AUTHORIZED DOCUMENTATION

Integration Guide

Novell®
Compliance Management Platform

1.0

November 25, 2008

www.novell.com

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide provides example solutions that you can implement when using the products available in the Novell® Compliance Management Platform. The guide is organized as follows:

Audience

This guide is intended for partners, consultants, and customers who are extremely familiar with the following Novell products:

- Identity Manager
- Access Manager
- Sentinel™
- eDirectory™
- iManager
- Identity Manager Resource Kit
- Analyzer for Identity Manager

Documentation Updates

For the most recent version of this document, see the Novell Compliance Management Platform documentation Web site (http://www.novell.com/documentation/ncmp10/)

Additional Documentation

For additional documentation, see the Novell Documentation Web site (http://www.novell.com/documentation).

Documentation Conventions

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

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

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Introduction

1

The Novell® Compliance Management Platform delivers business process automation that provides users with the appropriate resources, validated in real time to ensure compliance to company policy. The platform enables you to provision users based on how you do business, secure both Web and Client applications by granting access to users based upon provisioning policy, and monitor and validate user and system activity in real time with automated, policy-based corrective actions for non-compliant activities.

The platform consists of a set of core products, integration resources, and deployment resources.

1.1 Core Products

The following products form the core of the Novell Compliance Management Platform:

- **Identity Manager 3.6:** Identity Manager provides user provisioning and password management. You can automate the provisioning and deprovisioning of user accounts and the managing of passwords and user data throughout your organization's directories, applications, databases, and OS platforms. Through streamlined user administration and processes, Identity Manager helps organizations reduce management costs, increase productivity and security, and comply with government regulations.

  Identity Manager includes the Roles Based Provisioning Module 3.6.1 and Designer 3.0. The provisioning module enables a variety of identity self-service and roles provisioning tasks, so users can initiate provisioning and role assignment requests and approvers can manage the approval process for these requests. Designer 3.0 helps you design and deploy your Identity Manager system.

  For more information about Identity Manager, see the Identity Manager 3.6 documentation site (http://www.novell.com/documentation/idm36).

- **Access Manager 3.0.4:** Access Manager provides access management for network content, applications, and services across a broad range of platforms and directory services. With Access Manager, you can deliver simple access to employees, customers, and partners by using standards-based access management technologies that make it easy to securely share identity information across business and technical boundaries. In addition, you can enable single sign-on, which means your employees and partners only need to remember one login for authorized access to all corporate Web-based applications.

  For more information about Access Manager, see the Access Manager 3.0.4 documentation site (http://www.novell.com/documentation/novellaccessmanager).

- **Sentinel 6.1:** Sentinel™ provides a real-time, holistic view of security and compliance activities across your IT environment. Sentinel replaces labor-intensive manual processes for gathering, responding to, and reporting on security and compliance events—enabling you to manage risk more effectively, cut costs, and use your existing resources more efficiently.

For more information about Sentinel, see the Sentinel 6.1 documentation site (http://www.novell.com/documentation/sentinel61).

- **eDirectory 8.8.3:** eDirectory™ provides an LDAP directory service that forms the foundation of the Novell Compliance Management Platform.

  For more information about eDirectory, see the eDirectory 8.8.3 documentation site (http://www.novell.com/documentation/edir88).

- **iManager 2.7:** iManager is a Web-based administration console that provides customized secure access to network administration utilities and content from any location in the world. Using iManager, you can administer eDirectory and many Novell and third-party products, including Identity Manager.

  For more information about iManager, see the iManager 2.7 documentation site (http://www.novell.com/documentation/imanager27).

1.2 Integration Resources

The following components provide integration of the core products to increase the benefits you receive:

- **Identity Manager Driver for Sentinel and the Sentinel Identity Vault Collector:** The Identity Manager Driver for Sentinel (Sentinel driver) and the Sentinel Identity Vault collector gather identity information for use by Sentinel.

  In some systems, its possible for a single user account to be identified in multiple ways. For example, a Microsoft* Active Directory* account can be identified by its SAM account name (jsmith), its user's principal name (jsmith@company.com), and its LDAP distinguished name (cn=John Smith,cn=users, dc=company, dc=com). The Identity Manager Driver for Active Directory gathers these account identifiers and stores them on an Identity Vault user account that is associated with the Active Directory account. The Sentinel driver sends the identity information to the Identity Vault collector. Whenever an Active Directory event occurs that contains one of the identities, the Identity Vault collector injects the common identity (Identity Vault user identity) into the event so that events tracked through any of the identities are correlated with a single user in Sentinel views and reports.

  For more information about the Sentinel driver and the Identity Vault collector, see the *Identity Manager 3.6 Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

- **Identity Tracking Solution Pack:** The solution pack provides controls (views and reports) of events associated with users. Through these controls, you can monitor and report on account management activities (creation, deletion, and modification); suspicious user activities such as failed authentication, denied access, denied or increased account privileges, and impersonated account logins; account usage by users; and password management activities. Because of the identity injection provided by the Sentinel driver and Identity Vault collector, events are associated to individual users.

  For more information about the Identity Tracking Solution Pack, see the Novell Compliance Management Platform documentation site (http://www.novell.com/documentation/ncmp10).

1.3 Deployment Resources

The following resources are included to help you deploy your Identity Manager 3.6 solution:

- **Identity Manager Resource Kit 1.2:** The Resource Kit provides a VMware* image of a fully developed and deployed Identity Manager 3.6 solution. Also included is a Designer project and documentation that enables you to set up this solution instead of using the VMware image.

  The Resource Kit includes several business solutions that are common to Identity Manager customers, including employee life-cycle management (hire to termination), credential provisioning, and password expiration notification.

  XPOZ (pronounced “expose”) is a test harness for Identity Manager. It is a script interpreter that provides access to a number of applications through their exported API interfaces to allow for in-depth testing of an Identity Manager solution. XPOZ is also included in the Resource Kit.

  For more information about the Resource Kit, see the *Identity Manager Resource Kit 1.2 Overview Guide*.

- **Analyzer 1.0:** Analyzer for Identity Manager helps you ensure that general internal policies are adhered to for data quality, which includes data analysis, data cleansing, data reconciliation, and data monitoring/reporting. Analyzer lets you analyze, enhance, and control all data stores throughout the enterprise.

  For more information about Analyzer, see the Novell Compliance Management Platform documentation site (http://www.novell.com/documentation/ncmp10).

Initiating Workflow Approvals for Protected Resources

2

This solution requires Identity Manager, the Identity Manager Roles Based Provisioning Module, and Access Manager.

When users attempt to access a protected resource to which they have not been granted rights, Access Manager denies access. In some cases, a user might not be authorized to access the resource; in other cases, the user might be authorized to access the resource but has not been granted the rights required to gain access.

In either case, the most efficient method of handling the access denied message is to check the user's credentials to validate if he or she should be attempting to access the resource. If not, Access Manager can deny the request. However, if the user does have the credentials to allow access but has not been granted the appropriate approvals, you can implement a workflow process to enable the user to request access.

The following sections outline the sample configuration steps necessary to implement this scenario.

2.1 Assumptions

This scenario assumes the following:

- ❑ You have installed and set up Identity Manager, the Identity Manager Roles Based Provision Module, and Access Manager.
- ❑ The resource protected by Access Manager is based upon a credential of the user. In other words, the user is a member of a group, role, department, or so forth.
- ❑ The workflow process grants the user the necessary entitlement to fulfill the Access Manager Permit policy
- ❑ Although it is not necessary, some form of single sign-on authentication (such as an Identity Injection policy or SAML assertion) can be defined for the Identity Manager User Application so that the user redirection to the workflow process is seamless and does not prompt for additional credentials.

2.2 Configuring the Identity Manager User Application

The following steps explain how to configure the Identity Manager Role Based Provisioning Module so that users who attempt to access to a protected resource can be redirected to a workflow that allows them to initiate a request for access to a protected resource.

1. Log-in to the Identity Manager Role Based Provisioning Module as a UserApp Admin.

2 Click Administration, then click the *Page Admin* tab.

3 Under *Page Actions* (lower left corner), click *New* to create a new page.

4 Fill in the following page properties:

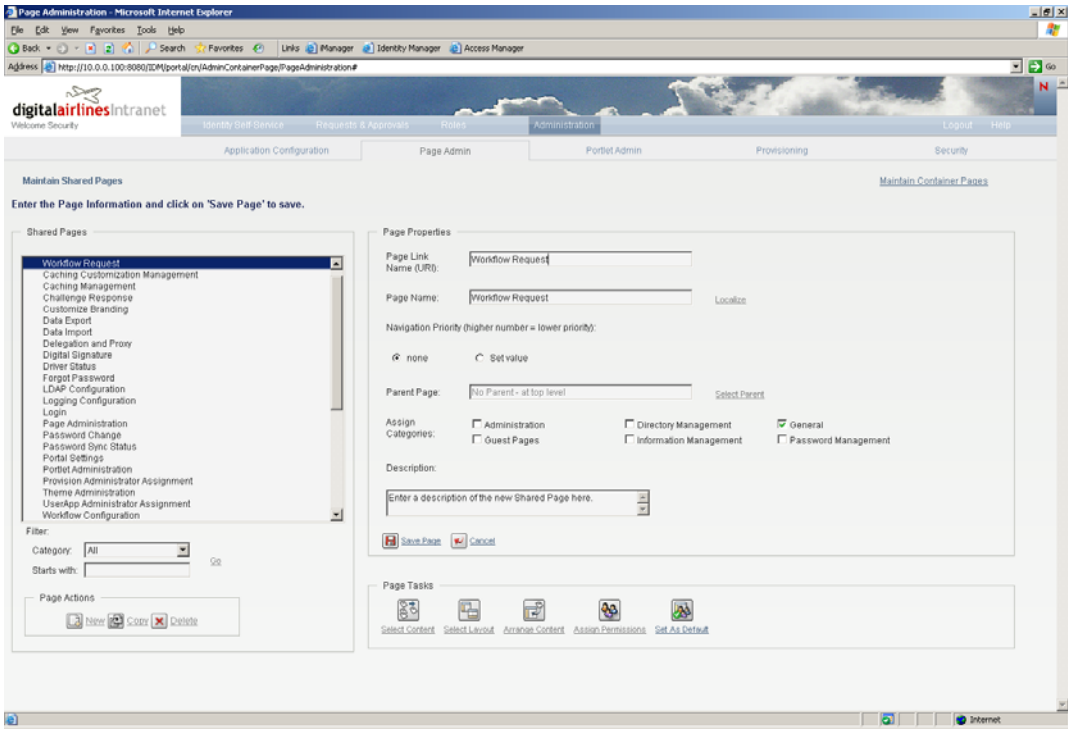
Page Link Name (URI): Specify a name for page link (for example, Workflow_Request).

Page Name: Specify a name for the page. By default, the page name is populated with the same name you entered for the page link name.

Assign Categories: Select the *General* option.

5 Click *Save Page*.

The resulting page looks similar to the following example:

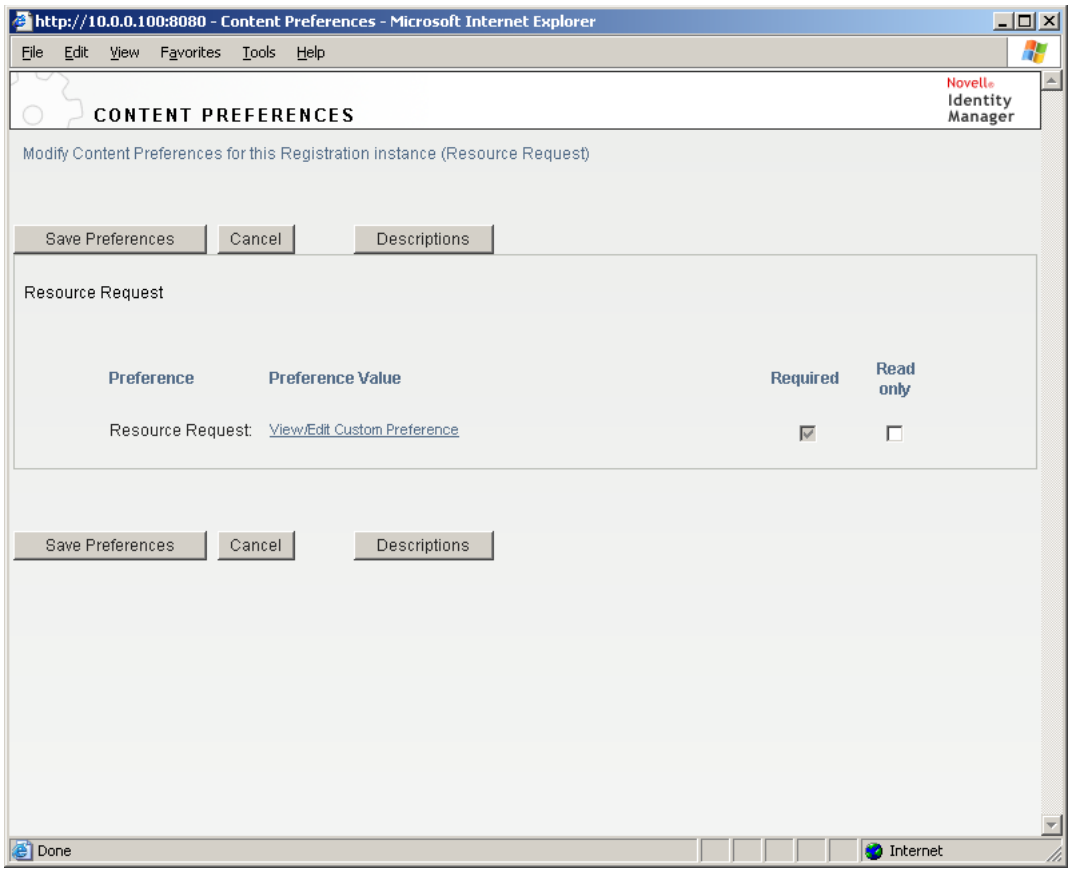


6 Under *Page Tasks*, click *Select Content* to display the Content Selector window.

7 In the *Available Content* list, select *Resource Request*, then click *Add* to move it to the *Selected Content* list (as shown in the above example).

