Access Manager 3.1 SP2 Beta 1 Scenarios

December 21, 2009

Novell®

The following scenarios have been designed to introduce you to the new features in Access Manager 3.1 SP2.

1 Linux Access Gateway Appliance Scenarios

1.1 Installing the SLES 11 Version

This beta scenario introduces you to the new Access Gateway Appliance which is built on SUSE® Linux Enterprise Server (SLES 11). The SLES 11 version of the Access Gateway Appliance supports newer hardware, and SLES 11 is a supported operating system that provides security updates.

The previous version of the Access Gateway Appliance is built on SLES 9 SP3. The SLES 9 operating system is no longer a supported operating system and does not run on the latest hardware.

1.1.1 Assumptions

You need an installed 3.1 SP2 version of the Administration Console and Identity Server. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).

1.1.2 Known Issues

- Bug 554518 -Network mode of installation through TFTP is not supported
- Bug 560278 -Installation: There is no provision to return to the configuration screen to make changes
- Bug 559398 - The network gateway address is removed when the network interface is restarted.
- Bug 558698 - The Linux Access Gateway SLES 11 appliance installation summary screen does not display SSL VPN, even if the Install and Enable SSL VPN option is selected. Also, the installation does not perform a password strength check.

1.1.3 Procedure

For installation instructions, see "Installing the Linux Access Gateway Appliance" (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bd1egh.html).

1.1.4 Test Results

To verify the installation of the Linux Access Gateway Appliance:

1. Log in to the Administration Console.
2. Click *Devices* > *Access Gateways*.

   If the installation was successful, the IP address of your Access Gateway appears in the Server list.

1.1.5 Troubleshooting Tips

For installation issues, refer to the following logs:

- RPM installation log file: `/tmp/novell_access_manager/inst_lag.log`
- Autoimport log file: `/tmp/novell_access_manager/inst_lag_import_<date>.log`
- Auto partition log file: `/var/adm/autoinstall/logs/diskParitition.sh.log`
- JCC configuration logs: `/opt/novell/devman/jcc/logs/configure.log.0`

1.2 Upgrading the Linux Access Gateway Appliance

This scenario explains how you can upgrade the SLES 9 Linux Access Gateway Appliances in a cluster from 3.0 SP4 to 3.1 SP2 and use the timeout per protected resource feature.

1.2.1 Assumptions

Your current Access Manager setup has a 3.0 SP4 IR4 version of the Administration Console, the Identity Server, and the Linux Access Gateway Appliance. The secondary Linux Access Gateway Appliance in your cluster also has the SSL VPN server installed.

1.2.2 Known Issues

- In Access Manager 3.0 SP4, the SSL VPN server installed with the Linux Access Gateway Appliance is accelerated by using its public IP address. After upgrading to 3.1 SP2, you must change the Web server IP address to the loopback IP address , 127.0.0.1. For more information, see *Section 2.2.7: Configuration Changes to the SSL VPN Server Installed with the Linux Access Gateway* in the *SSL VPN Server Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpnhelp/?page=/documentation/beta/novellaccessmanager31/sslvpnhelp/data/bmmi1it.html)
- The session timeout for Identity Server is 15 minutes in 3.0 SP4 and this is reflected in the default authentication timeout for all the contracts in the Identity Server. The session timeout for Identity Server is 60 minutes in 3.1 SP2.

1.2.3 Procedure

1. Upgrade the Administration Console and Identity Server to 3.1 SP2. For more information, see Upgrading Access Manager Components (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html) in the *Installation Guide*.

   For upgrade information, see Upgrading from Access Manager 3.0 SP4 to Access Manager 3.1 SP2 (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bgfx9yh.html) in the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).

2. Upgrade the secondary Linux Access Gateway Appliance to 3.1 SP2. For more information, see, Upgrading Access Manager Components (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bookinfo.html)

3. Upgrade the primary Linux Access Gateway Appliance to 3.1 SP2.

   After the successful upgrade of the Linux Access Gateway Appliances, the timeout per protected resource feature is not enabled by default.

4. To enable the timeout per protected resource feature:

   4a Modify the authentication contract configuration at the Identity Server.

   4b Apply the changes to the Linux Access Gateway Appliance cluster.

   The timeout per protected resource feature is enabled on the Linux Access Gateway Appliances.

5. If you have an SSL VPN server installed on the Linux Access Gateway Appliance, apply changes to the SSL VPN server after it is upgraded to 3.1 SP2, to get the 3.1 SP2 features.

   NOTE: Any SSL VPN connection made before the changes are applied at the SSL VPN server are not enabled for the new client cleanup options.

