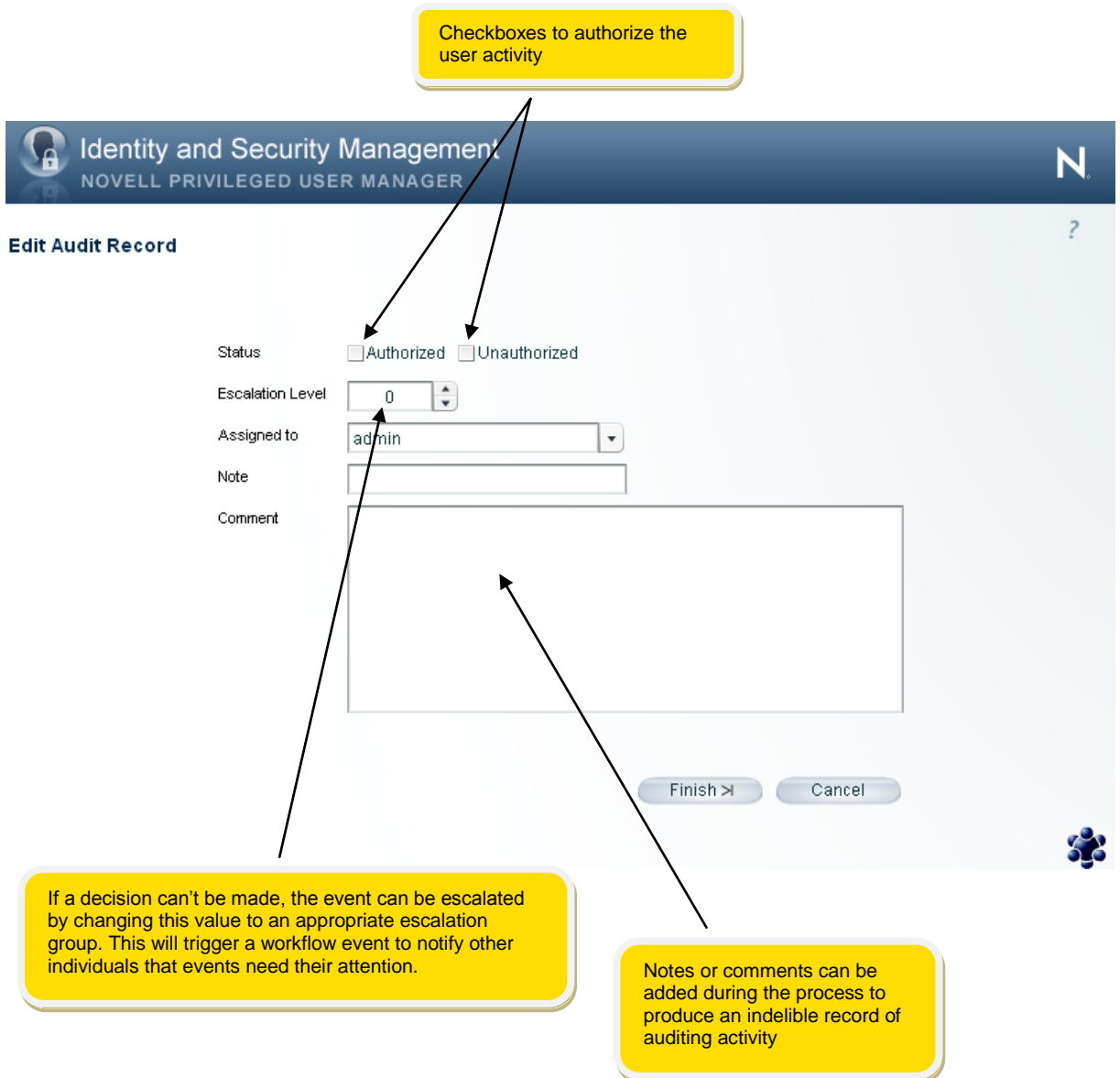
History

admin@usma-vfc1(192.168.5.105) 26 Jun 2008 05:57:39

- Keystroke: viewed by "admin"
- Status: Changed from "New" to "Pending"

Keystroke Edit Record

g) Click the Edit Record icon, you will see the following.



Checkboxes to authorize the user activity

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Edit Audit Record

Status  Authorized  Unauthorized

Escalation Level

Assigned to

Note

Comment

Finish > Cancel

If a decision can't be made, the event can be escalated by changing this value to an appropriate escalation group. This will trigger a workflow event to notify other individuals that events need their attention.

Notes or comments can be added during the process to produce an indelible record of auditing activity

h) Check the Authorized checkbox and click Finish.

Notice that the event is no longer visible in the view as the default filters are set to show only new or pending events. To display it again, change the filter and click Refresh.

This is the end of **Reviewing keystroke activity proactively**

To return to the Home Menu, click **Home** near the top of the screen.