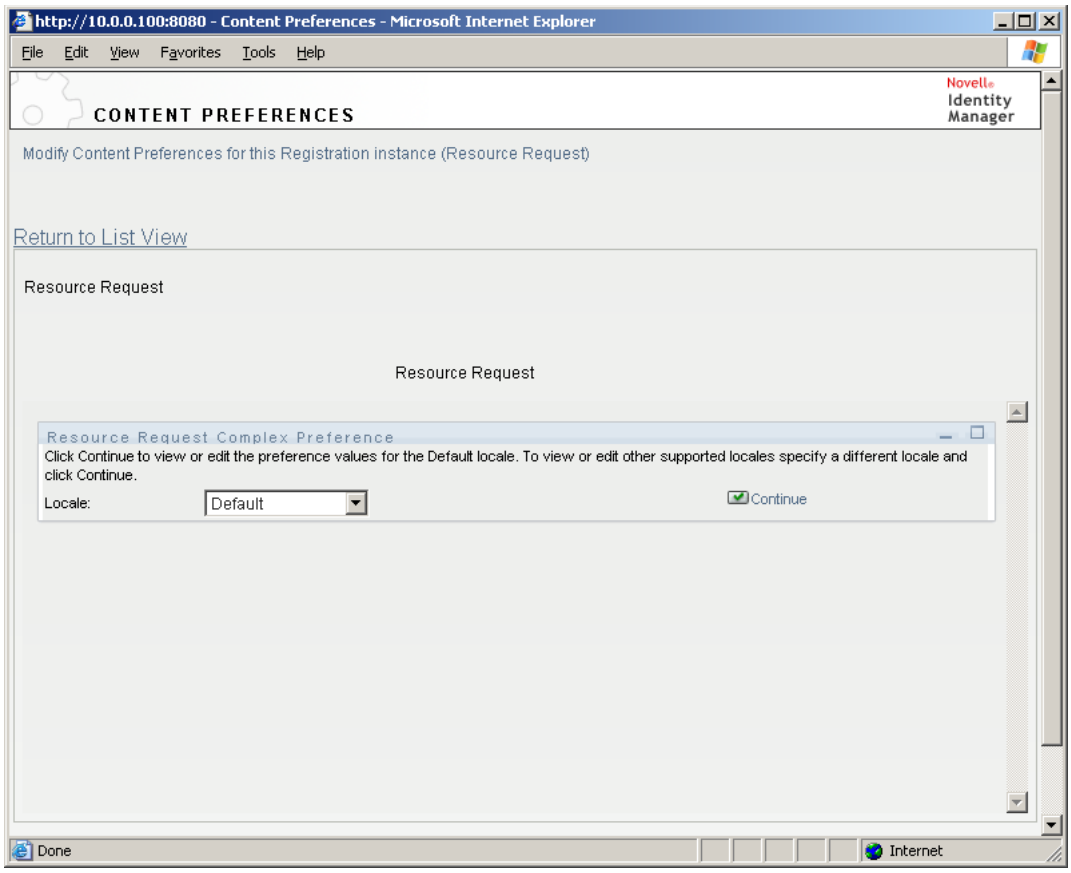
8 Select *Content Preferences*, then click *OK* when prompted to save your changes.

The Content Preferences window is displayed.



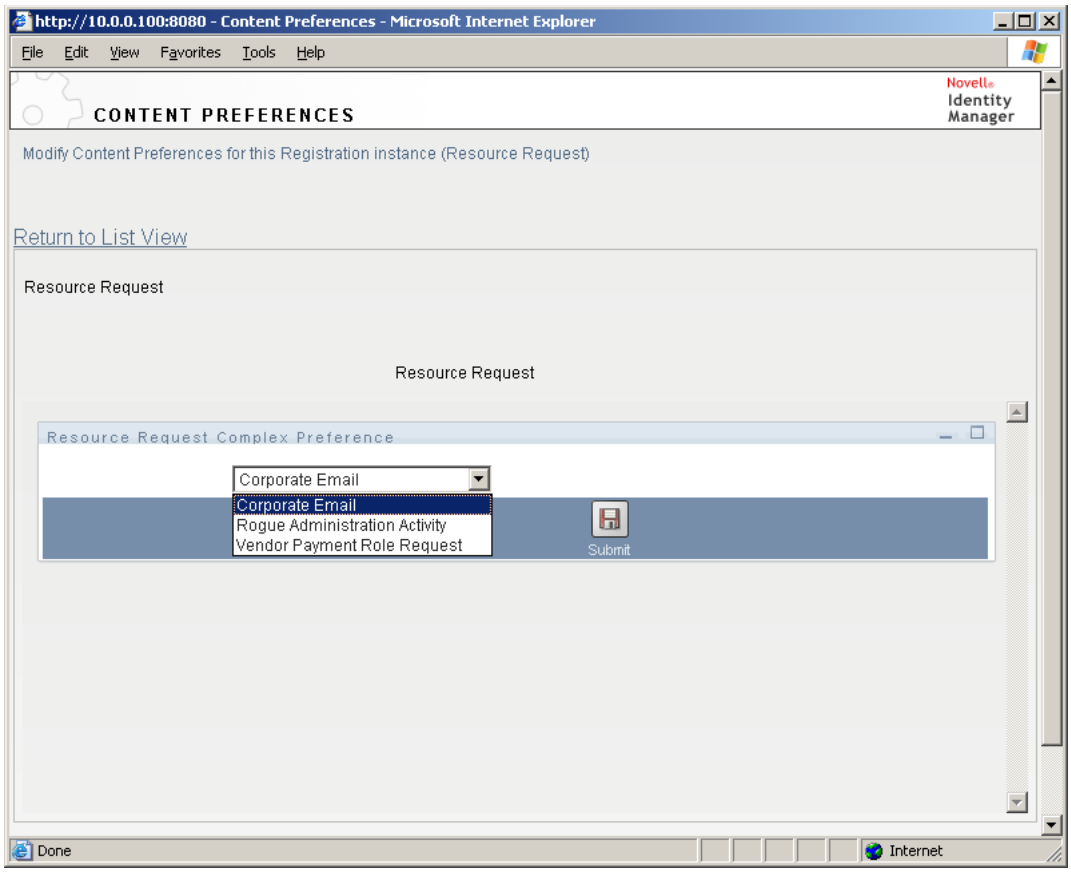
9 In the Content Preferences window, click *View/Edit Custom Preferences*.

The Resource Request Content Preferences box is displayed.

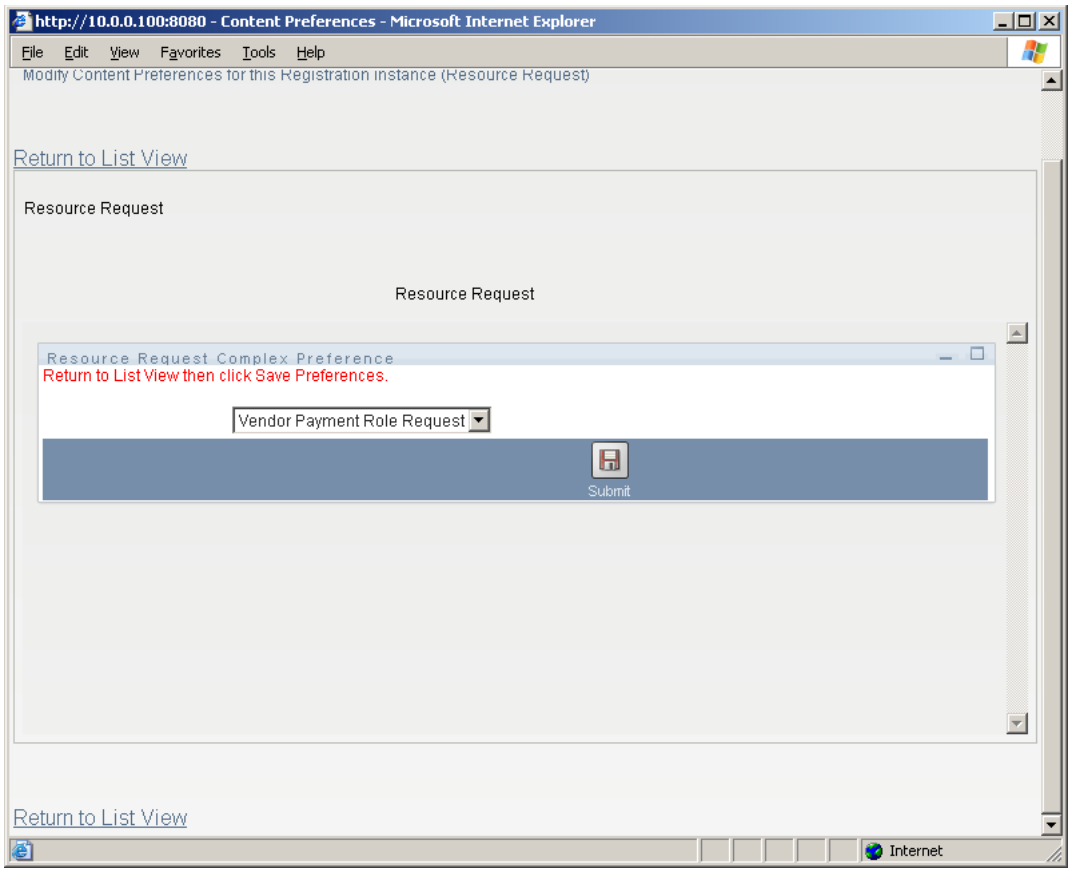


10 Click *Continue* to edit the Default locale, or, if necessary, select a different locale, then click *Continue*.

11 In the *Resource Request Complex Preference* list, select the workflow that you previously defined , then click *Submit*.

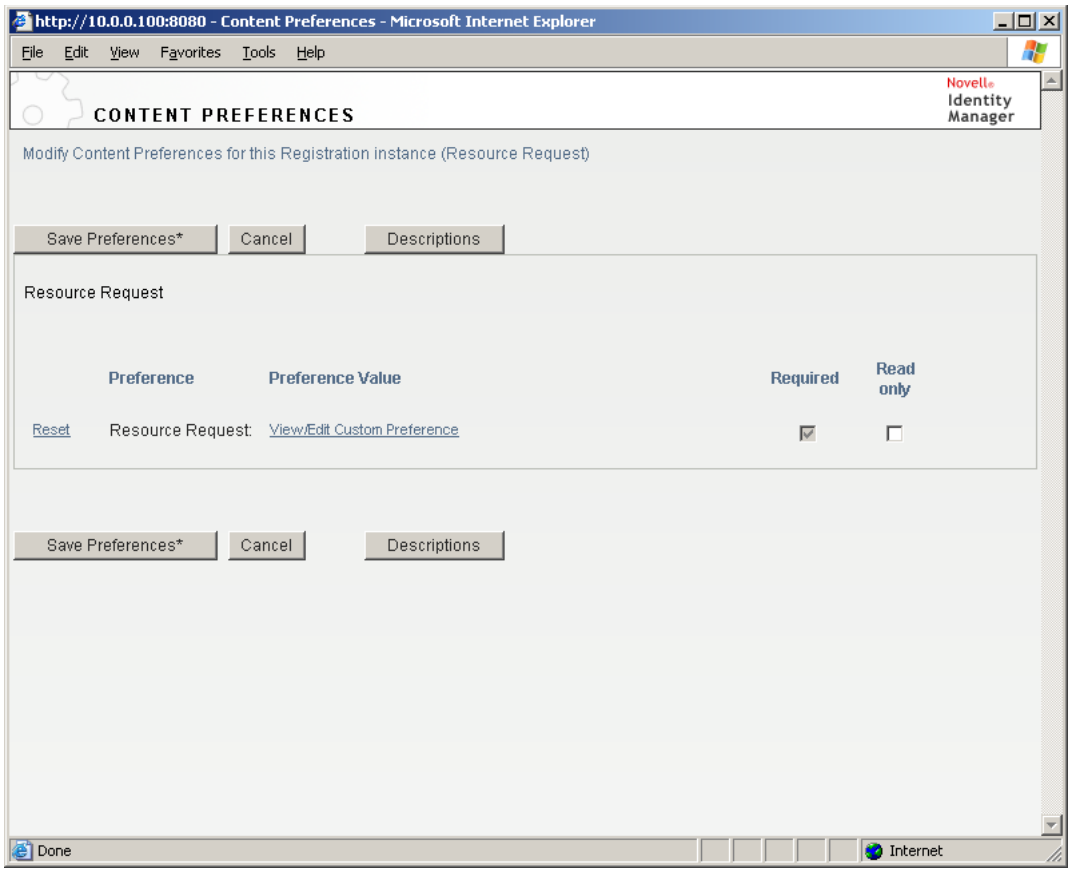


As shown in the following screen shot, you are prompted to return to the List View and save your preferences.