   ---

6. Upgrade the policies.

   For upgrade information, see "Upgrading the Policies" (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bgfx9yh.html#bhn7nna) in the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).

1.3 Migrating a SLES 9 Access Gateway to SLES 11

This scenario explains how to migrate a SLES 9 SP3 Access Gateway Appliance on 3.1.1 to the SLES 11 version of the Access Gateway Appliance. The 3.1 SP1 version of the Access Gateway Appliance should be in a test environment.

1.3.1 Assumptions

- You have an installed SLES 9 version of the Access Gateway that is imported into the Administration Console.
- You have an Administration Console and Identity Server that have been upgraded to 3.1 SP2. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).

1.3.2 Known Issues

None.

1.3.3 Procedure

1. Upgrade the 3.1 SP1 Access Gateway Appliance to 3.1 SP2. For installation instructions, see "Upgrading the Linux Access Gateway Appliance" (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bbycmhz.html).
2. Back up the SLES 9 Access Gateway configuration.

   The backup script allows you to restore touch files and customized error page configurations.

   2a. At the Access Gateway machine, log in as root.

   2b. Run the following script:

   ```
   lag-backup-restore.sh
   ```

   This script creates the following files:

   - **lagNoRestore.tar.gz:** This file contains information and files that don't need to be restored after migrating to SLES 11.
   - **lagRestore.tar.gz:** This file contains information and files that need to be restored after migrating to SLES 11.

   2c. Copy the tar files to another physical location.
3. Disconnect the Access Gateway Appliance from the network.
4. Install the SLES 11 version of the Access Gateway Appliance.

   For installation instructions, see "Installing the Linux Access Gateway Appliance" (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bd1egh.html)

   - Use the same DNS name and IP address as the SLES 9 version of the Access Gateway.
   - Import the Access Gateway into the same Administration Console.

     The Administration Console pushes the SLES 9 configuration details to the SLES 11 Access Gateway.
5. Restore the touch files and customized error pages:

   5a. Copy the `lagRestore.tar.gz` file to the Access Gateway.

   5b. Use the `lag-backup-restore.sh` script to restore the files.

1.3.4 Test Results

- Check the health of the Access Gateway in the Administration Console.
- Check the configuration of the Access Gateway, its policies, and its certificates.
- Check the system configuration settings, such as network settings and secondary IP addresses.

1.3.5 Troubleshooting Tips

For installation issues, refer to the following logs:

- RPM installation log file: `/tmp/novell_access_manager/inst_lag.log`
- Autoimport log file: `/tmp/novell_access_manager/inst_lag_import_<date>.log`

- Auto partition log file: `/var/adm/autoinstall/logs/diskParitition.sh.log`
- JCC configure logs: `/opt/novell/devman/jcc/logs/configure.log.0`

1.4 Configuring Timeout Per Protected Resource

This scenario explains how to restrict session availability based on user activity. It explains how to configure the Timeout Per Protected Resource feature.

In previous versions of Access Manager, there is one global session timeout for all the protected resources. With Access Manager 3.1 SP2, session availability for individual protected resources can be configured and managed for each resource by using Timeout Per Protected Resource. You can configure a specific authentication timeout value for each individual contract at the Identity Server, then assign the contracts to the protected resources of the Access Gateway.

1.4.1 Assumptions

If the authentication method used for the contract is Name/Password-Basic, the session might be active after the timeout because the browser can still send requests with the basic authentication header.

1.4.2 Procedure

1. At the Identity Server, configure authentication contract C1, using the Name/Password-Form method. Set the authentication timeout value to 15 minutes and set the Activity realm to `test`.
2. At the Access Gateway, create protected resource PR1 and assign C1 to it.
3. Use valid credentials to access the protected resource at 7:00 pm.
4. Leave the session idle for 5 minutes and access the resource again at 7:05 pm.
5. Leave the session idle for 10 minutes and access the resource again at 7:15 pm.
6. Leave the session idle for 15 minutes and access the resource again at 7:30 pm.

1.4.3 Test Results

- For Step 5: The session does not time out by 7:15 because the user was active at 7:05 pm.
- For Step 6: The session times out by 7:30 and the user is required to log in again.

1.4.4 Troubleshooting Tips

If the user does not time out after the configured timeout value has elapsed, check the defined contracts at the Identity Server to ensure that there is no other contract in the `test` activity realm. User activity in another contract in the same activity realm can affect your contract's timeout.

If the activity realm had not been configured and is left blank, any activity by the user at the Identity Server can affect the user's session timeout. You must specify a unique activity realm for this scenario to work.