**Reviewing keystroke activity forensically**

- a) Select the Reporting Console from the Home Menu



- b) Click on the **Command Control Reports** icon, then the **Sample report** icon

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Home/Reporting/Command Control Reports/Sample report

Report Data | LogFiles | Filter | General

Time	User	Host	RunAs	RunHost	Command	Authorized	Capture	Audit Status	Audit ID
Tue Jun 10 10:08:40	cusr1	fedvm3	cusr1	fedvm3	/usr/bin/ksh	yes	yes		7492888
Tue Jun 10 10:11:13	tusr1	fedvm1	root	fedvm1	id	yes	no		760b158
Tue Jun 10 10:11:20	tusr1	fedvm1	tusr1	fedvm1	ls -l	no	no		4bd266c
Tue Jun 10 10:12:14	tusr1	fedvm3	root	fedvm3	id	yes	no		ba8df33c
Tue Jun 10 10:12:18	tusr1	fedvm3	tusr1	fedvm3	ls -l	no	no		270e87fe
Tue Jun 10 10:12:27	tusr2	fedvm1	tusr2	fedvm1	id	no	no		8e55d9d
Tue Jun 10 10:12:31	tusr2	fedvm1	root	fedvm1	ls -l	yes	yes		7ab0b65
Tue Jun 10 10:12:40	tusr2	fedvm3	tusr2	fedvm3	id	no	no		ac79ef3b
Tue Jun 10 10:12:43	tusr2	fedvm3	tusr2	fedvm3	ls -l	no	no		98b6312
Tue Jun 10 10:12:59	rusr1	fedvm1	root	fedvm1	/usr/bin/rush	yes	yes		a7610cf5

Audit Manager: usma-vcf1

Apply Reset

- c) Click on the **LogFiles** tab

Notice that when rollover is enabled the old log files will all appear in the list and it is possible to still access any previous database and use it as part of the report.





d) Click on the **Filter** tab

Enter **\*usvi\*** in the **Command Filter** field and check the **Search audited commands** box as below, then click **Apply**.

Note that **usvi** is Novell's locked down version of **vi**, and gets called automatically when the user uses **vi**.

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Home/Reporting/Command Control Reports/Sample report

Report Data LogFiles **Filter** General

Delete Report  
Activity Report  
Keystroke Replay

Home  
Help  
About Framework  
Change Password  
Log off admin  
Install Consoles

Authorized  Yes  No  
Session capture  Yes  No

Submit User Filter  
Run User Filter  
Submit Host Filter  
Run Host Filter  
Command Filter **\*usvi\***  Search audited commands  
Audit ID Filter

After 15 Mar 2009 00:00  enabled  
Before 15 Mar 2009 23:59  enabled

Apply Reset

e) Now click back to the **Report Data** tab

Notice how the list of events has been filtered to include only those sessions where **vi** has been executed.

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Home/Reporting/Command Control Reports/Sample report

Report Data LogFiles Filter General

Delete Report  
Activity Report  
Keystroke Replay

Home  
Help  
About Framework  
Change Password  
Log off admin  
Install Consoles

Time	User	Host	RunAs	RunHost	Command	Authorized	Capture	Audit Status	Audit ID
Tue Jun 10 10:12:59	rusr1	fedvm1	root	fedvm1	/usr/bin/rush	yes	yes		a7610cf5-79

Audit Manager: usma-vfc1

Apply Reset



f) Double-click the event to bring up the keystroke player as below.

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Command Control Keystroke Report  Input  Output

Time	Standard Input
10 Jun 2008 10:13:02	id[CR]
10 Jun 2008 10:13:13	uname -a[CR]
10 Jun 2008 10:13:16	whoami[CR]
10 Jun 2008 10:13:22	passwd[CR]
10 Jun 2008 10:13:33	cd /etc[CR]
10 Jun 2008 10:13:38	more passwd[CR]
10 Jun 2008 10:13:51	cp /etc/passwd /tmp/file1[CR]
10 Jun 2008 10:13:55	cd /tmp[CR]
10 Jun 2008 10:14:00	ls -l[CR]
10 Jun 2008 10:14:10	ksh[CR]
10 Jun 2008 10:14:16	vi file1[CR]
10 Jun 2008 10:14:34	[KCUD1][KCUD1][KCUD1]dddddddothis is a test[ESC]ZZrm -rf file1[CR]
10 Jun 2008 10:14:38	ls -l[CR]
10 Jun 2008 10:14:41	cd /[CR]
10 Jun 2008 10:14:50	telnet □□□□□ssh fedvm3[CR]
10 Jun 2008 10:14:52	yes[CR]
10 Jun 2008 10:14:54	xxxxx[CR]
10 Jun 2008 10:15:00	id[CR]
10 Jun 2008 10:15:03	exit[CR]
10 Jun 2008 10:15:14	reboot[CR]

Terminal Type: vt100 Audit Manager: usma-vfc1

vt100  Find  Show control characters  
Decryption key  Refresh  Show audited commands  
 Show profile commands Cancel

g) Now type **vi** into the search field and click the **Find** button as below

Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Command Control Keystroke Report  Input  Output