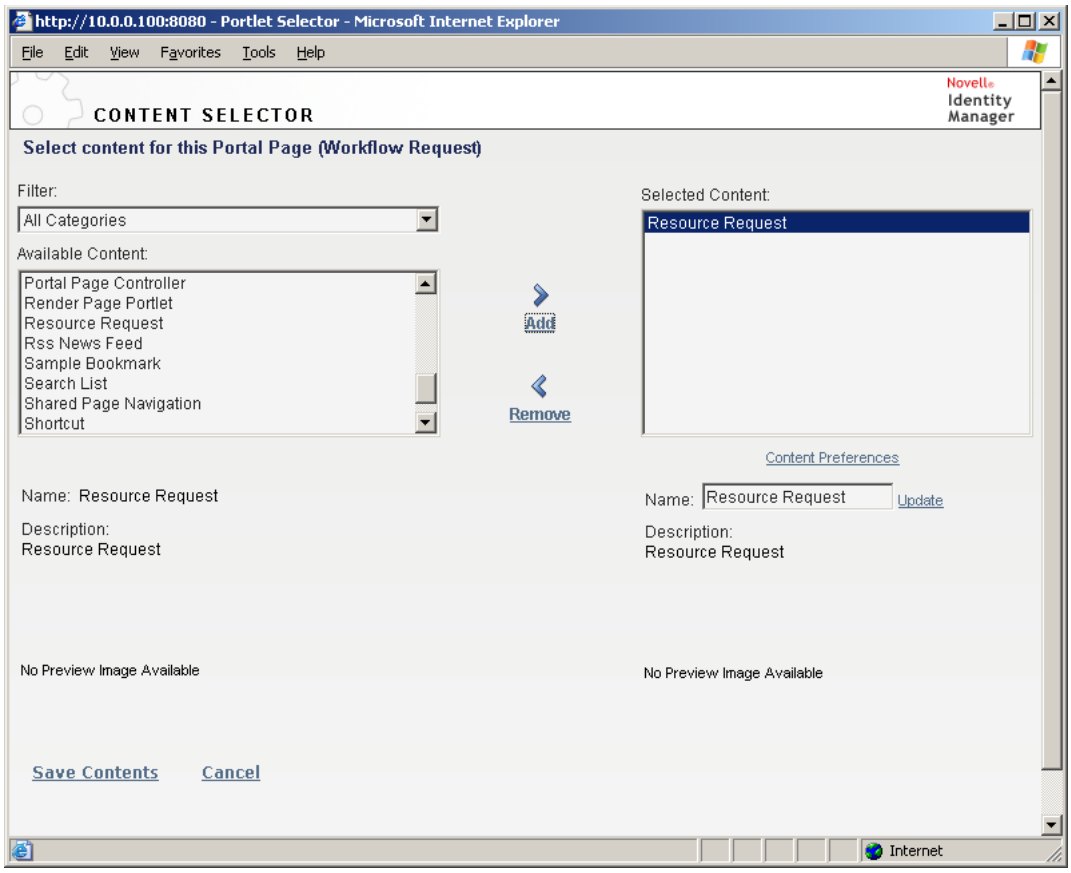


12 Click *Return to List View*.

13 Click *Save Preferences* to save the preferences and return to the Content Selector window.

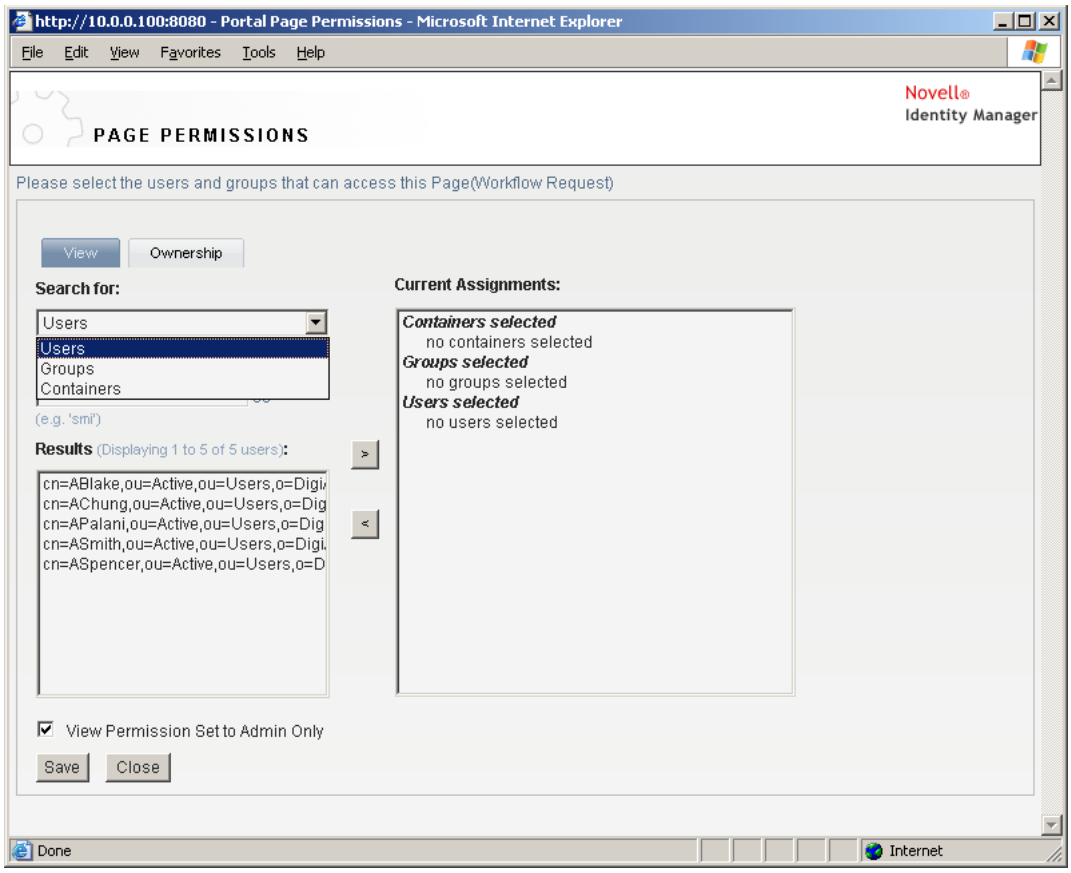


14 Click *Save Contents* to save the page contents and return to the Page Admin window.



15 Under *Page Tasks*, click *Assign Permissions* to display the Page Permissions window.

The Page Permissions window lets you give users permissions to view the newly created page.



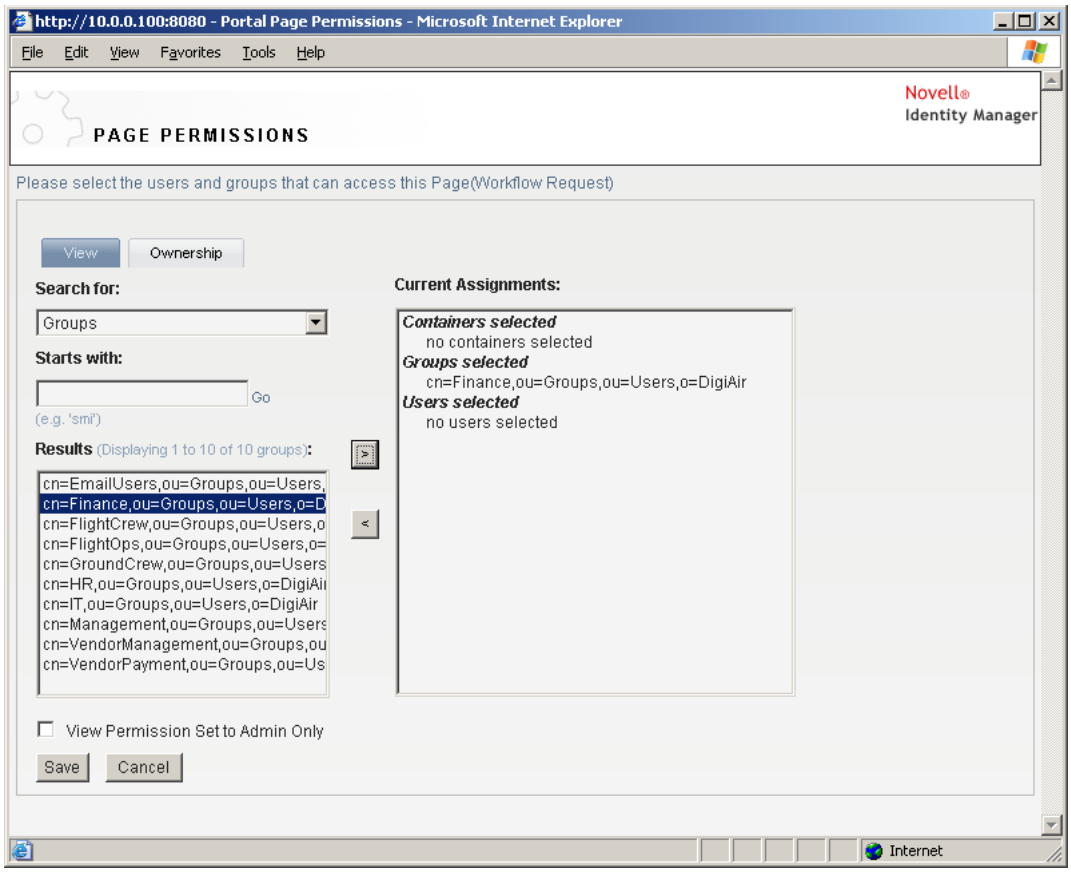
16 In the *Search for* list (located on the *View* tab), select *User*, *Group*, or *Container* as appropriate.

17 Enter search criteria in the *Starts with* field to narrow the search, then click *Go*.

or

To list all results, leave the *Starts with* field blank, then click *Go*.

18 After the results are displayed in the *Results* list, select the appropriate entity (or entities) to assign permissions to, then click the > button to add them to the *Current Assignments* list.



19 Verify that the *View Permission Set to Admin Only* option is not checked.

20 Click *Save*.

21 Click *Close*.

You have successfully set up the workflow page that you can redirect users to if they select the option to initiate the request process to gain approval to access this resource. You can access the workflow request directly at the following URL:

http://*ipaddress:port*/IDM/portal/cn/DefaultContainerPage/*Workflow_Request*

Replace *ipaddress:port* with the appropriate information for your environment. Replace *Workflow_Request* with the page link name you used in Step 4 on page 14.

Continue with Section 2.3, “Configuring Access Manager,” on page 22 for information on how to redirect a user to the workflow page you just created.

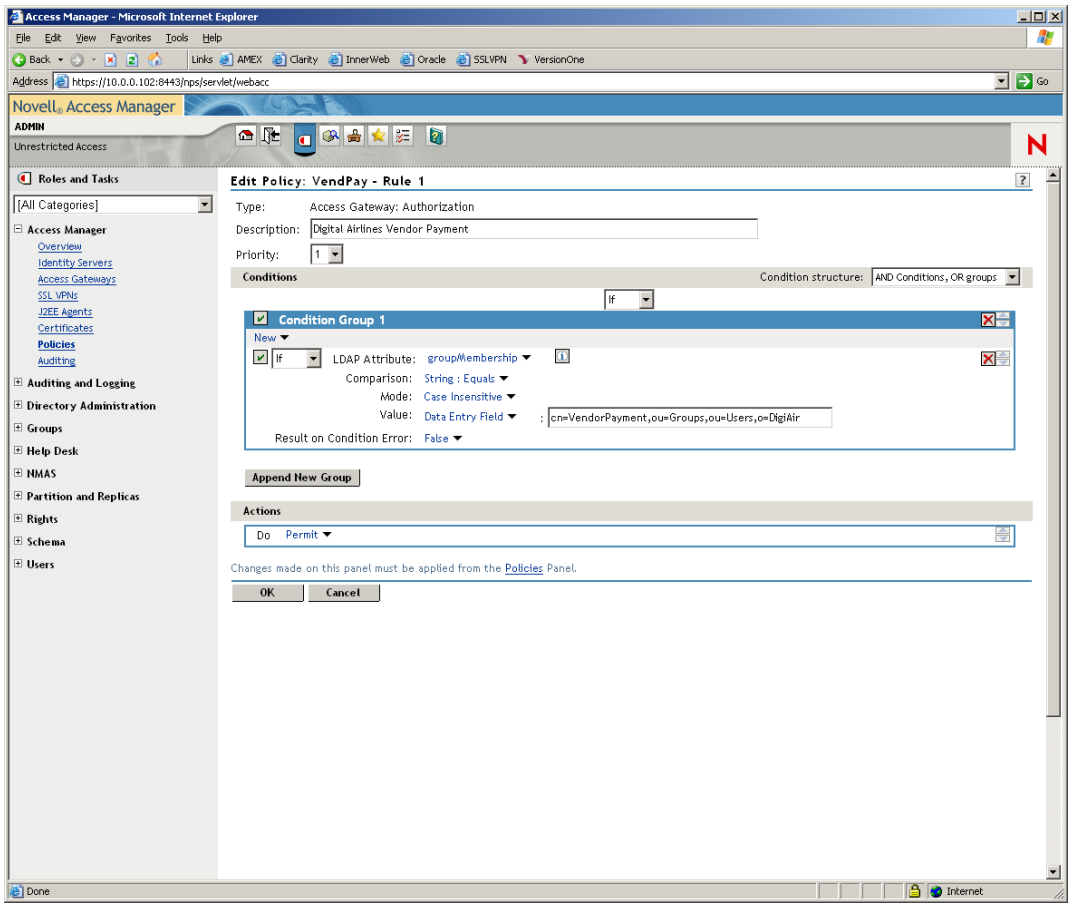
2.3 Configuring Access Manager

The following steps explain how to configure Access Manager to redirect a user to an Identity Manager workflow/approval process.

1 Configure a protected resource as directed in the Access Manager documentation.

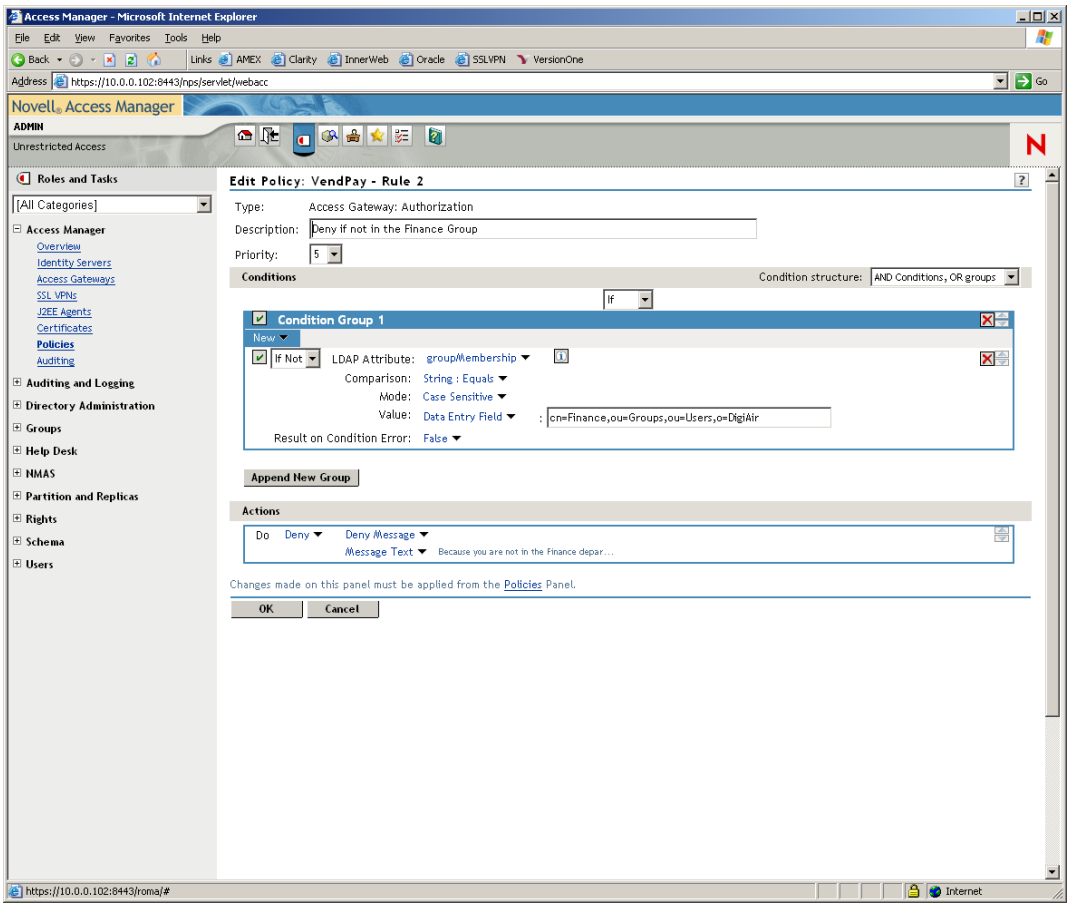
The following steps are example policies that allow access if users meet the criteria, request access if certain criteria are met or, deny access if users do not meet criteria and should not given the opportunity to request access.

2 Create a Permit rule similar to the one in the following example, based upon criteria for the user to be granted access to the resources.

