AUTHORIZED DOCUMENTATION

Integration Guide

Novell®
Compliance Management Platform

1.1

April 29, 2011

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. See 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.
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 an introduction to the products available in the Novell Compliance Management Platform. In addition, it describes several configuration scenarios that take advantage of the most useful points of integration among the products. 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 Rapid Deployment

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this document, see the Novell Compliance Management Platform documentation Web site (http://www.novell.com/documentation/ncmp11/)

Additional Documentation

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

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 and integration components. This section describes the components of the platform and also includes general usage notes:

1.1 What’s New in Novell Compliance Management Platform 1.1

The follow components of Novell Compliance Management Platform have been updated. The configuration scenarios described in this guide are based on these versions of the components.

Access Manager 3.1.3: For a list of what’s new in Access Manager 3.1.3, see “What’s New” (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/bjm97kd.html) in the *Novell Access Manager 3.1 Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).

Identity Manager 4.0.1 Advanced Edition: For a list of what’s new in Identity Manager 4.0.1, see “What’s New” (http://www.novell.com/documentation/idm401/idm_framework_install/?page=/documentation/idm401/idm_framework_install/data/bpo97tj.html) in the *Novell Identity Manager Framework Installation Guide* (http://www.novell.com/documentation/idm401/idm_framework_install/?page=/documentation/idm401/idm_framework_install/data/front.html).

Sentinel 6.1 Rapid Deployment and Sentinel 6.1: The Novell Compliance Management Platform supports Sentinel 6.1 Rapid Deployment (RD) and Sentinel 6.1. However, the Identity Tracking Solution Pack requires Sentinel 6.1 RD. For more information about Sentinel 6.1 RD, see the Sentinel 6.1 RD documentation site (http://www.novell.com/documentation/sentinel61rd/index.html). For more information about Sentinel, see the Sentinel 6.1 documentation site (http://www.novell.com/documentation/sentinel61/index.html).

Be sure to use the latest available version of Sentinel 6.1 RD or Sentinel 6.1.

NOTE: The Resource Kit has been removed in Novell Compliance Management Platform 1.1. Most of the resources contained within the Resource Kit are now included with Identity Manager 4.0.1.

1.2 Core Products

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

- **Identity Manager 4.0.1 Advanced Edition:** 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, the Identity Reporting Module, and Designer. 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. The reporting module provides the ability to generate reports that show critical business information about various aspects of your Identity Manager configuration. Designer helps you design and deploy your Identity Manager system.

  For more information about Identity Manager, see the Identity Manager 4.0.1 documentation site (http://www.novell.com/documentation/idm401).

  To download Identity Manager, see the Identity Manager 4.0.1 download page (http://download.novell.com/Download?buildid=Z1X0k_2Sih0).

- **Access Manager 3.1.3:** 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 3.1 documentation site (http://www.novell.com/documentation/novellaccessmanager31/index.html).

  To download Access Manager, see the Access Manager 3.1 download page (http://download.novell.com/Download?buildid=3wq_4OFbYgk).

- **Sentinel 6.1 Rapid Deployment:** Sentinel RD is the rapid deployment of Sentinel, a product that automates the task of monitoring and managing both security devices and trusted-insider activities on critical company resources.

  For more information about Sentinel RD, see the Sentinel RD documentation site (http://www.novell.com/documentation/sentinel61rd/). For more information about Sentinel, see the Sentinel 6.1 documentation site (http://www.novell.com/documentation/sentinel61/index.html).

  To download Sentinel 6.1 RD, see the Sentinel 6.1 RD download page (http://download.novell.com/Download?buildid=-OtFQyD752o). To download the latest patch, see Sentinel 6.1 RD patch download page (http://download.novell.com/protected/Summary.jsp?buildid=hTD_ZVZAHb0).

1.3 Integration Components

The following additional components help you to integrate the core products of the Novell Compliance Management Platform:

- **Identity Manager Driver for Sentinel and the Identity Vault Collector:** The Identity Manager Driver for Sentinel (Sentinel driver) and the Identity Vault Collector gather identity information for use by Sentinel. The Sentinel driver and the Identity Vault Collector work with many different systems.

  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 Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide* (http://www.novell.com/documentation/ncmp11/ncmp_sentinel_driver/?page=/documentation/ncmp11/ncmp_sentinel_driver/data/bookinfo.html).

  The Identity Manager Driver for Sentinel and the Identity Vault Collector are part of Identity Manager Advanced Edition. To download Identity Manager Advanced Edition, see the Novell Identity Manager 4.0.1 download page (http://download.novell.com/Download?buildid=Z1X0k_2Sih0).

- **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.

  The Identity Tracking Solution Pack requires the latest available version of Sentinel 6.1 RD.