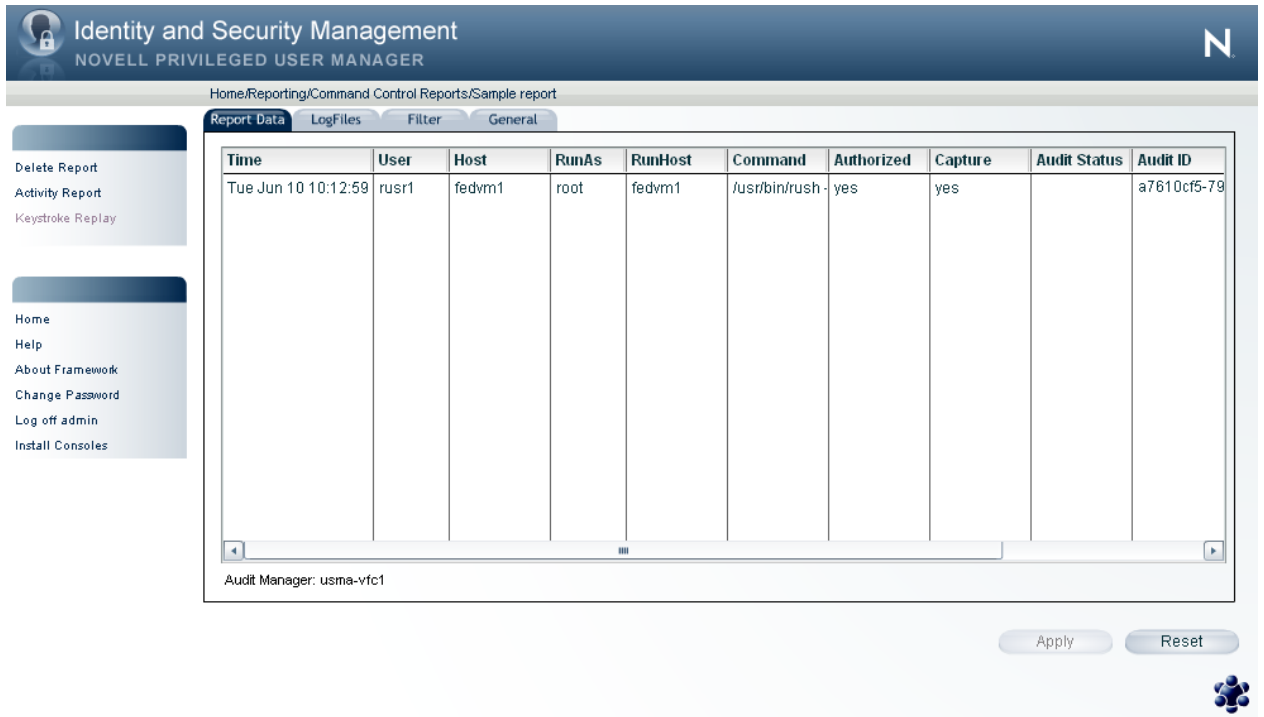
Time	Standard Input
10 Jun 2008 10:13:22	passwd[CR]
10 Jun 2008 10:13:33	cd /etc[CR]
10 Jun 2008 10:13:38	more passwd[CR]
10 Jun 2008 10:13:51	cp /etc/passwd /tmp/file1[CR]
10 Jun 2008 10:13:55	cd /tmp[CR]
10 Jun 2008 10:14:00	ls -l[CR]
10 Jun 2008 10:14:10	ksh[CR]
10 Jun 2008 10:14:16	vi file1[CR]
10 Jun 2008 10:14:34	[KCUD1][KCUD1][KCUD1][KCUD1]dddddddothis is a test[ESC]ZZrm -rf file1[CR]
10 Jun 2008 10:14:38	ls -l[CR]
10 Jun 2008 10:14:41	cd /[CR]
10 Jun 2008 10:14:50	telnet □□□□□ssh fedvm3[CR]
10 Jun 2008 10:14:52	yes[CR]
10 Jun 2008 10:14:54	xxxxx[CR]
10 Jun 2008 10:15:00	id[CR]
10 Jun 2008 10:15:03	exit[CR]
10 Jun 2008 10:15:14	reboot[CR]
10 Jun 2008 10:15:18	exit[CR]
10 Jun 2008 10:15:18	[ENDSESSION]

Terminal Type: vt100 Audit Manager: usma-vfc1

vt100  Find  Show control characters  
Decryption key  Refresh  Show audited commands  
 Show profile commands Cancel

Notice that the highlight bar moves to the first instance of **vi**.

h) Click **Cancel** to return to Command Control Reports



Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Home/Reporting/Command Control Reports/Sample report

Report Data LogFiles Filter General

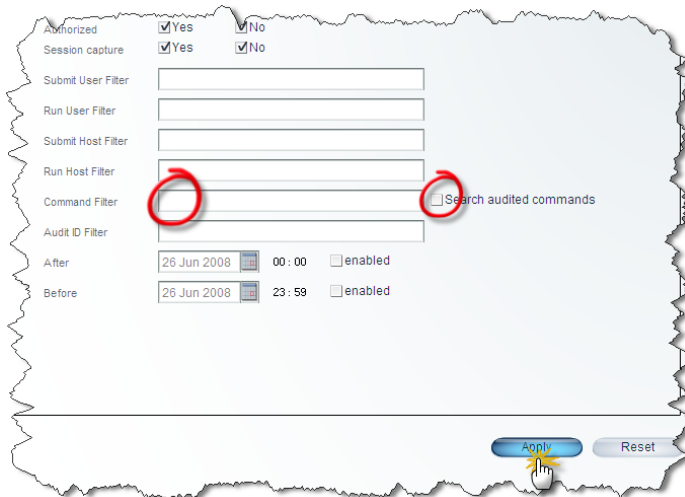
Time	User	Host	RunAs	RunHost	Command	Authorized	Capture	Audit Status	Audit ID
Tue Jun 10 10:12:59	rusr1	fedvm1	root	fedvm1	/usr/bin/rush	yes	yes		a7610cf5-79

Audit Manager: usma-vfc1

Apply Reset

i) Click on the **Filter** tab

Clear the **Command Filter** field and uncheck the **Search audited commands** checkbox, then click **Apply**.



Authorized  Yes  No  
 Session capture  Yes  No  
 Submit User Filter   
 Run User Filter   
 Submit Host Filter   
 Run Host Filter   
 Command Filter   Search audited commands  
 Audit ID Filter   
 After 26 Jun 2008 00:00  enabled  
 Before 26 Jun 2008 23:59  enabled

Apply Reset

j) Click on the **Report Data** tab

Notice how all events are now showing in the list.