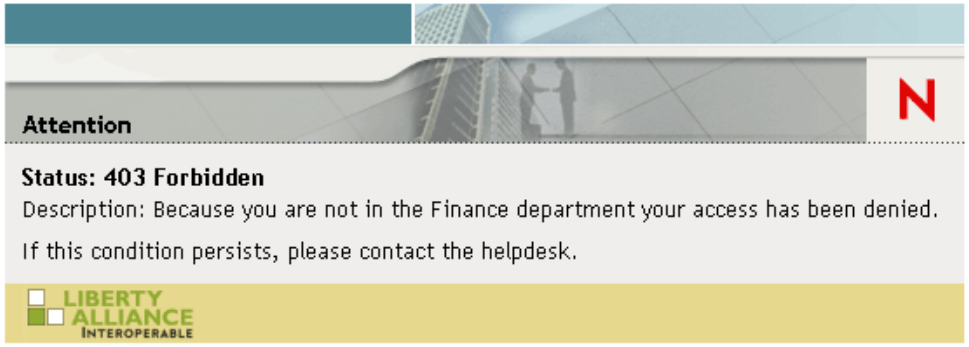


3 Verify that the priority for this rule is the lowest number (in this example, it is 1).

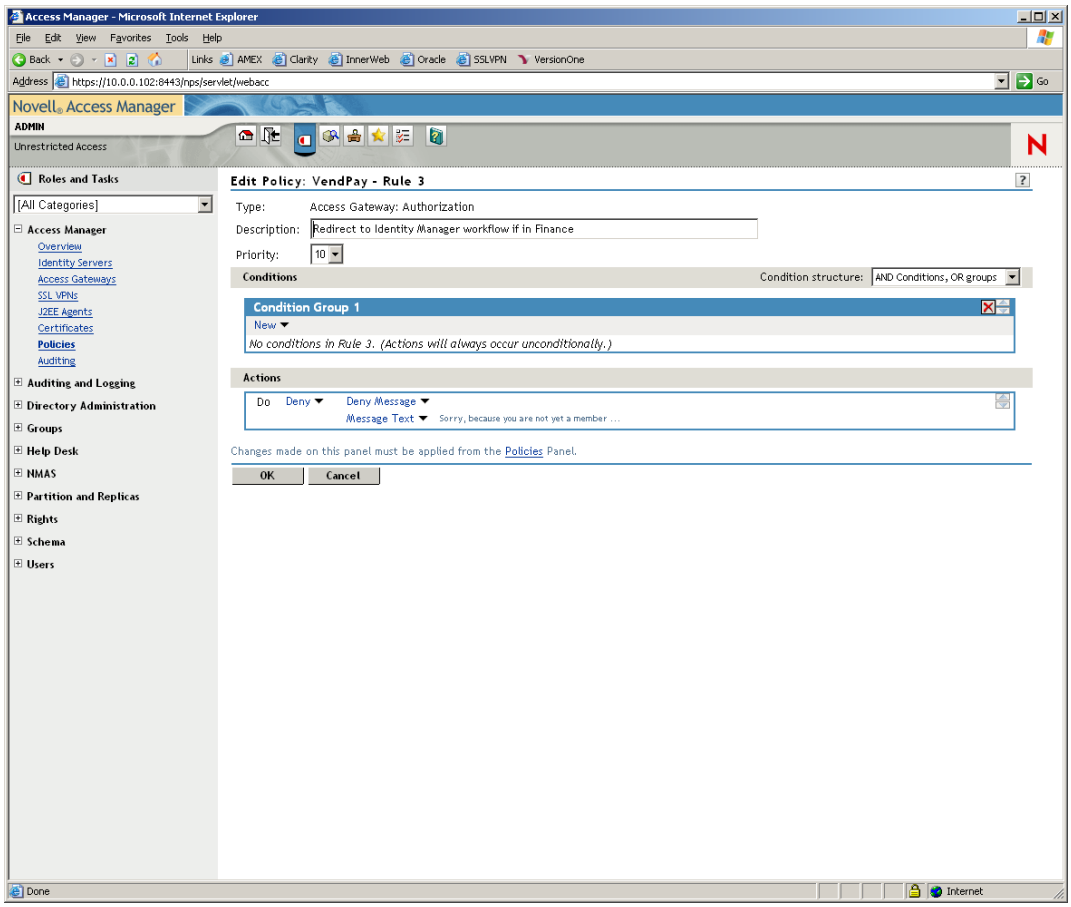
4 Create a Deny rule similar to the one in the following example, based upon criteria for the user to not have access to this resource and to be denied.



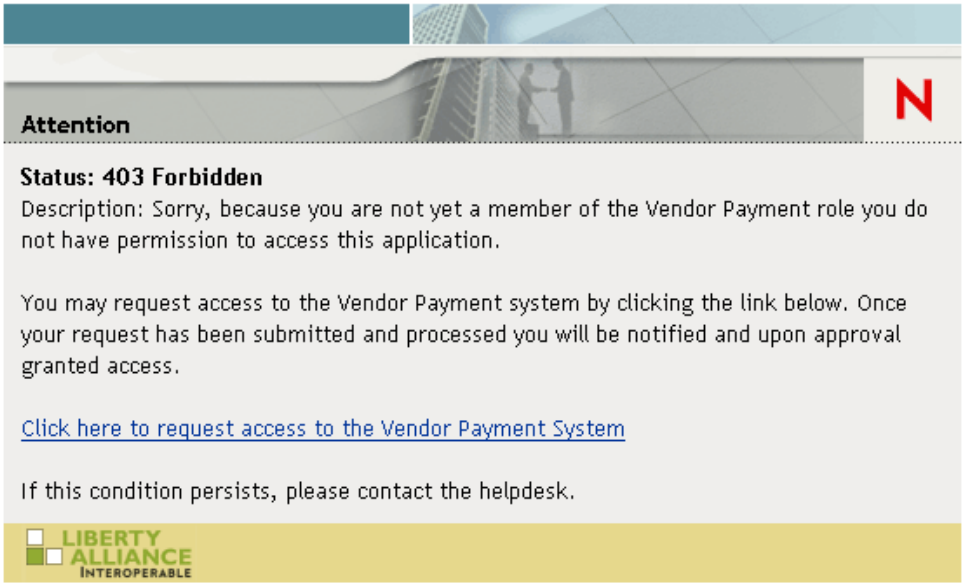
5 Verify that the priority of this rule is the next highest number (in this example, it is 5). The message text of this policy should state why the user has been denied access, for example:



6 Create a Deny policy similar to the one in the following examples, based upon criteria that display a message to users explaining why they have been denied access, and providing a link to request access to the resource.



7 Set the priority of this policy to the next highest number (in this example, it is 10). The message text of this policy should state why the user has been denied and how to gain access.



The content of the *Message Text* field looks like the following in HTML:

```
Sorry, because you are not yet a member of the Vendor Payment role you do not
have permission to access this application.
<BR><BR>
You may request access to the Vendor Payment system by clicking the link below.
Once your request has been submitted and processed you will be notified and
upon approval granted access.
<BR><BR>
<A HREF="http://ipaddress:port/IDM/portal/cn/DefaultContainerPage/
Workflow_Request">
Click here to request access to the Vendor Payment System</A>
<BR>
```

Replace `http://ipaddress:port/IDM/portal/cn/DefaultContainerPage/Workflow_Request` with the URL created in the previous section.

3 Synchronizing Identity Manager Forgotten Password Challenge Response with SecureLogin Passphrase

This solution requires Identity Manager and SecureLogin.

Identity Manager and SecureLogin both enable users to recover from forgotten or unknown passwords. Identity Manager uses Challenge Response to enable users to replace a forgotten password, and with a new password. SecureLogin uses Passphrases to enable users to reset a forgotten password or change an old password to a new one.

The Identity Manager Challenge Response and the SecureLogin Passphrase are similar mechanisms. Both use a challenge question and response to authenticate in place of a password and then present the user with an interface to reset the password. For users who manage passwords through both products, maintaining two sets of challenge questions and responses can be confusing.

The following sections provide information to help you configure Identity Manager Challenge Response and SecureLogin Passphrase to use the same challenge questions.

3.1 Setting Up Provisioning of Credentials to SecureLogin

In addition to synchronizing passwords among multiple directories and applications, Identity Manager can provision credentials (for example, application IDs, passwords, and other login data) to SecureLogin through Credential Provisioning policies. This enables you to automate the management of passwords throughout your enterprise, regardless of whether the passwords are used in Identity Manager connected systems or SecureLogin applications.

Synchronizing the challenge questions used by Identity Manager Challenge Response and SecureLogin Passphrase does not require you to have Identity Manager provision credentials to SecureLogin. However, if you are interested in doing so, see the *Novell Credential Provisioning for Identity Manager 3.6* guide.

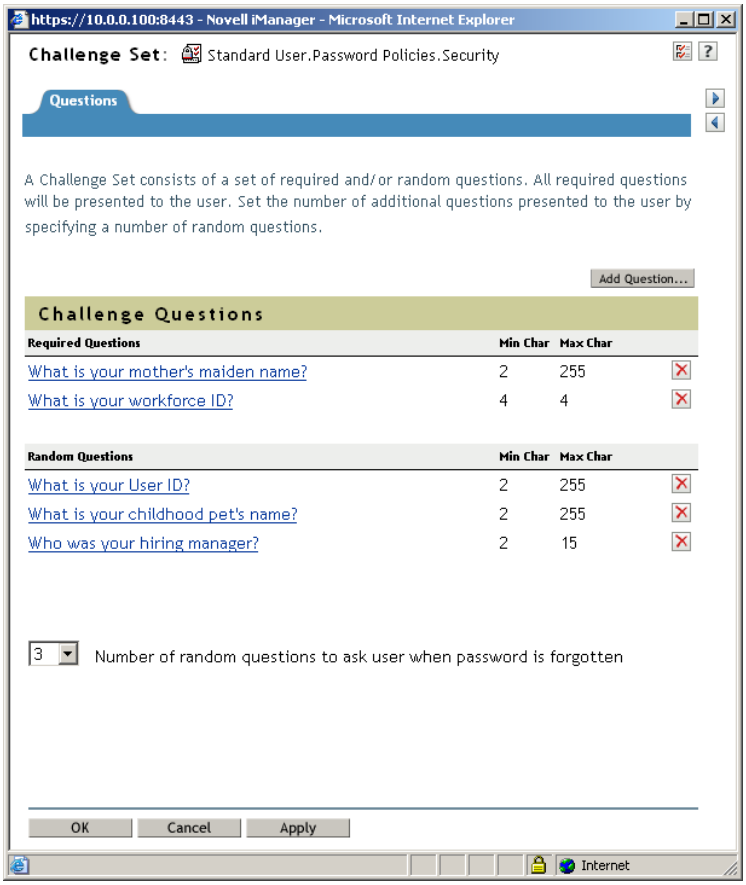
3.2 Configuring Identity Manager Challenge Response

Complete the following tasks to configure questions for Identity Manager Challenge Response:

- Create a Challenge Set (or modify an existing set) that includes a question that has non-subjective response (such as "What is your workforce ID?"). For instructions, see "Managing Forgotten Passwords" (http://www.novell.com/documentation/password_management32/pwm_administration/data/bqf5d1x.html) in the *Novell Password Management 3.2 Guide*.

  Keep in mind the following as you create the Challenge Set:

  - You can use multiple questions.
  - This same questions will be used as the SecureLogin Passphrase questions. The user will need to supply the responses in both Identity Manager and SecureLogin. Therefore, you want the questions to be non-subjective so that the answers are always the same.
  - Do not allow users to set their own challenge questions. Remove any *[User Defined]* required or random questions.



- Assign the Challenge Set to each Password policy that applies to Identity Manager and SecureLogin users. For instructions, see "Managing Forgotten Passwords" (http://www.novell.com/documentation/password_management32/pwm_administration/data/bqf5d1x.html) in the *Novell Password Management 3.2 Guide*.

3.3 Configuring SecureLogin Passphrase

This solution assumes that SecureLogin is used in eDirectory™ mode with or without Novell® SecretStore®.

The following sections provide examples of two methods you can use to configure the SecureLogin Passphrase question so that it is the same as the Identity Manager Challenge Response question. The first method requires manual configuration of the question through iManager. The second method uses Identity Manager policies to automatically provision the Passphrase question.

- Section 3.3.1, "Configuring the Passphrase Question in iManager," on page 29
- Section 3.3.2, "Provisioning the Passphrase Question through Identity Manager," on page 30

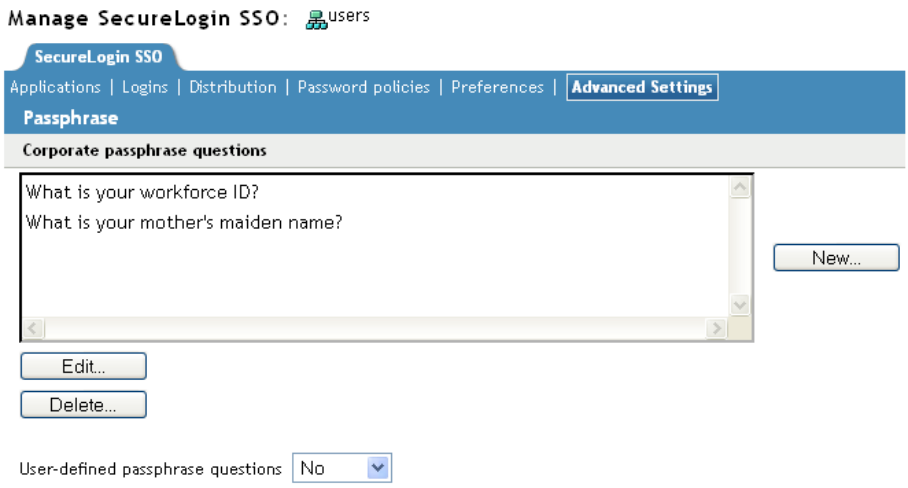
3.3.1 Configuring the Passphrase Question in iManager

Complete the following tasks to configure the Passphrase question in iManager:

- ❑ Create a Passphrase question that is the same as the Identity Manager Challenge Response question. For instructions, see "Creating a Passphrase Question" (http://www.novell.com/documentation/securelogin61/nsl61_administration_guide/data/b9o01em.html) in the *SecureLogin 6.1 Administration Guide*.

  Keep in mind the following as you create the Passphrase question:

  - Passphrase questions can be modified on individual users or on containers. You need to modify the question on whatever combination of objects are required to match the users covered by the Identity Manager Password policies associated with the Challenge Response question.
  - You can use multiple questions, but they must be the same questions that were used in the Identity Manager Challenge Response.
  - Do not allow users to set their own challenge questions. Set the *User-defined passphrase question* option to *No*.



- ❑ Make sure that the Passphrase question and the Identity Manager Password policy are assigned to the same users.

3.3.2 Provisioning the Passphrase Question through Identity Manager

You can use Identity Manager policy to automatically populate the Passphrase question and response. This method not only has the advantage of automation but ensures consistency between the Identity Manager Challenge Response and the SecureLogin Passphrase.

The one limitation of this method is that you can only provision one Passphrase question and response. This means that your Identity Manager Challenge Response can include multiple questions, but your SecureLogin passphrase can include only one question.