2 Timeout Per Protected Resource Scenarios

2.1 Same Activity Realm

The purpose of this scenario is to introduce you to the Timeout Per Protected Resource feature, which is new in Access Manager 3.1 SP2. This scenario is designed to help you understand the effect of having two authentication contracts in the same activity realm.

2.1.1 Assumptions

- You have an installed and configured 3.1 SP2 version of an Administration Console, an Identity Server, and an Access Gateway. The Access Gateway can be either an Access Gateway Appliance or an Access Gateway Service.
- The base URL of the Identity Server is secure (it uses SSL/HTTPS).
- You understand authentication methods and authentication contracts.
- You have read "Assigning a Timeout Per Protected Resource" (http://www.novell.com/documentation/beta/novellaccessmanager31/accessgatehelp/data/prlist.html#bmn94qo).

2.1.2 Known Issues

None

2.1.3 Procedure

1. Create a new authentication method (M1):
   - **1a** Select *Secure Name/Password – Form* for the class.
   - **1b** Select the *Identifies User* option.
   - **1c** Select a user store.
2. Create a new authentication contract (C1).:
   - **2a** Make sure the URI is unique.
   - **2b** Set the *Authentication Timeout* to 5 minutes.
   - **2c** Specify `Same` for the *Activity Realm*.
   - **2d** Select `M1` for the *Method*.
   - **2e** Click *Next*.
   - **2f** Modify the *Text* and *Image* to fit your needs.
   - **2g** Click *Finish*.
3. Create a new authentication method (M2):
   - **3a** Select *Secure Name/Password – Form* for the class.
   - **3b** Select the *Identifies User* option.
   - **3c** Select a user store.
4. Create a new authentication contract (C2):
   - **4a** Make sure the URI is unique.
   - **4b** Set the *Authentication Timeout* to 10 minutes.
   - **4c** Specify `Same` for the *Activity Realm*.
   - **4d** Select `M2` for the *Method*.

4e Click *Next*.

4f Modify the *Text* and *Image* to fit your needs.

4g Click *Finish*.

5 Update the Identity Server.

6 Make sure the Access Gateway has two protected resources (PR1 and PR2). Create them if necessary.

7 Assign authentication contract C1 to protected resource PR1.

8 Assign authentication contract C2 to protected resource PR2.

9 Update the Access Gateway.

10 Access a page on protected resource PR1 from a client browser.

You should be prompted to authenticate.

11 Access a page on protected resource PR2 with the same browser session.

You should be prompted to authenticate again. Make sure to use the same user for both logins.

12 Refresh the page on protected resource PR2 at least once a minute over a time period greater than 5 minutes.

13 Go back to the page on protected resource PR1.

Access should still be allowed. The user has not been inactive, so the activity has kept the session to PR1 active.

14 Access the page on protected resource PR2 again.

15 Let the browser sit idle for a time period greater than 5 minutes but less than 10 minutes.

16 Refresh the page on protected resource PR2.

The page should refresh without prompting you to authenticate.

17 Access the page on protected resource P1.

You should be prompted to authenticate again. You have been idle longer than the contract's timeout limit.

2.1.4 Test Results

Activity on a protected resource with the same realm as other protected resources prevents authentication timeout on the other protected resources.

Each protected resource can have a different authentication timeout.

2.1.5 Troubleshooting Tips

- An authentication contract with an empty realm or a realm of `Any` allows activity from any protected resource to prevent a timeout on a protected resource that uses that contract.

- Single sign-on can give the appearance that an authentication timeout has not occurred. Keeping the authentication method of each authentication contract unique eliminates single sign-on. Having two contracts with the same method essentially gives both contracts the longest timeout of the two. Single sign-on allows the user to access the resource with the shorter timeout as long as the resource with the longer timeout has not expired.
- The *Any Contract* option can be assigned the authentication timeout of any of the authentication contracts. The *Any Contract* option is assigned the timeout of the authentication contract that the user used to authenticate. In the case of an unknown authentication contract from a federated authentication, the contract is assigned the default session timeout. When the *Any Contract* option times out, it can be assigned a different timeout if single sign-on gives the user access by using a different authentication contract than the contract that was used with the previous authentication with the *Any Contract* option. To prevent authentication timeout confusion, all authentication contracts should be assigned the default session timeout if the *Any Contract* option is used.

2.2 Unique Activity Realms

The purpose of this scenario is to introduce you to the Timeout Per Protected Resource feature and to help you understand that protected resources that use authentication contracts with unique activity realms are not affected by activity on other protected resources with different contracts.