#### Note

Filters can be used ad-hoc to search for events with specific criteria, or saved for later use.

This is the end of **Reviewing keystroke activity forensically**

To return to the Home Menu, click **Home** near the top of the screen

### Use Command Control to access a privileged shell

- a) On your test system, create 2 user accounts:

User account called **cusr1** with **/usr/bin/crush** as the shell  
User account called **rusr1**

- b) Login as **cusr1** and notice how you are dropped straight into a shell.

This shell runs as the **cusr1** user account but will audit all keystroke activity

- c) Type some test commands to generate activity, then type **exit**

- d) Login as **rusr1** and from the command line execute **usrun rush**

You will be in a shell that is running as root with full keystroke auditing and Command Risk Analysis processing.

Additionally you should not be able to run the following commands:

passwd  
/bin/ksh  
ksh  
/usr/bin/ksh

- e) Type some test commands to generate activity, then type **exit**

- f) Still logged in as **rusr1**, execute **usrun shell**

Notice how you are taken into the rush shell as in the previous step.

This demonstrates the ability for Command Control to rewrite commands.

This is the end of **Use Command Control to access a privileged shell**

You may now view your generated events using the **forensic** method as described earlier in this guide.

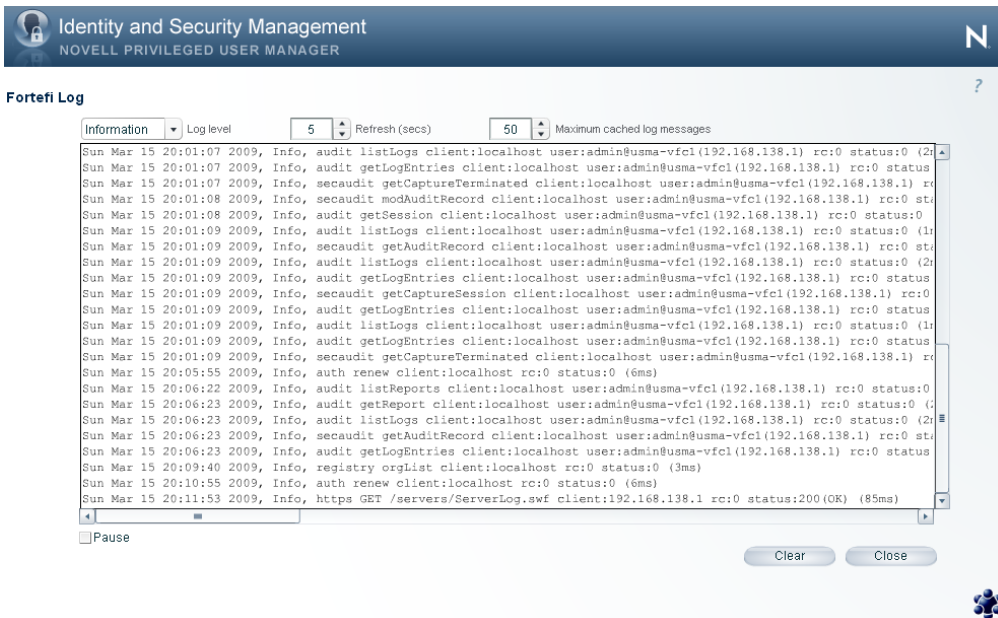


**Review Novell Privileged User Manager system logs**

- a) Select the Hosts Console from the Home Menu



- b) Select your host by selecting it in the domain tree, then click **View Host Log** as below.



This is the end of **Review Novell Privileged User Manager System Logs**

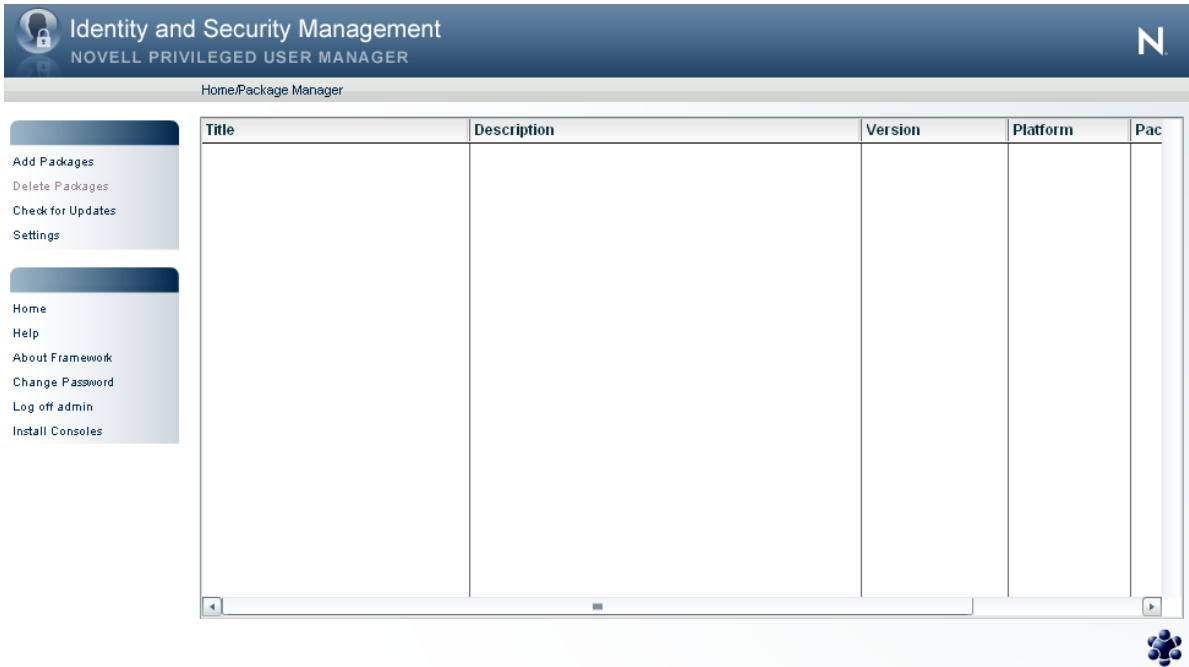
To return to the Home Menu, click **Close**, then click **Home** near the top of the screen