Complete the following tasks to provision the Passphrase question:

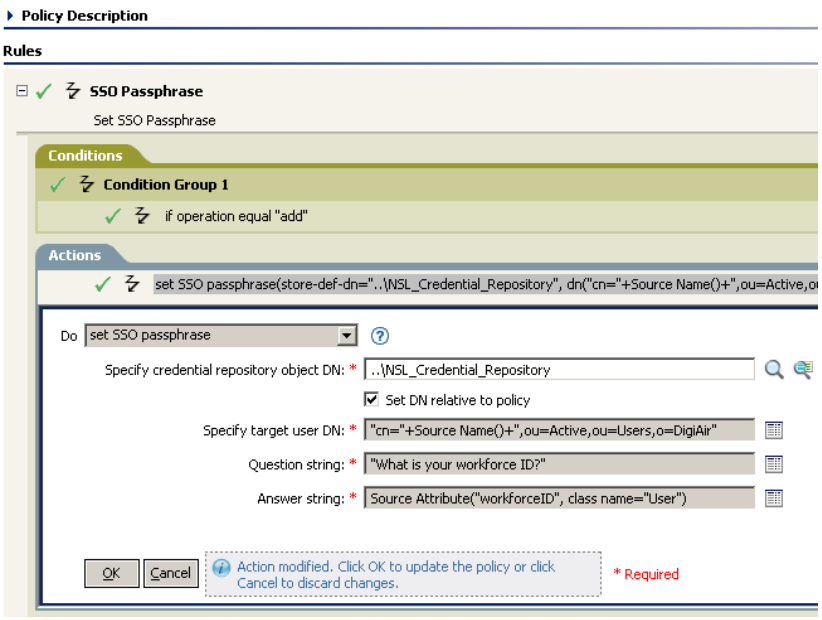
- ❑ Select a driver whose policies you want to modify to initiate provisioning of the Passphrase question.

  For example, if you use a specific driver to add user objects to the Identity Vault, you can modify that driver's policies so that when a new user is added the SecureLogin Passphrase is provisioned.

- ❑ Create the Passphrase provisioning policy. For instructions, see "Creating Credential Provisioning Policies" in the *Novell Credential Provisioning for Identity Manager 3.6* guide.

  Keep in mind the following as you create the policy:

  - The policy must be able to identify the user dn. Make sure the policy is located in a place on the Publisher channel where that information is available.
  - Use the `set SSO passphrase` action to set the Passphrase question and response. Make sure that the question is non-subjective and that the response comes from data that is available on the User object. Using User object data enables you to ensure that the response in both Identity Manager and SecureLogin must be the same.



Reporting when Terminated Users Accessing Company Resources

4

This solution requires Sentinel™ and Identity Manager.

Industry research shows that the biggest threat of data breach is from former employees who attempt to access resources after their employment has ended. This solution allows you to track terminated employees for a set amount of time. If the terminated employee tries to access a resource, then an alert is issued (e-mail or workflow).

The following sections outline the steps required to implement this scenario.

4.1 Assumptions

The steps for this scenario assume the following:

- ❑ Sentinel 6.1 is installed and configured. For more information, see the *Sentinel 6.1 Installation Guide* (http://www.novell.com/documentation/sentinel61/index.html).
- ❑ Install and configure the eDirectory™ Collector. The documentation for the eDirectory Collector is included with the Collector. Download the eDirectory Collector and the documentation from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- ❑ Install and configure the Identity Manager Collector. The documentation for the Identity Manager Collector is included with the Collector. Download the Identity Manager Collector and the documentation from the Sentinel 6.1 Content Web site (http://support.novell.com/product/sentinel/secure/sentinel61.html). For configuration documentation of the Identity Manage Collector with Identify Manager, see the *Identity Manager 3.6 Reporting Guide for Novell Sentinel*.
- ❑ Install and configure event Collectors for all integrated systems that are part of the Identity Manager solution. For example, if you are synchronize Active Directory accounts with Identity Manager, you need to download and configure the Active Directory Services Collector. All Sentinel Collectors are located at the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- ❑ The Identity Tracking Solution Pack is downloaded from the Sentinel Solution Pack Download Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- ❑ Install and configure Identity Manager or use the Resource Kit. For more information, see the *Identity Manager 3.6 Installation Guide* or the *Identity Manager Resource Kit 1.2 Overview Guide*.

The Sentinel rules are dependent upon the business logic that is implemented in the Resource Kit. For more information, see "Business Logic" in the *Identity Manager Resource Kit 1.2 Architecture Reference Guide*.

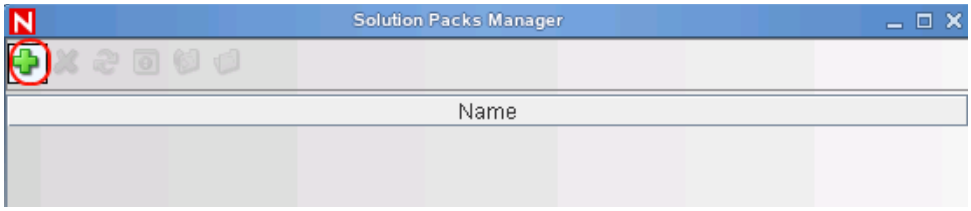
- ❑ The Sentinel driver and Identity Vault Collector are installed and configured. For more information, see the *Identity Manager 3.6 Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

4.2 Installing the Identity Tracking Solution Pack

If you have already installed the Identity Tracking Solution Pack, skip this section and proceed directly to Section 4.3, "Configuring the Global Setup," on page 32.

1. Start the Sentinel Control Center and log in as a user with rights to manage Solutions Packs.

   The Solution Manager option must be checked for the user under *Permissions* > *Solution Pack*.
2. Select *Tools* > *Solution Pack* from the menu to start the Solution Pack Manager.
3. Click *Add* to start the import wizard.



4. Select *Import a solution Pack plugin file (.zip)*, then click *Next*.
5. Browse to and select the Identity Tracking Solution Pack where you downloaded it, then click *Open*.

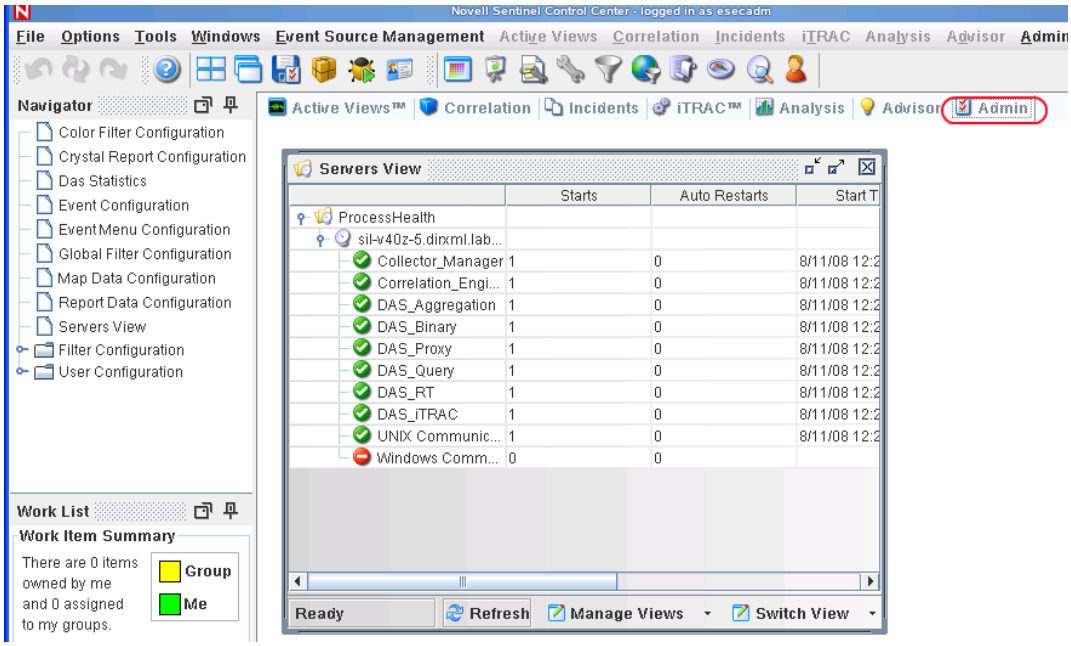
   The filename is `Identity-Tracking_6.1r1.spz.zip`.
6. Review the solution pack directory, then click *Next*.
7. Review the solution pack details, then click *Finish*.

4.3 Configuring the Global Setup

The Identity Tracking Solution Pack requires some global configuration that must be completed. This configuration needs to be completed before any additional configuration. If you have completed these global configuration task for another use case, you can skip this section.

The Sentinel data field must be able to hold Identity Manager attribute data.

1. Start the Sentinel Control Center, then click the *Admin* tab.



2 Select *Admin* > *Event Configuration* from the toolbar.

3 In the left pane, browse to and select *ReservedVar43*.

The tag is rv43.

4 In the *Label* field in the right pane, change the display label to Data, then click *Apply*.

5 Click *Save*, the close the Event Configuration window and reopen it to see the changes take place.

4.4 Installing the Identity De-Provisioning Control

The Identity De-Provisioning Control contains a set of reports and rules to monitor common identity de-provisioning and access violation actions within the enterprise.

- **Employee TerminationViolation:** A report that lists any attempts to access enterprise resources by terminated employees.
- **IdT - Identity Terminated Employees Rule:** A rule that identifies the terminated employees within the enterprise.
- **IdT - Remove Reactivated Employees Rule:** A rule that identifies the reactivated employees within the enterprise.
- **IdT - Unauthorized Access By Terminated Employees Rule:** A rule that identifies unauthorized access by terminated employees within the enterprise.

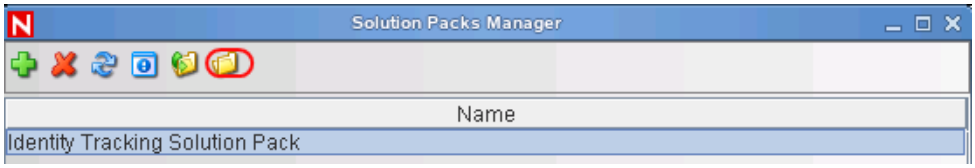
This control makes a series of assumptions about how terminated employees are handled in the enterprise.

1. Terminated employees are simply designated as being no longer employed. The Resource Kit enforces this standard by setting the employeeStatus attribute to Inactive for all terminated employees. For more information about this process, see "Termination Process" in the *Identity Manager Resource Kit 1.2 Architecture Reference Guide*.

   If other methods are used to identify the terminated employees, the IdT - Identify Terminated Employees Rule needs to be modified if your method does not use the employeeStatus attribute.
2. Modifying the status of the employee automatically triggers the disabling of all associated accounts to ensure that the user no longer has access to enterprise resources. If this is not the case in your environment, you might need to modify the IdT - Unauthorized Access By Terminated Employees rule to filter out events from those special accounts. For example, if former employees are still allowed to use an e-mail account.

To install the Identity De-Provisioning Collector:

1. Launch the Solution Manager by selecting *Tools* > *Solution Pack* in the toolbar in the Sentinel Control Center.
2. Select *Identity Tracking Solution Pack*, then click *Open with Solution Manager*.



3. Highlight Identity De-Provisioning in the left pane of the Solution Manager, then click *Install*.
4. Verify that the Identity De-Provisioning Control is listed, then click *Next*.
5. Select your Correlation Engine from the drop-down list as the location where the Identity De-Provisioning rules are installed.
6. Select the *IdT-Unauthorized Access By Terminated Employees (Deployment)*, then click *Next*.
7. Select whether the Crystal server is local or remote by selecting one of the following options:
   - *Publish to Crystal Server*
   - *Install to Local Directory*
8. Specify the following Crystal server information:
   - **Server Name:** Specify the Crystal server DNS name or IP address.
   - **User Name:** Specify an administrative user for the Crystal server.
   - **Password:** Specify the administrative user's password.
9. Click *Next* after you have specified the Crystal server information.
10. Review the contents of the Identity De-Provisioning Control, then click *Install*.
11. Review the installation summary, then click *Finish*.

4.5 Configuring the Identity De-Provisioning Control

There are additional configuration steps required to implement the Identity De-Provisioning Control.

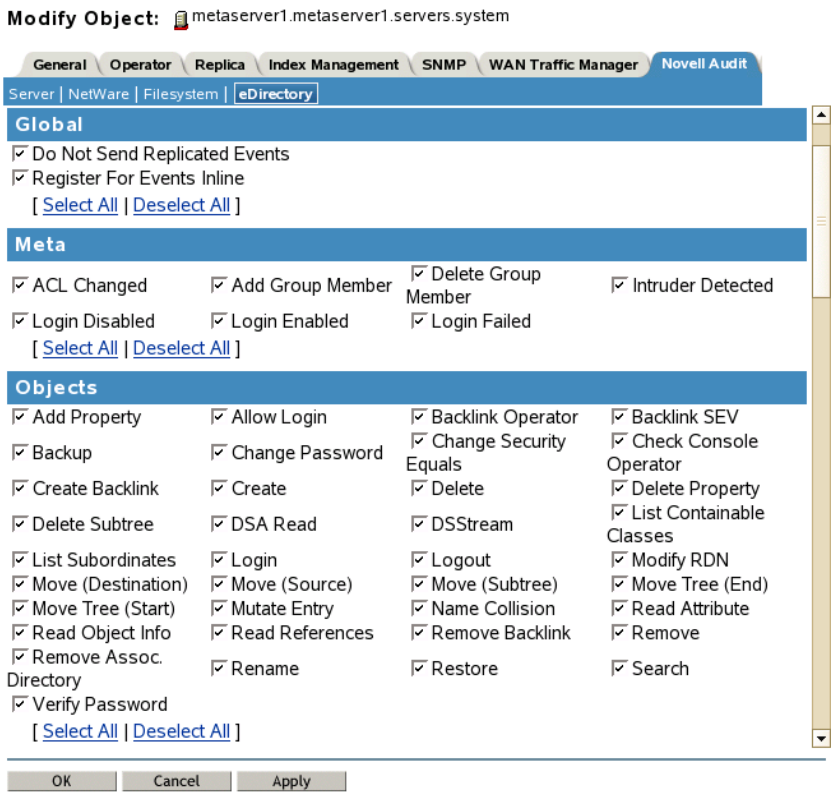
- Section 4.5.1, "Enabling Audit on All Endpoint Systems," on page 35
- Section 4.5.2, "Configuring the Unauthorized Access by Terminated Employee Rule," on page 36

4.5.1 Enabling Audit on All Endpoint Systems

You must enable each endpoint system to audit the desired user events. This process defines which events are sent to Sentinel to track. The endpoint systems are the systems that are part of the Identity Manager solution. For example, eDirectory or Active Directory are endpoint systems.