2.2.1 Assumptions

- You have an installed and configured 3.1 SP2 version of an Administration Console, an Identity Server, and an Access Gateway. The Access Gateway can be either an Access Gateway Appliance or an Access Gateway Service.
- The base URL of the Identity Server is secure (it uses SSL/HTTPS).
- You understand authentication methods and authentication contracts.
- You have read "Assigning a Timeout Per Protected Resource" (http://www.novell.com/documentation/beta/novellaccessmanager31/accessgatehelp/data/prlist.html#bmn94qo).

2.2.2 Known Issues

None.

2.2.3 Procedure

1 Create a new authentication method (M1):

1a Select *Secure Name/Password – Form* for the class.

1b Select the *Identifies User* option.

1c Select a user store.

2 Create a new authentication contract (C1):

2a Make sure the URI is unique.

2b Set the *Authentication Timeout* to 5 minutes.

2c Specify `AR1` for the *Activity Realm*.

2d Select M1 for the *Method*.

2e Click *Next*.

2f Modify the *Text* and *Image* to fit your needs.

2g Click *Finish*.

3 Create a new authentication method (M2):

3a Select *Secure Name/Password – Form* for the class.

3b Select the *Identifies User* option.

3c Select a user store.

4 Create a new authentication contract (C2):

4a Make sure the URI is unique.

4b Set the *Authentication Timeout* to 10 minutes.

4c Specify `AR2` for the *Activity Realm*.

4d Select M2 for the *Method*.

4e Click *Next*.

4f Modify the *Text* and *Image* to fit your needs.

4g Click *Finish*.

5 Update the Identity Server.

6 Make sure the Access Gateway has two protected resources (PR1 and PR2). Create them if necessary.

7 Assign authentication contract C1 to protected resource PR1.

8 Assign authentication contract C2 to protected resource PR2.

9 Update the Access Gateway.

10 Access a page on protected resource PR1 from a client browser.

You should be prompted to authenticate.

11 Access a page on protected resource PR2 with the same browser session.

You should be prompted to authenticate again. Make sure to use the same user for both logins.

12 Refresh the page on protected resource PR2 at least once a minute over a time period greater than 5 minutes.

13 Go back to the page on protected resource PR1.

You should be prompted to authenticate again.

2.2.4 Test Results

- Activity on a protected resource with a different activity realm and different protected resources does not prevent the authentication timeout from happening on the other protected resources.
- Each protected resource can have a different authentication timeout.

2.2.5 Troubleshooting Tips

- An authentication contract with an empty realm or a realm of `Any` allows activity from any protected resource to prevent a timeout on a protected resource that uses that contract.

- Single sign-on can give the appearance that an authentication timeout has not occurred. Keeping the authentication method of each authentication contract unique eliminates single sign-on. Having two contracts with the same method essentially gives both contracts the longest timeout of the two. Single sign-on allows the user to access the resource with the shorter timeout as long as the resource with the longer timeout has not expired.
- The *Any Contract* option can be assigned the authentication timeout of any of the authentication contracts. The *Any Contract* option is assigned the timeout of the authentication contract that the user used to authenticate. In the case of an unknown authentication contract from a federated authentication, the contract is assigned the default session timeout. When the *Any Contract* option times out, it can be assigned a different timeout if single sign-on gives the user access by using a different authentication contract than the contract that was used with the previous authentication with the *Any Contract* option. To prevent authentication timeout confusion, all authentication contracts should be assigned the default session timeout if the *Any Contract* option is used.

3 Access Gateway Service Scenarios

3.1 Installing the Access Gateway Service

This beta scenario introduces you to the new Access Gateway Service that can be installed on a SLES 11 server with a 64-bit operating system or on a Windows* Server* 2008 with a 64-bit operating system.

3.1.1 Assumptions

You need an installed 3.1 SP2 version of the Administration Console and Identity Server. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).

3.1.2 Known Issues

None.

3.1.3 Procedure

For installation instructions, see "Installing the Access Gateway Service" (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bitxc3y.html).

3.1.4 Test Results

To verify the installation of the Access Gateway Service:

1. Log in to the Administration Console.
2. Click *Devices* > *Access Gateways*.

   If the installation was successful, the IP address of your Access Gateway appears in the Server list.

3.2 Configuring the Access Gateway Service to Protect a Web Server

This beta scenario illustrates that the Access Gateway Service is configured just like the Access Gateway Appliance and can be used to protect the same kind of resources.