**Download Novell updates and deploy to your host**

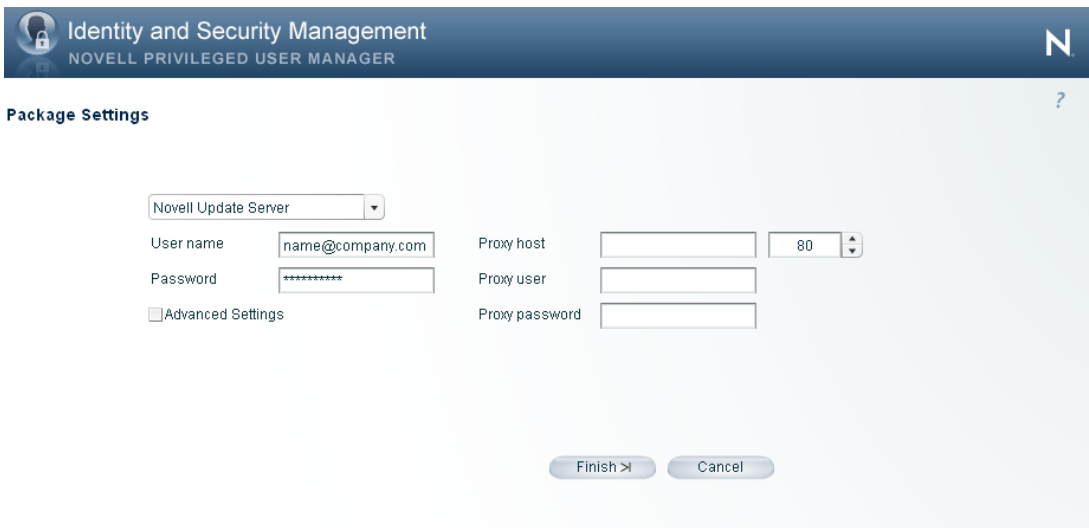
- a) Select the Package Manager console from the Home Menu



- b) Select **Settings** from the left-hand menu

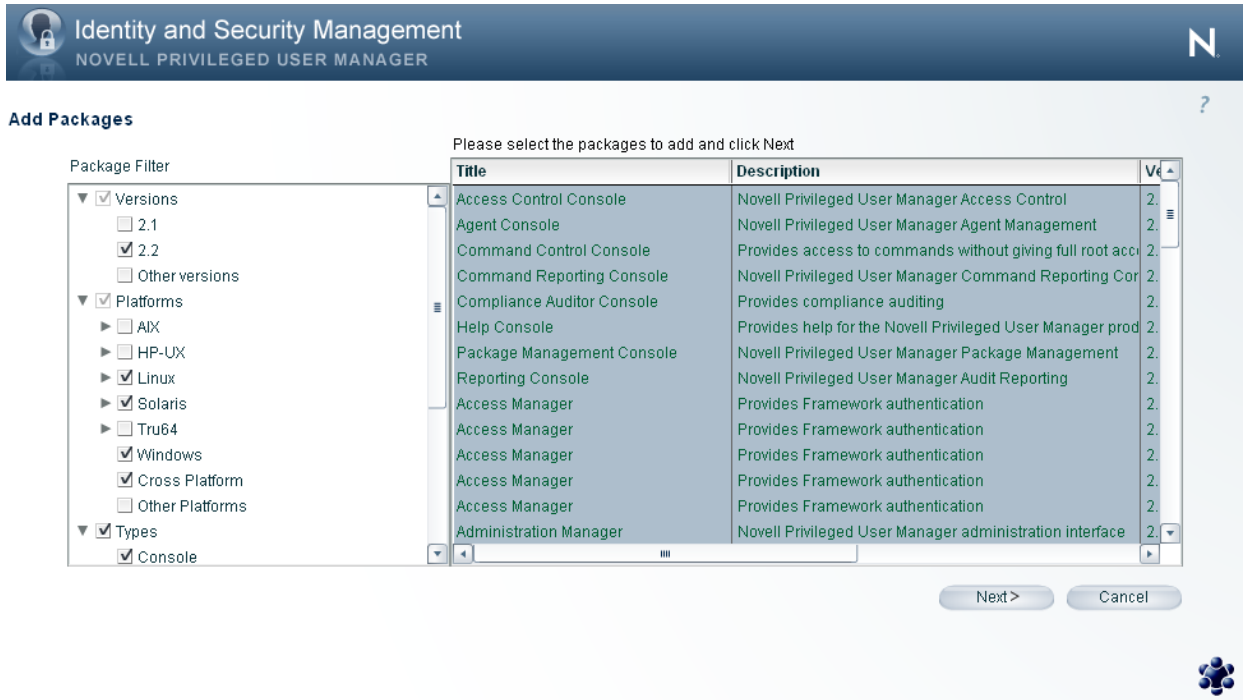


Enter the access credentials (supplied by Novell), into the **User name** and **Password** boxes as shown below, If applicable, enter any proxy host information, and then click **Finish**.