Configuration steps for each endpoint system are different. For example, in eDirectory you set the events to track on the properties of each object. You need to track events that are related to user authentication, such as, when a login or logout occurs. Figure 4-1 is an example of enabling events on the server object.

Figure 4-1 *Enabling Audit Events on eDirectory*



4.5.2 Configuring the Unauthorized Access by Terminated Employee Rule

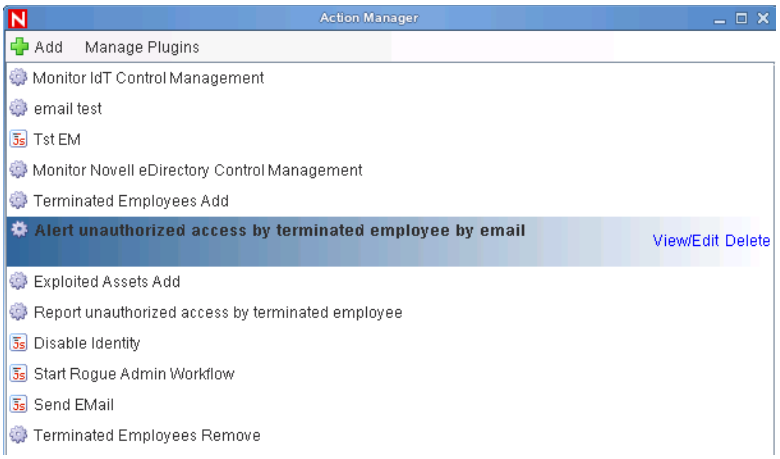
This rule detects unauthorized access to enterprise resources. The rule contains two actions that need to be configured for your enterprise.

- “Configuring the Alert Unauthorized Access by Terminated Employee by E-mail Action” on page 36
- “Configuring the Report Unauthorized Access by Terminated Employee Action” on page 36

Configuring the Alert Unauthorized Access by Terminated Employee by E-mail Action

The correct alias account that receives the e-mail alerts must be configured.

1. In the Sentinel Control Center, select *Tools* > *Action Manager*.
2. Select *Alert unauthorized access by terminated employee by e-mail*, then click *View/Edit*.

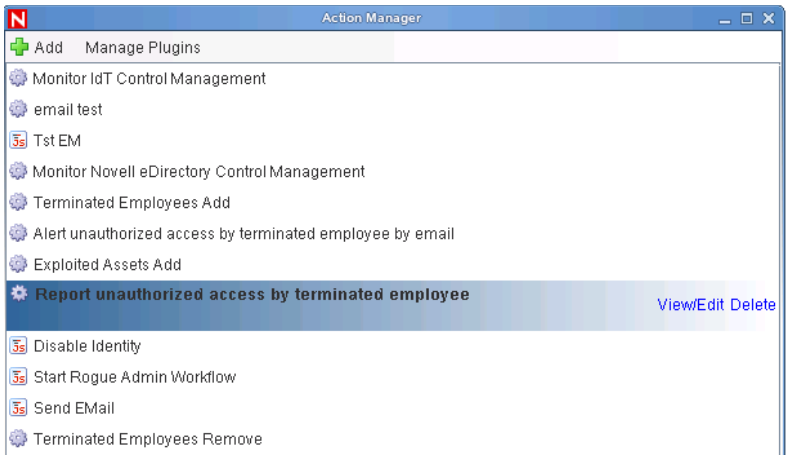


3. Add the correct alias in the *To* field, then click *Save*.

Configuring the Report Unauthorized Access by Terminated Employee Action

The Sentinel workflow that reports unauthorized access must contain a valid value for the person that receives the reports.

1. In the Sentinel Control Center, select *Tools* > *Actions Manager*.
2. Select *Report unauthorized access by terminated employee*, then click *View/Edit*.



3 Specify the correct user name in the *Responsible* field, then click *Save*.

Sending Alerts when Rogue Administration Occurs

5

This solution requires Identity Manager and Sentinel™.

When an identity attribute is changed by an administrator, not by Identity Manager, Sentinel logs the event and then takes the appropriate action. For example, the action can be an e-mail, an alert, or the rogue administrator's account is terminated. This solution not only detects the rogue activity, it detects who performed the activity and then takes immediate action against the account.

This solution uses the SOAP integrator feature of Sentinel to integrate with the User Application. The SOAP integrator allows Sentinel to call the SOAP endpoints provided by the User Application to initiate User Application workflows. These workflows are usually stored in the User Application's Provisioning Request Definitions stored under the Directory Abstraction Layer (DAL).

The Rogue_Administration_Activity workflow is called from Sentinel, sets the users' LoginDisabled attribute equal to True, and sends the Default Approver (user or group) a workflow item to notify them that the user might be attempting illicit network activity.

The following sections outline the steps required to implement this scenario.

5.1 Assumptions

The steps for this scenario assume the following:

- ❑ Sentinel 6.1 is installed and configured. For more information, see the *Sentinel 6.1 Installation Guide* (http://www.novell.com/documentation/sentinel61/index.html).
- ❑ Install and configure the eDirectory Collector. The documentation for the eDirectory Collector is included with the Collector. Download the eDirectory™ Collector and the documentation from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- ❑ Install and configure the Identity Manager Collector. The documentation for the Identity Manager Collector is included with the Collector. Download the Identity Manager Collector and the documentation from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html). For configuration documentation of the Identity Manager Collector with Identify Manager, see the *Identity Manager 3.6 Reporting Guide for Novell Sentinel*.

- Install and configure event Collectors for all integrated systems that are part of the Identity Manager solution. For example, if you are synchronize Active Directory accounts with Identity Manager, you need to download and configure the Active Directory Services Collector. All Sentinel Collectors are located at the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- The Identity Tracking Solution Pack is downloaded from the Sentinel Solution Pack Download Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- Identity Manager 3.6 is installed and configured. For more information, see the *Identity Manager 3.6 Installation Guide*.
- Identity Manager Roles Based Provisioning Module 3.6.1 is installed and configured. For more information, see the *Identity Manager Roles Based Provisioning Module Installation Guide* (http://www.novell.com/documentation/idmrbpm361/index.html).
- Designer 3.0 is installed. For more information, see "Installing Designer" in the *Identity Manager 3.6 Installation Guide*.
- You have a copy of the `Rogue_Administration_Activity.xml` file. It is located in the Designer project for the Resource Kit. Even if you do not install the Resource Kit, you must have a copy of the project to obtain the file. The `Rogue_Administration_Activity.xml` file contains the rogue administration workflow that must be imported to complete this scenario.

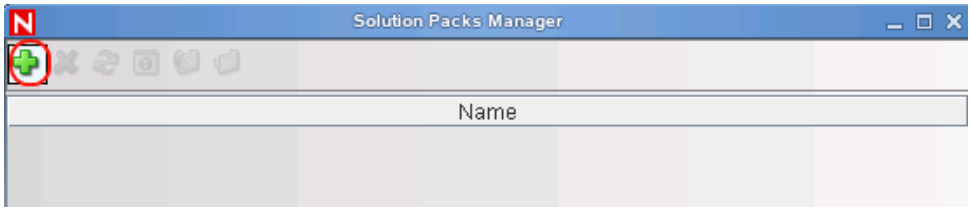
  The Resource Kit Designer Project is located at Novell Downloads (http://download.novell.com/index.jsp) under the *my downloads* tab. The `RK12_Project.zip` file is the Designer project. Download and unzip this file before proceeding.
- The Sentinel driver and Identity Vault Collector are installed and configured. For more information, see the *Identity Manager 3.6 Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

5.2 Installing the Identity Tracking Solution Pack

If you have already installed the Identity Tracking Solution Pack, skip this section and proceed directly to Section 5.3, "Installing the Rogue Administration Control," on page 41.

1. Start the Sentinel Control Center and log in as a user with rights to manage Solutions Packs.

   The Solution Manager option must be selected for the user, under *Permissions* > *Solution Pack*.
2. Select *Tools* > *Solution Pack* from the menu to start the Solution Pack Manager.
3. Click *Add* to start the import wizard.



4. Select *Import a solution Pack plugin file (.zip)*, then click *Next*.
5. Browse to and select the Identity Tracking Solution Pack where you downloaded it, then click *Open*.

   The filename is `Identity-Tracking_6.1r1.spz.zip`.

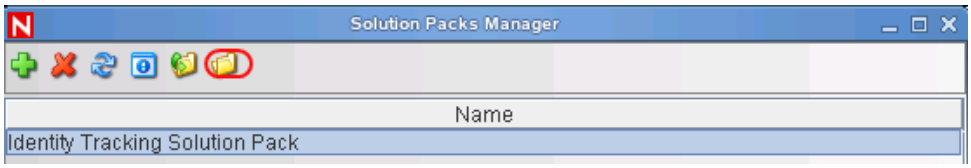
6 Review the solution pack directory, then click *Next*.

7 Review the solution pack details, then click *Finish*.

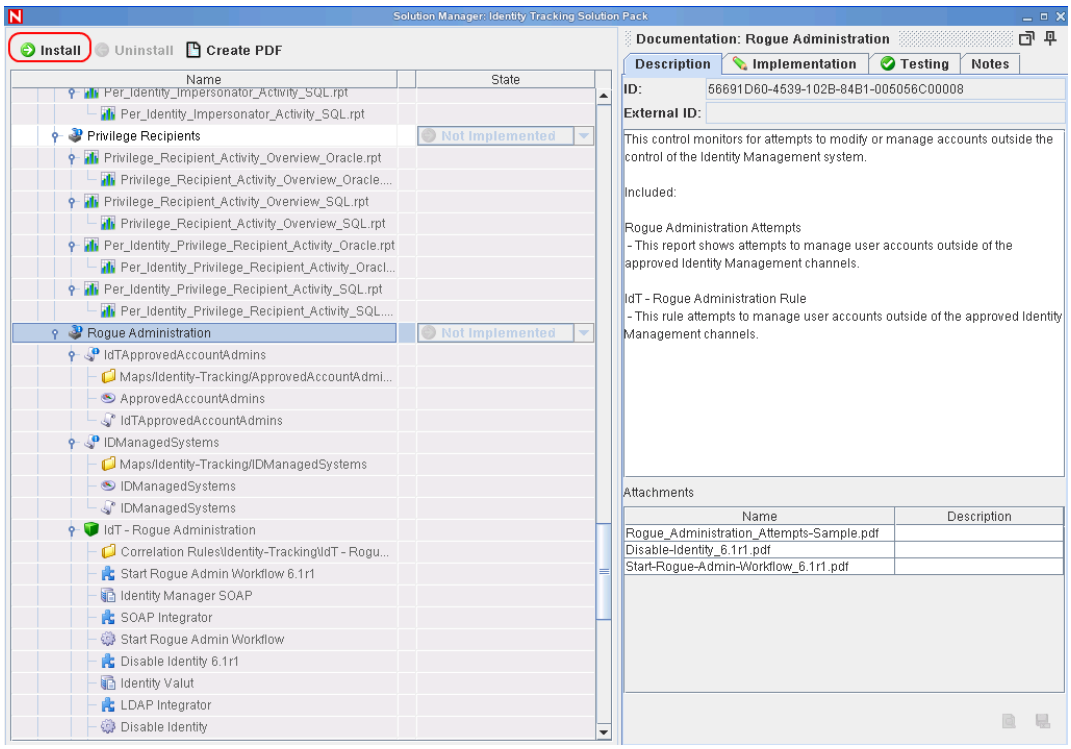
5.3 Installing the Rogue Administration Control

1 Launch the Solution Manager by selecting *Tools* > *Solution Pack* in the toolbar in the Sentinel Control Center.

2 Select *Identity Tracking Solution Pack*, then click *Open with Solution Manager*.



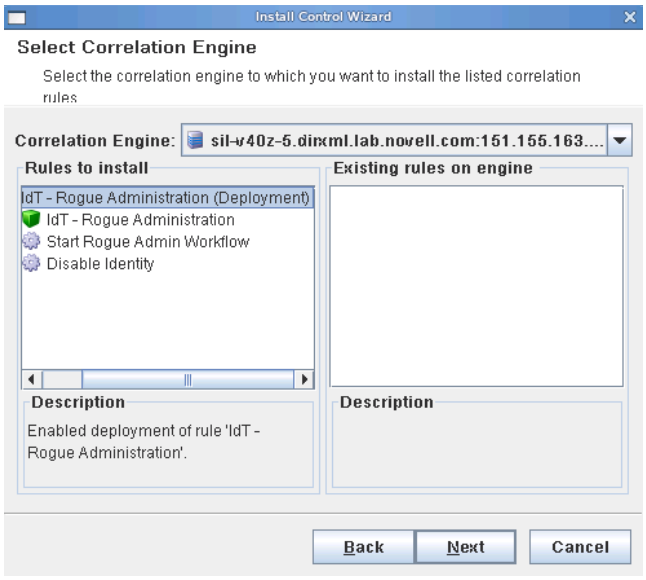
3 Select Rogue Administration in the left pane of the Solution Manager, then click *Install*.



4 Verify that the Rogue Administration Control is listed, then click *Next*.

5 Select your Correlation Engine from the drop-down list as the location where the Rogue Administration rules are installed.

6 Select *IdT-Rogue Administration (Deployment)*, then click *Next*.



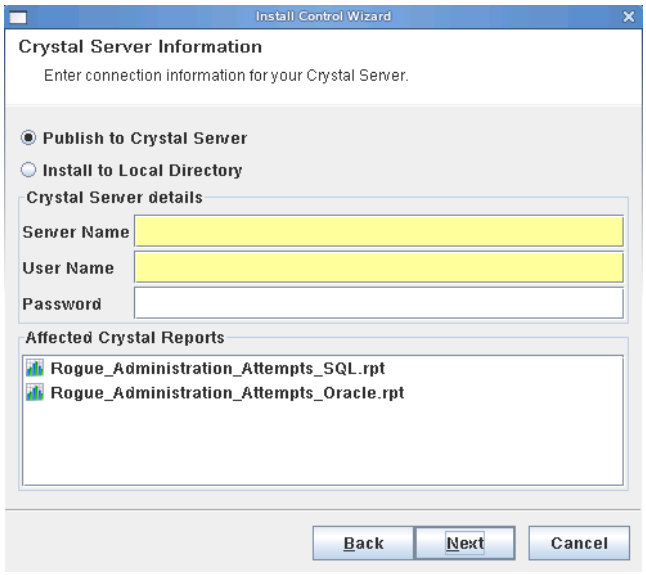
7 Select whether the Crystal server is local or remote by selecting:

- *Publish to Crystal Server*
- *Install to Local Directory*

8 Specify the following Crystal server information:

- **Server Name:** Specify the Crystal server DNS name or IP address.
- **User Name:** Specify an administrative user for the Crystal server.
- **Password:** Specify the administrative user's password.