3.2.1 Assumptions

- You have an installed 3.1 SP2 version of the Administration Console. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).
- You have an installed and configured 3.1 SP2 version of the Identity Server. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).
- You have an installed Access Gateway Service. See Section 3.1, "Installing the Access Gateway Service," on page 10.

3.2.2 Known Issues

None.

3.2.3 Procedure

For configuration instructions, use one of the basic configuration scenarios from the *Setup Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/basicconfig/data/bookinfo.html):

- To use an existing Web server, see "Configuring the Access Gateway" (http://www.novell.com/documentation/beta/novellaccessmanager31/basicconfig/data/b1wyfmu.html).
- To set up a Web server with the Digital Airlines sample pages, see "Digital Airlines Example (http://www.novell.com/documentation/beta/novellaccessmanager31/basicconfig/data/bayxa4y.html).

3.2.4 Troubleshooting Tips

See "Troubleshooting the Access Gateway Service" (http://www.novell.com/documentation/beta/novellaccessmanager31/accessgatehelp/data/bjxln4j.html).

4 SSL VPN Server Scenarios

4.1 Importing and Exporting Client Integrity Check Policies

Access Manager 3.1 SP2 provides the option to back up and restore the Client Integrity Check policies through the Import and Export feature.

4.1.1 Assumptions

The most basic way to test the feature is to export of existing Client Integrity Check policies, delete them, then import an exported Client Integrity Check policy file.

Users can also create new Client Integrity Check policies for a different OS under different application types, such as Process, AbsoluteFile, Registry, Service, Package, and RPM.

These policies can then be saved, exported, and imported.

Policies can't be imported or exported selectively.

4.1.2 Known Issues

None.

4.1.3 Procedure

1. Log in to the Administration Console, then click *Devices* > *SSL VPNs* > *Edit*.
2. Click *Client Integrity Check Policies*.
3. Create new policies for different operating systems:

   For example:

   3a Select *Windows OS*.

   3b Create a Category and Application named `test`

   3c Create an Application Definition for an AbsoluteFile with the following attributes and values:

   ```
   Name: c:\test\test1.exe
   Version: 2
   HashMD5: 253627d4dbb0e7a177a2b1a0e0ba8ae8
   ```

   3d Click *OK* on each page and save the policies.

   3e Create similar policies for other application definitions such as process and service.

   3f Create similar policies for Linux* and Macintosh*.
4. Enable some of the categories and applications and disable others.
5. Click *OK*, then update the SSL VPN server.
6. Click *SSL VPNs* > *Edit* > *Client Integrity Check Policies*.
7. Click *Export* to export the file, specify a name, then save the file.
8. Delete the existing policies.
9. Click *OK*, then update the SSL VPN server.
10. Click *SSL VPNs* > *Edit* > *Client Integrity Check Policies*.

11 Click *Import*, browse to the file, then click *OK*.

12 Verify that all the policies, including the default policy and the policies you created have been imported with the correct application definition.

4.1.4 Test Results

The exported Client Integrity Check policies should be imported with the correct application definitions and enabled/disabled status.

4.1.5 Troubleshooting Tips

- Did you click *OK* on each step to save the newly created policy? Clicking *Cancel* after defining a policy results in the loss of that definition from the export file.
- Did you enable the category? By default, the newly created category is disabled and the application is enabled.

4.2 Configuring Client Cleanup Options

The Access Manager 3.1 SP2 provides an option in the Administration Console to control the desktop cleanup options for the SSL VPN users.

You can configure the following client cleanup options:

- Clear Browser Private Data
- Clear Java Cache
- Uninstall Enterprise Mode
- Leave Behind the Client Components
- Uninstall ActiveX control (for Internet Explorer* users only)

You set the default values for the cleanup options for the SSL VPN users when they log out. Based on these settings, the SSL VPN user can have some options enabled and others disabled.

You can allow or deny the user the ability to override the default settings.

The combination of these two settings enables you to control the cleanup options for the SSL VPN users.

4.2.1 Assumptions

You know the options that the users should not be allowed to control and the options that the users can be allowed to configure.

4.2.2 Known Issues

None.

4.2.3 Procedure

1 Log in to the Administration Console.

2 Click *Devices > SSL VPNs > Edit > Client Policies*.

3 In the *Client Cleanup Options* section, configure default values and configure whether the user can modify the default.

   By default *Java Cache Cleanup* and *Clear Browser Private Data* options are enabled and the *Allow User to Override* option is enabled for all options.

   For this beta scenario, allow the user to override the default setting for some of the options. For more information on the options, click the help (?) icon.