- c) From the main Package Manager Console, select **Add Packages** from the left-hand menu.

A selection list will be displayed as below. Make sure you select the checkboxes shown on the left for the **Types** and **Components** groups, at a minimum. Check the appropriate operating systems you have (or planning to have) in your Framework under **Platforms**.



**Add Packages**

Please select the packages to add and click Next

Title	Description	Ver
Access Control Console	Novell Privileged User Manager Access Control	2.
Agent Console	Novell Privileged User Manager Agent Management	2.
Command Control Console	Provides access to commands without giving full root acco	2.
Command Reporting Console	Novell Privileged User Manager Command Reporting Cor	2.
Compliance Auditor Console	Provides compliance auditing	2.
Help Console	Provides help for the Novell Privileged User Manager prod	2.
Package Management Console	Novell Privileged User Manager Package Management	2.
Reporting Console	Novell Privileged User Manager Audit Reporting	2.
Access Manager	Provides Framework authentication	2.
Access Manager	Provides Framework authentication	2.
Access Manager	Provides Framework authentication	2.
Access Manager	Provides Framework authentication	2.
Access Manager	Provides Framework authentication	2.
Administration Manager	Novell Privileged User Manager administration interface	2.

Next > Cancel

Select any module and click **Ctrl-A** to select all modules for download, click **Next**.

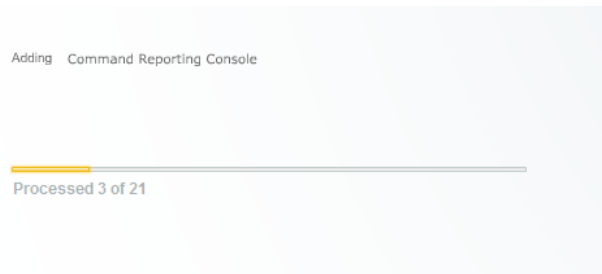
**To select a range**

Click on the top item and then click on the bottom item while holding the shift key down.

**To select single items**

Hold the Ctrl key down while clicking individual rows to alternately select or deselect

- d) Modules will start downloading to your Package Manager as shown below.