9 Click *Next* after you have specified the Crystal server information.



10 Review the contents of the Rogue Administration Control, then click *Install*.

11 Review the installation summary, then click *Finish*.

5.4 Configuring the Rogue Administration Control

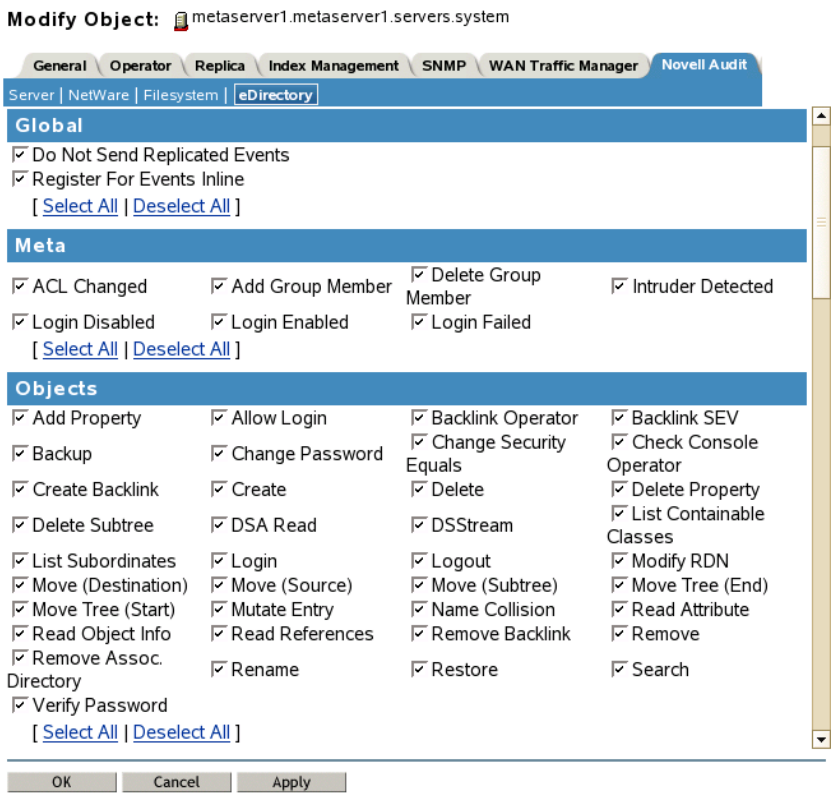
There are additional configuration steps required to implement the Rogue Administration Control.

5.4.1 Enabling Audit on All Endpoint Systems

You must enable each endpoint system to audit the desired account management events. This process defines which events are sent to Sentinel to track. The endpoint systems are the systems that are part of the Identity Manager solution. For example, eDirectory or Active Directory are endpoint systems.

Configuration steps are different for each endpoint system. For example, in eDirectory you set the events to track on the properties of each object. You need to track events that are related to account management, such as, a user create, a user delete, or a user modify. Figure 4-1 is an example of enabling events on the server object.

Figure 5-1 *Enabling Audit Events on eDirectory*

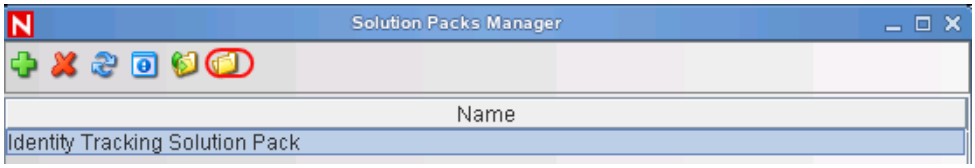


5.4.2 Copying Script Files

There are script files that are included in the Rogue Administration Control that must be copied to the `ESEC_HOME/config/exec` directory. These scripts simplify the addition of entries to the IDMManagedSystems map and the ApprovedAccount Admins map.

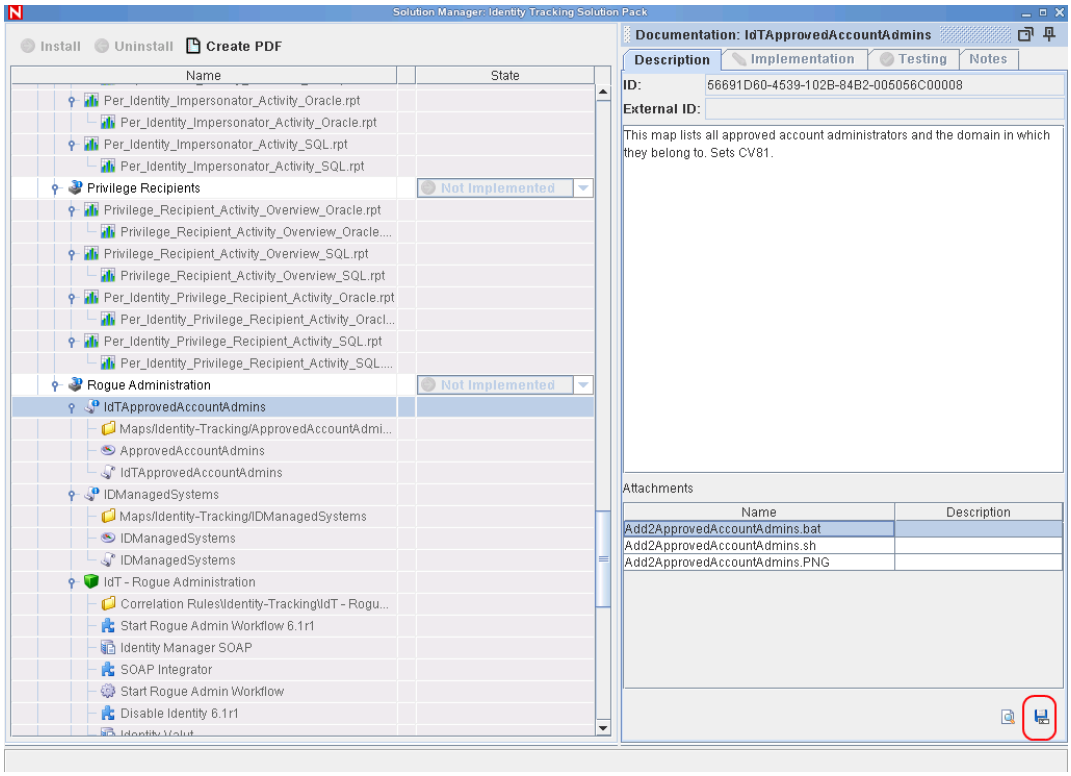
To copy the scripts:

1. Launch the Solution Manager by selecting *Tools* > *Solution Pack* in the toolbar for the Sentinel Control Center.
2. Select *Identity Tracking Solution Pack*, then click *Open with Solution Manager*.



3. In the left pane, browse to and select the IdTApprovedAccountAdmins.
4. In the right pane, select `Add2ApprovedAccountAdmins.bat` or `Add2ApprovedAccountAdmins.sh`, then click *Save*.

   The `.bat` files is for Windows and the `.sh` file is for Linux/UNIX.



5 In the left pane, browse to and select *IDManagedSystems*.

6 In the right pane, select `Add2IDManagedSystems.bat` or `Add2IDManagedSystems.sh`, then click *Save*.

5.4.3 Configuring Right-Click Menu Options

1 From the Sentinel Control Center, select the *Admin* tab.

2 Click *Admin* > *Event Menu Configuration*.

3 Click *Add*.

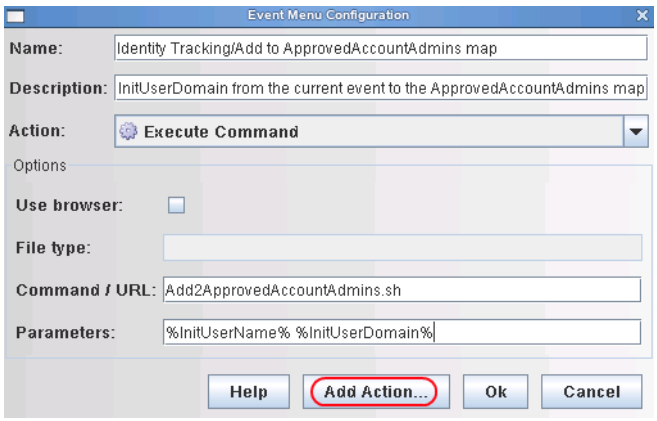
4 Use the following information to complete the configuration:

- **Name:** Specify the name as `Identity Tracking/Add to ApprovedAccountAdmins map`.
- **Description:** Specify the description as `Adds InitUserName and InitUserDomain from the current event to the ApprovedAccountAdmins map`.
- **Action:** Select *Execute Command* from the drop-down list.
- **File Type:** Leave this field blank.
- **Command/URL:** Specify `Add2ApprovedAccountAdmins.bat` or `Add2ApprovedAccountAdmins.sh` as the name of the script file to execute.

  The `.bat` file is for Windows and the `.sh` file is for Linux/UNIX.
- **Parameters:** Specify %InitUserName% %InitUserDomain% for the parameters.

  The delimiter for Linux/UNIX is a space and the delimiter for Windows is a comma.

5 Click the *Add Action* button.

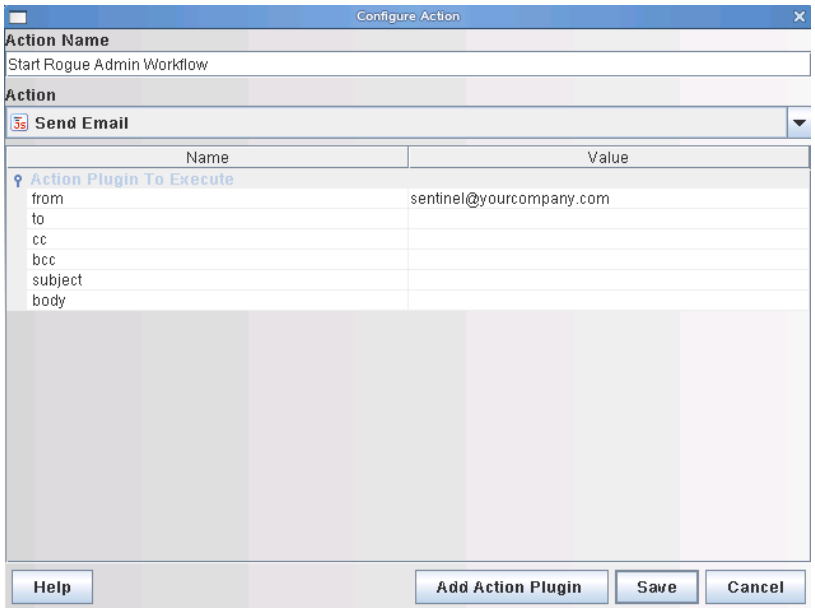


6 Select *Import an Action plugin file (.zip),* then click *Next*.

7 Browse to and select the Rogue Administration Action, then click *Open*.

The Rogue Administration Action filename is `Start-Rogue-Admin-Workflow_6.1r1.acz.zip`.

8 In the *Action Name* field, specify `Start Rogue Admin Workflow`, then click *Save*.



9 Click *OK*.

10 Click *Add*.

11 Use the following information to configure a second option:

- **Name:** Specify the name as `Identity Tracking/Add to IDManagedSystems map`.
- **Description:** Specify the description as `Adds Collector from the current event to the IDManagedSystems map`.
- **Action:** Select *Execute Command* from the drop-down list.

- **File Type:** Leave this field blank.
- **Command/URL:** Specify `Add2IDManagedSystems.bat` or `Add2IDManagedSystems.sh` as the name of the script file to execute.

  The `.bat` file is for Windows and the `.sh` file is for Linux/UNIX.
- **Parameters:** Specify %CollectorId% for the parameters.

  The delimiter for Linux/UNIX is a space and the delimiter for Windows is a comma.

12 Click *OK* to save the changes.

5.4.4 Populating the ApprovedAccountAdmin Map

The ApprovedAccountAdmin map must be populated with an administrator username and the domain of the integrated systems.

1 Create a test identity and ensure that the account is create in the integrated system.

2 Find the associated event in the Sentinel Active view.

3 Right-click the event, then select the *Identity Tracking* submenu.

4 Click *Add to ApprovedAccountAdmins map*.

5.4.5 Populating the IdentityManagedSystems Map

To populate the IdentityManagedSystems map with the CollectorID of the systems that have accounts managed by Identity Manager:

1 Generate activity on each integrated system.

2 Find the associated events in the Sentinel Active view.

3 Right-click an event, then select the new Identity Tracking submenu.

4 Click *Add to IDManagedSystems map*.

5.4.6 Configuring the SOAP Integrator

Sentinel contains a SOAP Integrator that allow Sentinel to Integrate with the User Application. The SOAP Integrator must be configured to communicate to the User Application. After the Rogue Administration Control is installed, the SOAP Integrator must be configured to communicate with the User Application server.

1 In the Sentinel Control Center, click *Tools* > *Integrator Manager* from the toolbar.

2 Select the Identity Manager SOAP Integrator from the list on the left.

NOTE: The the SOAP Integrator must be named `Identity Manager SOAP`.

---

3 Click the *SOAP Connection Settings* tab, then use the following information to configure the connection settings on the Identity Manager SOAP Integrator:

- **URL:** Specify the Web service URL used to get WSDL from the User Application server. The User Application is the SOAP provider for Identity Manager. The correct URL is located in the `server.xml` file for Tomcat on the User Application server.

  For example, specify `http://10.0.0.3:8444/IDMProv/provisioning/service?wsdl`.

- **Service Name:** Specify `ProvisioningService` as a SOAP service.
- **Port:** Specify `ProvisioningPort` as the SOAP port.
- **Use SSL:** Select *Use SSL* if the connection to the User Application server is secure.
- **Use Authentication:** Select *Use Authentication* to enable authentication to the User Application server.
- **Username:** Specify a user with administrative rights to start workflows. Use LDAP notation with the DN of the user.
- **Password:** Specify the administrator's password.

4 Click *Refresh Web Service API* to regenerate the WSDL API.

5 Click *Test*, then verify that the Integrator test completes successfully.

6 Click *Save* to save the changes.

5.4.7 Configuring the LDAP Integrator

Sentinel contains an LDAP Integrator that allows Sentinel to communicate with eDirectory. After the Rogue Administration Control is installed, the LDAP Integrator must be configured to communicate with eDirectory.

1 In the Sentinel Control Center, click *Tools* > *Integrator Manager* in the toolbar.

2 Select the Identity Vault from the list on the left.

NOTE: The LDAP Integrator must be named `Identity Vault`.

---

3 Click the *LDAP Connection Settings* tab, then use the following information to configure the connections setting on the Identity Vault Integrator:

- **Server:** Specify the IP address of the eDirectory server.
- **Port:** Specify the TCP port LDAP uses on the eDirectory server.

  The default port for unsecured communication is 389.
- **Use SSL:** Select this option to use a secure connection to the eDirectory server.

  The default port for secure communication is 636.
- **Login:** Specify the DN of a user that has administrative rights to eDirectory.