4 Click *OK*.

5 Update the SSL VPN server.

6 Log in as an SSL VPN client.

7 Click *Logout*.

   Based on the configuration in the Administration Console, you can select some cleanup options, but others are disabled.

4.2.4 Test Results

Your selection for the cleanup options should be available when you log out as an SSL VPN client.

4.3 Configuring for HMAC (Hash-Based Message Authentication Code)

HMAC is an option provided by OpenVPN* to authenticate the client before OpenVPN negotiation is initiated. It means that the first packet from the OpenVPN client to the OpenVPN server contains the HMAC signature. This beta scenario verifies that the client gets the HMAC key from the server and uses it to authenticate.

You generate the HMAC key by using the Administration Console. This beta scenario verifies that any ongoing client connections are torn down with an OpenVPN error and that subsequent connections are successful.

4.3.1 Assumptions

The HMAC key is applicable only for Enterprise mode clients.

4.3.2 Known Issues

None.

4.3.3 Procedure

1 Log in to the Administration Console.

2 Click *Devices > SSL VPNs > Edit > Basic Configuration*.

3 In the Other Configuration section, set the *Authentication Hardening* option to *On*.

   The *Re-generate* button appears beside the option with the current time stamp.

4 Click *OK*.

5 Update the SSL VPN server.

6 As an Enterprise client, connect to SSL VPN server by using the published SSL VPN URL.

7 In the Administration Console, click *Devices > SSL VPNs > Basic Configuration*.

8 Click *Regenerate for HMAC*, then click *OK*.

9 Update the SSL VPN server.

10 From another client machine, connect to the SSL VPN server.

4.3.4 Test Results

In the above scenario, the first client should successfully connect after the *Authentication Hardening* is enabled.

When you click *Re-generate*, the first client connection should be terminated.

The second client connection should be successful.

4.3.5 Troubleshooting Tips

At the server:

- Check the `/etc/opt/novell/sslvpn/config.xml` file to verify that the following lines are in the file:

  ```
  <EnableHMACKeyForTLS>true</EnableHMACKeyForTLS>
  <HMACKeyForTLS LastModified="<time stamp>"><HMAC key></HMACKeyForTLS>
  ```

- Check that the `/opt/novell/sslvpn/hmac.key` file holds the same HMAC key as in the `config.xml` file.
- After regenerating the key, the time stamp should change appropriately. The `config.xml` file and the `hmac.key` file should be updated with a new key.

At the client:

- Check the OpenVPN logs and verify that the HMAC key (and the size of the key) is used every time a connection is made.
- When the key is regenerated, the client connection should terminate, and you should see an HMAC authentication failure in the OpenVPN logs at the client and server.

4.4 IP Range Support in Traffic Policies

In the previous releases of Access Manager, a single traffic rule for the SSL VPN could be configured to allow or deny access to one destination IP or network. In the 3.1 SP2 release, you can configure a traffic rule to allow or deny access to multiple destinations.

A destination can be one of the following:

- A single Host IP address
- Range of IP addresses
- Network/mask
- Full tunnel

4.4.1 Assumptions

You have an understanding of how to configure SSL VPN traffic policies through the Administration Console. For more information on configuring traffic rules, see "Configuring Traffic Policies" (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpnhelp/data/trafficpolicy.html) in the *SSL VPN Server Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpnhelp/data/bmr43tr.html).

4.4.2 Known Issues

For this beta release, there is no limit on the number of destination address entries for a single rule. After this beta, a limit will be introduced.

4.4.3 Procedure

1. Log in to the Administration Console.
2. Click *Devices* > *SSL VPNs* > *Edit* > *Traffic Policies*.
3. Click the policy to be modified.
4. In the *Destination Addresses* field, add, remove, or modify the address entries.

   A destination address entry can be one of the following:

   - A single host IP address, such as `192.168.45.1`
   - A range of IP addresses in the same subnet, such as `192.168.46.8-192.168.46.21`
   - A network or mask, such as `192.168.47.0/255.255.255.0`
   - A full tunnel, such as `0.0.0.0`
5. Modify the other parameters in the rule as needed.
6. Click *OK* to save the changes.
7. Update the SSL VPN server.
8. From an SSL VPN client, try to establish a connection from an IP address that conforms to the policy.
9. From an SSL VPN client, try to establish a connection from an IP address that does not conform to the policy.
10. Verify that the access policies are enforced for the multiple destination addresses according to the configured rule.

4.4.4 Test Results

The policy to allow or deny access should be effective for all the applications, servers, and machines where the IP address matches the single destination IP address, belongs to the range of destination IP addresses, or belongs to the network of destination IP addresses that were configured in the traffic rule.