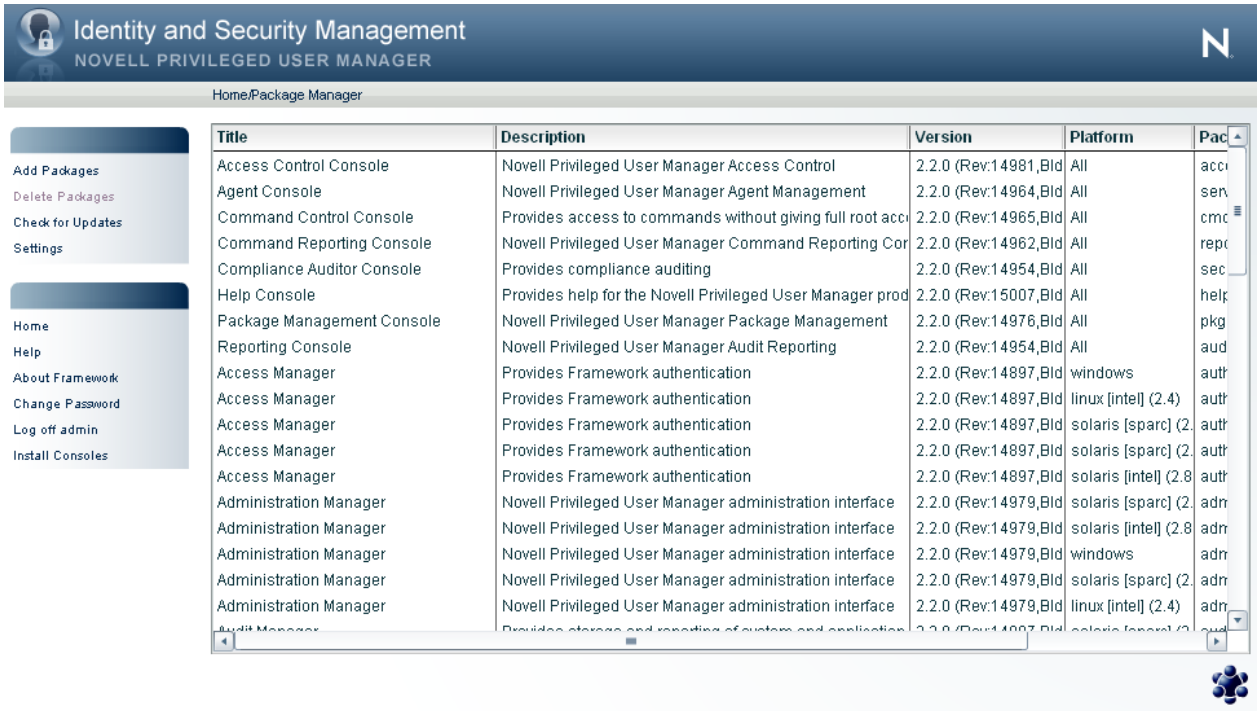
Adding Command Reporting Console

Processed 3 of 21

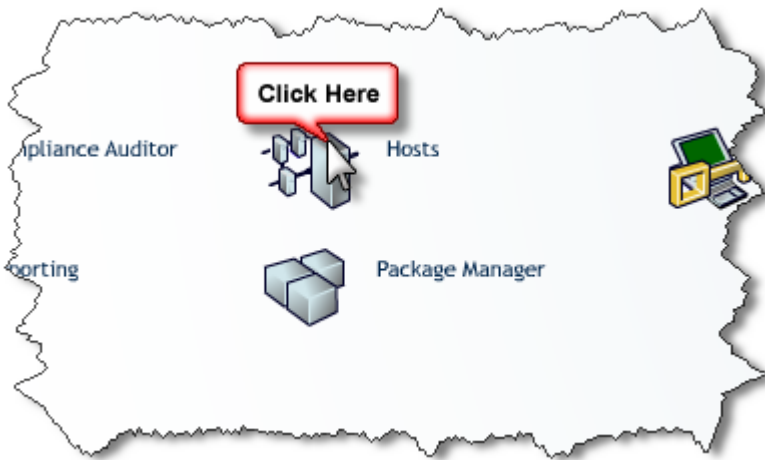
When all modules have been successfully transferred to your Package Manager, click **Finish**



e) Verify that the Package Manager looks similar to the following:



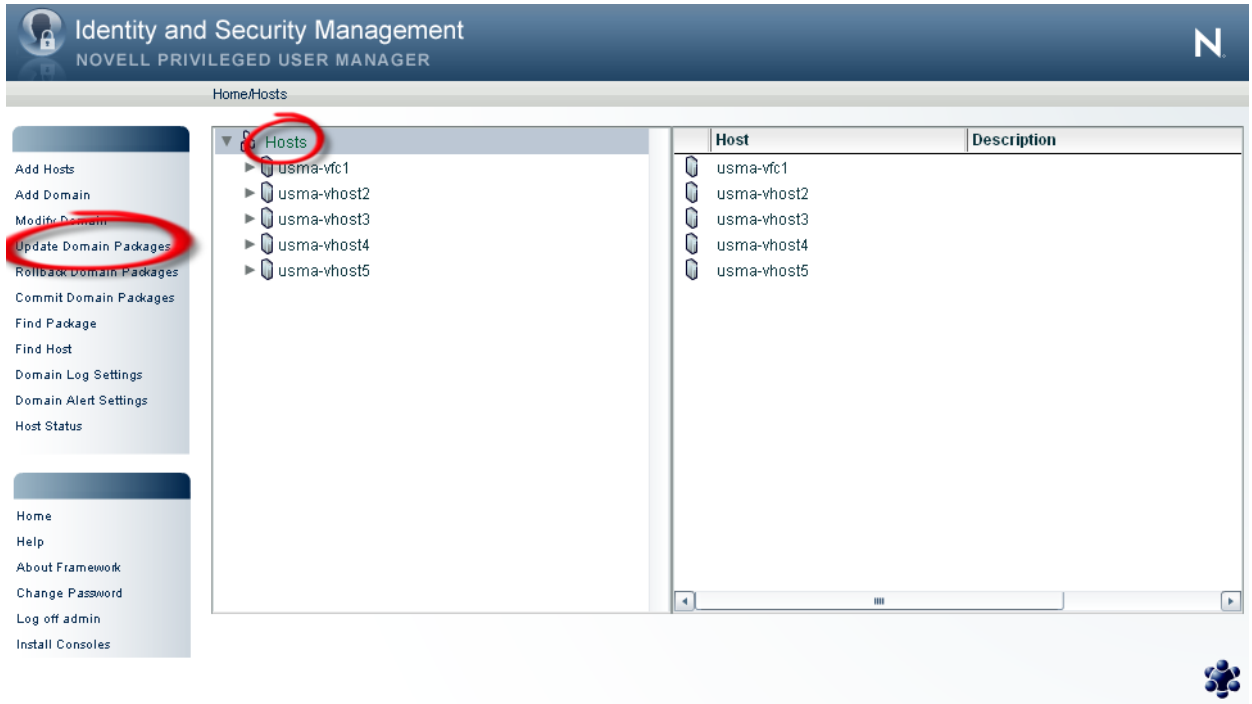
f) Click **Home** on the top menu to return to the Home Menu, then select the Hosts Console