  Use the LDAP format. For example, `cn=admin,o=novell`.
- **Password:** Specify the administrator user’s password.

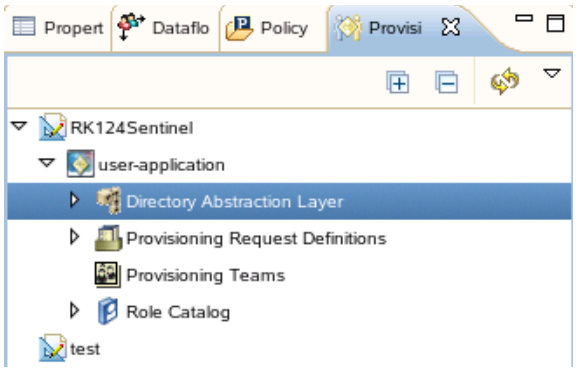
4 Click *Save* to save the changes.

5.5 Importing the Rogue Administration Workflow

Use the following procedure if the rogue administration workflow does not exist in the DAL:

1 In Designer, click *Windows* > *Show View* > *Provisioning View* in the toolbar.

2 In the Provisioning view, right-click the Directory Abstraction layer, then click *Import from File*.



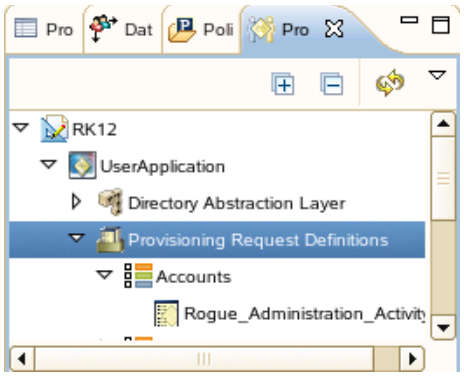
3 In the warning message, click *OK*.

4 Browse to and select the `Rogue_Administration_Activity.xml` file from the Resource Kit Designer project, then click *OK*.

The file is located in *`location_of_designer_workspace`*`/designer_workspace/RK12/Designer/Documents/Resources/provisioning_requests`.

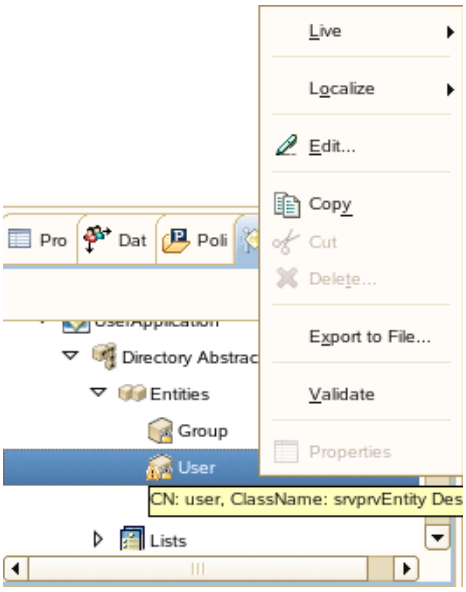
5 Click *OK* to import the workflow.

6 Verify that the workflow imported by browsing to it under *UserApplication* > *Provisioning Request Definitions* > *Accounts* > *Rogue_Administration_Activity*.



7 Verify that the LoginDisabled attribute exists on the User entity by right-clicking the Rogue_Administration_Activity, then select *Validate* to run the Project Checker.

7a If the LoginDisabled attribute does not exist on the User entity, right-click the *Directory Abstraction Layer* > *Entities* > *User*, then select *Edit*.



7b Right-click the User entity in the left pane, then select *Add Attribute*.

7c Browse to and select the LoginDisabled attribute in the left pane.

7d Click *Add Attribute*, then click *OK*.

8 Press Ctrl+S to save the changes.

9 Deploy the changes in the Identity Vault. For more information, see "Deploying a Project to an Identity Vault" in the *Designer 3.0.1 for Identity Manager 3.6 Administration Guide*.

10 Restart the User Application and the User Application driver to apply the changes. To restart the User Application server:

- Reboot the application server.
- Redeploy the application WAR file.
- Force the application to restart. The applications are JBoss* or WebSphere*.

Validating Provisioned Users with System Utilization

6

This solution requires Identity Manager and Sentinel™.

After a user is provisioned to a resource, Sentinel tracks the users's utilization of that particular resource. If a resource is not used for a specified number of days, an Identity Vault job is initiated that starts a de-provisioning action. This allows you to validate whether users who are provisioned to resources are utilizing those resources.

The following sections outline the steps required to implement this scenario.

6.1 Assumptions

The steps for this scenario assume the following:

- ❑ Sentinel 6.1 is installed and configured. For more information, see the *Sentinel 6.1 Installation Guide* (http://www.novell.com/documentation/sentinel61/index.html).
- ❑ Install and configure the eDirectory™ Collector. The documentation for the eDirectory Collector is included with the Collector. Download the eDirectory Collector and the documentation from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- ❑ Install and configure the Identity Manager Collector. The documentation for the Identity Manager Collector is included with the Collector. Download the Identity Manager Collector and the documentation from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html). For configuration documentation of the Identity Manager Collector with Identify Manager, see the *Identity Manager 3.6 Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.
- ❑ Install and configure event Collectors for all integrated systems that are part of the Identity Manager solution. For example, if you are synchronize Active Directory accounts with Identity Manager, you need to download and configure the Active Directory Services Collector. All Sentinel Collectors are located at the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).
- ❑ The Identity Tracking Solution Pack is downloaded from the Sentinel Solution Pack Download Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).

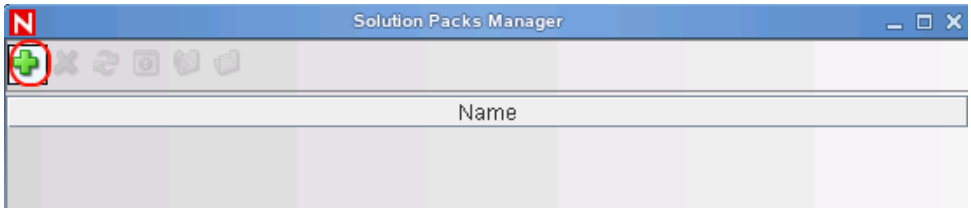
- ❑ Identity Manager 3.6 is installed and configured. For more information, see the *Identity Manager 3.6 Installation Guide*.
- ❑ The Sentinel driver and Identity Vault Collector are installed and configured. For more information, see the *Identity Manager 3.6 Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

6.2 Installing the Identity Tracking Solution Pack

If you have already installed the Identity Tracking Solution Pack, skip this section and proceed directly to Section 6.3, "Configuring the Global Setup," on page 52.

1. Start the Sentinel Control Center and log in as a user with rights to manage Solutions Packs.

   The Solution Manager option must be selected for the user under *Permissions* > *Solution Pack*.
2. Select *Tools* > *Solution Pack* from the menu to start the Solution Pack Manager.
3. Click *Add* to start the import wizard.



4. Select *Import a solution Pack plugin file (.zip)*, then click *Next*.
5. Browse to and select the Identity Tracking Solution Pack where it was downloaded, then click *Open*.

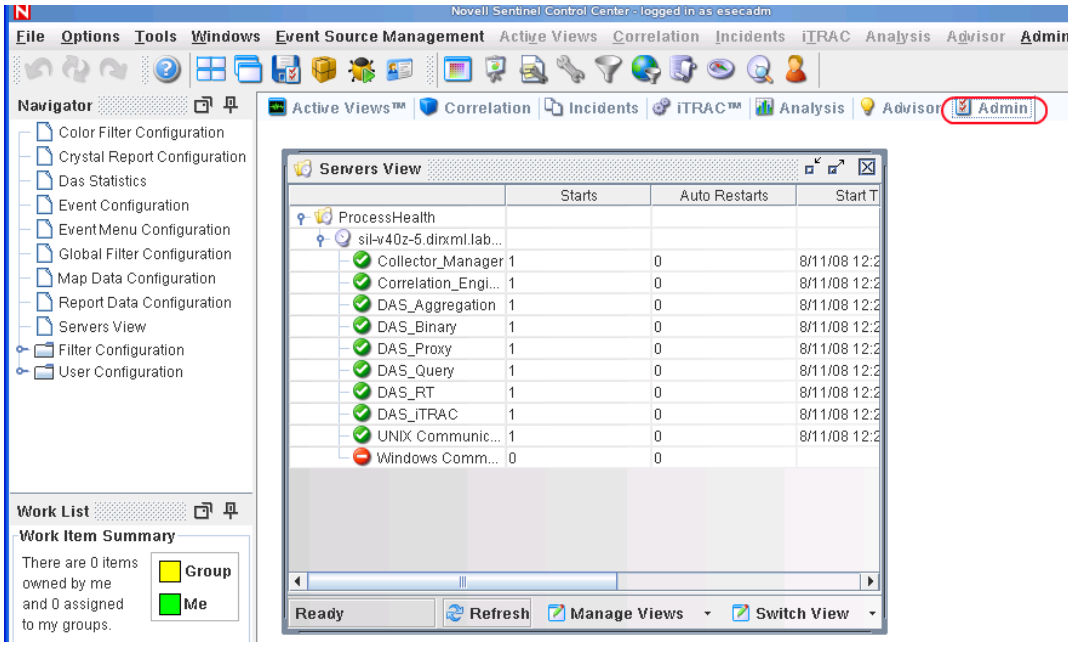
   The filename is `Identity-Tracking_6.1r1.spz.zip`.
6. Review the solution pack directory, then click *Next*.
7. Review the solution pack details, then click *Finish*.

6.3 Configuring the Global Setup

The Identity Tracking Solution Pack requires some global configuration that must be completed. This configuration needs to be completed before any additional configuration. If you have completed these global configuration task for another use case, you can skip this section.

The Sentinel data field must be able to hold Identity Manager attribute data.

1. Start the Sentinel Control Center, then click the Admin tab.



2 Select *Admin* > *Event Configuration* from the toolbar.

3 In the left pane, browse to and select *ReservedVar43*.

The tag is rv43.

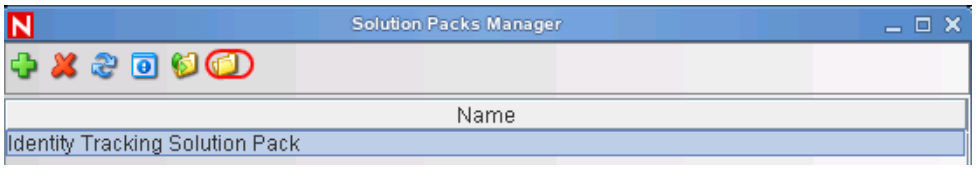
4 In the *Label* field in the right pane, change the display label to *Data*, then click *Apply*.

5 Click *Save*, the close the Event Configuration window and reopen it to see the changes take place.

6.4 Installing the Account Usage Management Control

1 Launch the Solution Manager by selecting *Tools* > *Solution Pack* in the toolbar in the Sentinel Control Center.

2 Select Identity Tracking Solution Pack, then click *Open with Solution Manager*.



3 Select *Account Usage Management* in the left pane of the Solution Manager, then click *Install*.

4 Verify that the Account Usage Management Control is listed, then click *Next*.

5 Review the contents of the Account Usage Management Control, then click *Install*.

6 Review the installation summary, then click *Finish*.

6.5 Configuring the Account Usage Control

There are additional configuration steps required to implement the Identity De-Provisioning Control.

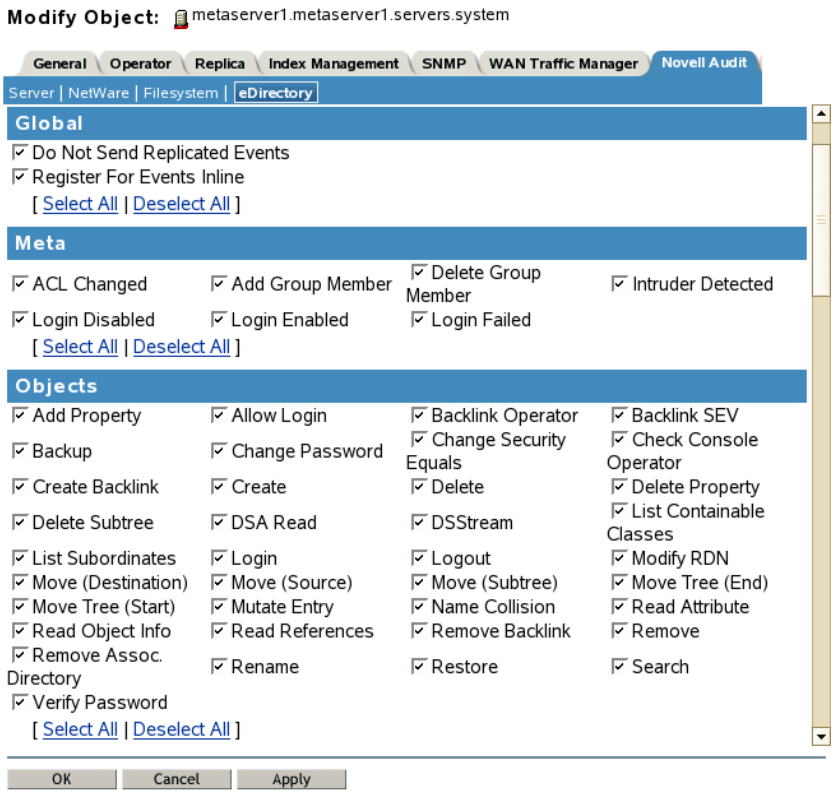
- Section 6.5.1, “Enabling Audit on All Endpoint Systems,” on page 54
- Section 6.5.2, “Configuring the Account Usage Report,” on page 55

6.5.1 Enabling Audit on All Endpoint Systems

You must enable each endpoint system to audit all user authentication events. This process defines which events are sent to Sentinel to track. The endpoint systems are the systems that are part of the Identity Manager solution. For example, eDirectory or Active Directory are endpoint systems.

Configuration steps are different for each endpoint system. For example, in eDirectory you set the events to track on the properties of each object. You need to track events that are related to user authentication, such as, when a login or logout occurs. Figure 4-1 is an example of enabling events on the server object.

Figure 6-1 *Enabling Audit Events on eDirectory*



6.5.2 Configuring the Account Usage Report

The Account Usage Report summarizes account usage for each user in the selected department for the last 120 days. Accounts that have not been used for over 90 days are considered to be inactive. There is a test report named Account Usage Test that provides a 4-day time-out for account activity, in order to test this use case.

Documentation Updates

A

The documentation was updated on the following dates:

A.1 September 24, 2008

Updates were made to the following sections. The changes are explained below.

A.1.1 Core Products

The following update was made in this section:

Location	Change
“Access Manager 3.0.4:” on page 9	Changed the statement of support from Access Manager 3.0.3 to Access Manager 3.0.4.