4.4.5 Troubleshooting Tips

- Check the tunnel logs on the client and server.
- Check the policy resolver and service logs in Kiosk mode.

4.5 Support for New Operating Systems

With Access Manager 3.1 SP2, the SSL VPN server introduces support for new client and server operating systems and for new browsers:

- The following client operating systems are now supported:
  - Windows 7 (32-bit and 64-bit)
  - MAC 10.6 Snow Leopard
- Kiosk mode is now supported on the SUSE Linux Enterprise Desktop (SLED) 11 64-bit client.
- The SSL VPN server can now be installed and configured on SLES 11.
- Internet Explorer 8 and Mozilla* Firefox* 3.5 browsers are now supported.

4.5.1 Assumptions

- You have an understanding of how to configure the SSL VPN server by using the Administration Console.
- You have access to the SSL VPN Server Guide (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpnhelp/data/bmr43tr.html).
- You have access to the SSL VPN User Guide (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpnclienthelp/data/bookinfo.html).
- Kiosk mode is not supported on 64-bit Windows clients.

4.5.2 Known Issues

In a Windows 7 32-bit client, the Internet Explorer 8 browser cannot be used in the Kiosk mode to access HTTP data to the protected Web servers. However, Internet Explorer 8 can be used to establish the SSL VPN connection, and the Mozilla Firefox browser can be used to access HTTP data. The Enterprise mode works without problems.

4.5.3 Procedure for Using New Client Supported Operating Systems

1. Configure the SSL VPN Server:
   - **1a** Log in to the Administration Console.
   - **1b** Configure traffic policies to access the protected servers.
   - **1c** Configure Client Integrity Check policies to check for antivirus/firewall and verify the integrity of client workstations.
   - **1d** Configure the client cleanup options.
   - **1e** Update the SSL VPN server.
2. From a Windows 7 machine (32-bit or 64-bit), establish a client connection:
   - **2a** Use Internet Explorer 8 or Firefox 3.5 to connect to the SSL VPN server in Enterprise mode.
   - **2b** Verify that the client integrity check policies are enforced.
   - **2c** Verify that the traffic policies are enforced by accessing the application servers in the protected network.

2d Log out of the session and verify that the client cleanup options are enforced by verifying the browser private data and Java* cache.

2e Verify the above scenario in Kiosk mode from a 32-bit Windows 7 client.

3 From a Macintosh 10.6 Snow Leopard machine, establish a client connection:

3a Use the Safari browser to connect to the SSL VPN server in Enterprise mode.

3b Verify that the client integrity check policies are enforced.

3c Verify that the traffic policies are enforced by accessing application servers in the protected network.

3d Log out of the session and verify that the client cleanup options are enforced by verifying the browser private data and Java cache.

3e Verify the above scenario in Kiosk mode.

4 From a SLED 11 64-bit client, establish a client connection:

4a Use the Mozilla Firefox browser to connect to the SSL VPN server in Kiosk mode.

4b Verify that the client integrity check policies are enforced.

4c Verify that the traffic policies are enforced by accessing application servers in the protected network.

4d Log out of the session and verify that the client cleanup options are enforced by verifying the browser private data and Java cache.

4.5.4 Test Results for New Client Operating Systems

- In each of the clients, the browser should be able to successfully establish the SSL VPN session.
- Client integrity check policies should be enforced properly.
- Traffic policies should be enforced. The client should be allowed or denied access to the various application servers in the protected network according to the traffic policies.
- After session logout, the browser private data and Java cache should be cleared according to the configured client cleanup options.

4.5.5 Procedure for Using the SSL VPN Server on a New Operating System

1 Install the SSL VPN server on a SLES 11, 64-bit or 32-bit operating system.

For instructions, see the *SSL VPN Server Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpn_serverguide/data/).

2 Log in to the Administration Console.

3 Configure the traffic policies, client integrity check policies, and client cleanup options.

4 Update the SSL VPN server.

5 Make a client connection to the server.

6 Access the application servers in the protected network.

4.5.6 Test Results for New Server Operating Systems

- The SSL VPN server should be successfully installed and imported into the Administration Console.

- The server should be updated with the latest configuration when changes are applied from the Administration Console.
- Clients should be able to successfully establish connections to the server.
- Client integrity check policies and traffic policies should be properly enforced on the client.