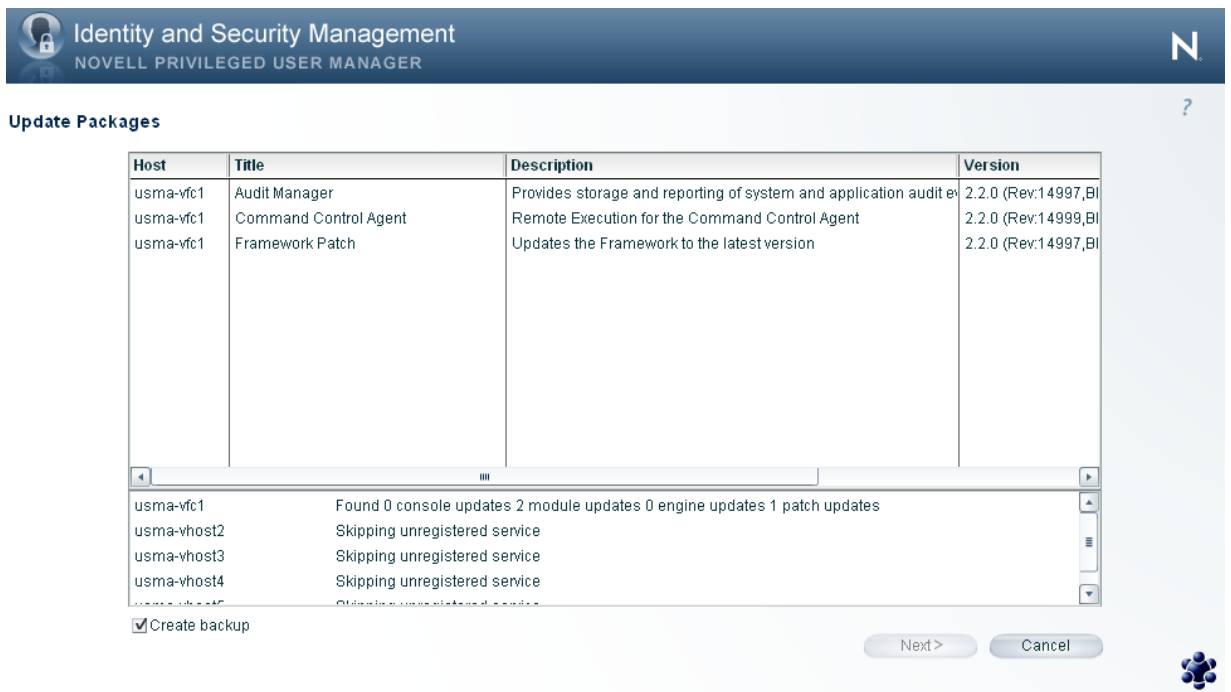
In this next step, we will check to make sure that there are no updated components in the Package Manager that need to be deployed to our test environment.

## g) Update installed Framework host modules

From the main console menu, select **Hosts**. You may have one or more hosts in your Framework depending on your evaluation, select the **Hosts** node at the top.

h) Click **Update Domain Packages** from the left-hand menu.

If there are updates available, a list of modules that can be updated will be displayed as below.



Select any line and click **Ctrl-A** to select all updates, click **Next**.

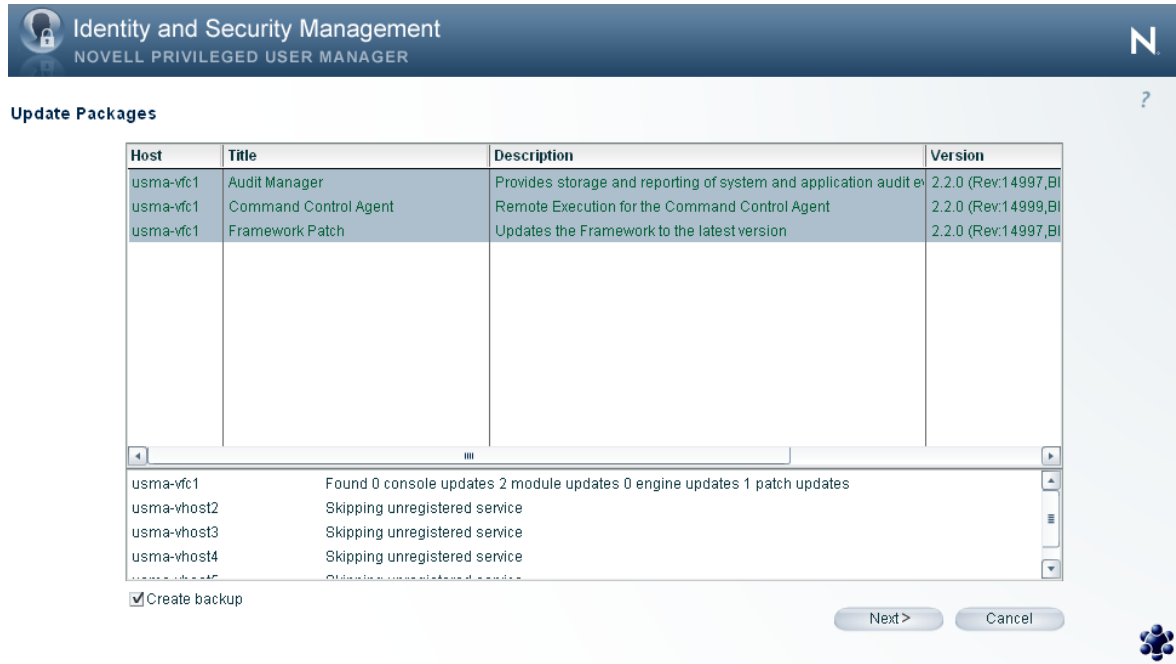
**To select a range**

Click on the top item and then click on the bottom item while holding the shift key down.

**To select single items**

Hold the Ctrl key down while clicking individual rows to alternately select or deselect

Once your updates have been selected as below, click **Next**.



Identity and Security Management  
NOVELL PRIVILEGED USER MANAGER

Update Packages

Host	Title	Description	Version
usma-vfc1	Audit Manager	Provides storage and reporting of system and application audit ev	2.2.0 (Rev:14997,BI
usma-vfc1	Command Control Agent	Remote Execution for the Command Control Agent	2.2.0 (Rev:14999,BI
usma-vfc1	Framework Patch	Updates the Framework to the latest version	2.2.0 (Rev:14997,BI

Found 0 console updates 2 module updates 0 engine updates 1 patch updates

Create backup

Next > Cancel

Verify the modules on your host(s) have been updated successfully, click **Finish**.

If any console updates have been applied, log off, close and then reopen your browser before logging back on to the administration console to ensure existing Flash files are flushed from your cache. Run through the update process again in case further updates are required.