4.5.7 Troubleshooting Tips

- If the client connection fails, check the logs. Check the browser agent logs and the respective components for more details on the error.
- If the server is not responding, check the server logs in the following locations:

```
/ar/opt/novell/tomcat5/logs/catalina.out
/ar/log/messages
/ar/log/novell-openvpn.log
/ar/log/stunnel.log
```

4.6 MD5 Checksum in Client Integrity Check Policies

The Client integrity check enforcement for the application definition type of AbsoluteFile has been extended to use MD5 checksum. With this change, you can now use the file name as well as the MD5 checksum value of the file to verify the client integrity.

4.6.1 Assumptions

None.

4.6.2 Known Issues

None.

4.6.3 SSL VPN Server Procedure

1. Log in to the Administration Console.
2. Click *Devices* > *SSL VPNs* > *Edit* > *Client Integrity Check Policies*
3. Create new policies for different operating systems.

   For example:

   3a Select *Windows OS*.

   3b Create a Category and Application named `test`.

   3c Create an Application definition for an AbsoluteFile with the following attributes and values:

   ```
   Name: c:\test\test1.exe
   Version: HashMD5:253627d4dbb0e7a177a2b1a0e0ba8ae8
   ```

   The MD5 checksum is automatically calculated if the file is provided through the *Browse* button.

   3d Click *OK* and save the policy.
4. Create policies for Linux and Macintosh.
5. Save the policies and assign them to a Security Level.
6. Update the SSL VPN server.

4.6.4 Client Procedure

The following steps are for a Windows client. Similar steps can be performed on a Linux or Macintosh client.

1. Verify that the `c:\test\test1.exe` file exists on the Windows client.
2. Verify that the MD5 checksum of `test1.exe` is same as the one defined on the server.
3. On the client machine, open a browser and connect to the SSL VPN server.
4. Access the CIC log and verify that the client integrity check passed.
5. Log out of the SSL VPN connection and close the browser.
6. Insert or delete one or more characters from the `test1.exe` file.
7. Connect to the SSL VPN server again.
8. Access the CIC log and verify that the client integrity check failed.

   The Client Integrity Check policies can be associated with security levels which in turn can be associated with the traffic policies. To see the complete impact of CIC check failures, create the associations and then test them.

4.6.5 Test Results

The client integrity check should pass only when the name and MD5 checksum of the file on the client is the same as the definition on the SSL VPN server.

4.6.6 Troubleshooting Tips

- If you initially had a file whose MD5 checksum was calculated on the SSL VPN server, then the file was transferred to the client, the file's checksum might get changed. One of the reasons for this could be that a binary file was transmitted in ASCII mode.
- Ensure that the filename and the path are correct.
- Ensure that the application definition as well as the category are enabled. The category is disabled by default.

4.7 Translating the Port on the ESP-Enabled SSL VPN Server

The Tomcat bundled with Access Manager does not run with root or administrative privileges, and it must use ports above 8000. Therefore, Tomcat listens on ports such as 8080 and 8443 and cannot listen on the standard HTTP and HTTPS ports, namely port 80 and 443. With the 3.1 SP2 release, the ESP-enabled SSLVPN provides an option to translate the listening port to a standard listening port.

4.7.1 Assumptions

- Supported only on the ESP-enabled SSL VPN server.
- You have installed the 3.1 SP2 version of the Administration Console. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).

- You have installed and configured 3.1 SP2 version of the Identity Server. For installation information, see the *Access Manager Installation Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/installation/data/bookinfo.html).
- You have installed and configured 3.1 SP2 version of the ESP-enabled SSL VPN server. For installation and configuration information, see the *SSL VPN Server Guide* (http://www.novell.com/documentation/beta/novellaccessmanager31/sslvpn_serverguide/data/).

4.7.2 Known Issues

None.

4.7.3 Procedure

1. Log in to the Administration Console.
2. Select the ESP-enabled SSLVPN server, then click *Edit*
3. Select *Authentication Configuration*.
4. Specify details of the Embedded Service Provider Base URL.

   For this beta scenario, select HTTP and specify port 80.
5. Select the *Enable Port Translation* option.
6. In the *To* field, specify the port Tomcat listens on.

   For this beta scenario, specify 8080.
7. Click *OK* twice, then update the SSL VPN server.
8. From a client, establish a SSL VPN connection using port 80.

   The operating system translates the request for port 80 to port 8080 before sending it to Tomcat.

4.7.4 Test Results

An SSL VPN client can connect using port 80 rather than port 8080.

4.7.5 Troubleshooting Tips

Run the `iptables` command on the SSL VPN server and verify that the proper port translation entries are available.

5 Documentation Conventions

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

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

6 Legal Notices

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

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

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

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

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

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