  For more information on the Identity Tracking Solution Pack, see Section 2.2, “Using the Identity Tracking Solution Pack,” on page 14.

  To download the Identity Tracking Solution Pack, see the Novell Downloads page (http://download.novell.com/index.jsp).

- **User Application CMP Extension Package:** The User Application CMP Extension package includes these resources:

  - Rogue Administration Work Flow
  - "Login Disabled" attribute on the User DAL entity

  The workflow includes the ability to set three GCV values (Rogue Administration - Security Review Timeout (In Minutes), Rogue Administration - Escalation Timeout (In Minutes), and Rogue Administration - Escalation Addressee DN).

To take advantage of these features, you need *Version 1.0.6* or higher of this package. When you install the latest 4.0.1 packages for the User Application Driver, you will get this package automatically. You can use *Help > Check for Updates* in Designer to be sure if you have the latest version.

For more information on using the User Application CMP Extension package, see Section 2.5.6, “Adding the CMP Extension Package to the User Application Driver,” on page 39.

- **EAS Sentinel Link Configuration Utility** The *EAS Sentinel Link Configuration Utility* is a new feature of CMP 1.1. This utility configures the receiving server in the Event Auditing Service to listen for events forwarded from Sentinel via Sentinel link.

  To download the EAS Sentinel Link Configuration Utility, see the Novell Downloads page (http://download.novell.com/index.jsp).

1.4 System Requirements

In addition to the core products and integration components listed above, you may need to have one or more additional system components. Depending on your configuration, you may need the following system components to use the Novell Compliance Management Platform 1.1:

Table 1-1 *System Requirements*

Component Type	Component	Minimum Required Version
Connectors	Windows Event (WMI) Connector	6r6
	NOTE: This Connector replaces the WMS Connector.	
	Audit Connector	6r9
	Syslog Connector	6r10
Collectors	Active Directory Collector	6.1r6
	Identity Manager Collector	6.1r7
	eDirectory Collector	6.1r9
	Identity Vault Collector	6.1r2
	iManager Collector	6.1r4
	Access Manager Collector	6.1r4
	NOTE: The Access Manager Collector 6.1r4 does not support Novell Access Manager 3.1 SP3. To collect events from version 3.1.3, check the Sentinel Plug-ins download site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) page for the latest release of this collector.	

To get the Connectors and Collectors, you need to go to the Sentinel Plug-ins download site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) page.

1.5 Usage Notes for CMP 1.1

Here are some important usage notes for the Novell Compliance Management Platform 1.1:

- When using Novell Compliance Management Platform 1.1, you need to use the latest versions of all the core products supported by the platform. You cannot mix and match CMP 1.1 products, which means that you cannot use earlier versions of one or more individual products if you plan to upgrade to CMP 1.1.

  NOTE: CMP 1.0.1 will be dropped as soon as CMP 1.1 is released. The only officially supported upgrade path is from CMP 1.0.1 to CMP 1.1.

- Novell Compliance Management Platform is a SKU and therefore includes a new license. Once you have this license, you can take full advantage of platform functionality.
- In general, the use cases supported in CMP 1.1 are the same as those supported in CMP 1.0.1. However, there are a few exceptions. These are the exceptions:
  - The Novell Compliance Management Platform does not support a direct connection between the Identity Reporting Module and Access Manager. It does however support SSO access from RBPM to the reporting module.
  - It is possible to configure Access Manager such that when a user attempts to access a system to which they are not authorized, the user is redirected to a role or resource request within the User Application.
- Here are some things to keep in mind when using the reporting capabilities of Novell Compliance Management Platform:
  - If you want to run custom reports against auditing data in the public schema of the SIEM database, you should use Sentinel reports instead of Identity Manager reports.
  - The Correlated Resource Assignments Events by Users report depends on data from the public schema. Due to latency issues, this report may not contain all of the data synchronized from Sentinel at execution time. If you do not see all of the data you would expect to see, rerun the report again at a later time.

Configuration Scenarios

2

This section describes several common usage scenarios for the Novell Compliance Management Platform.

2.1 Assumptions

The steps for this scenario assume the following:

- ❑ Install and configure Sentinel 6.1 or Sentinel 6.1 RD. For more information, see the *Sentinel 6.1 Installation Guide* (http://www.novell.com/documentation/sentinel61/s61_install/data/) or the *Sentinel 6.1 Rapid Deployment Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/).
- ❑ (Conditional) If you are using Sentinel RD, you must install the Sentinel RD 6.1 HF1. You can download this patch from Novell Downloads Web site (http://download.novell.com).
- ❑ 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 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).
- ❑ Download the Identity Tracking Solution Pack from the Novell Downloads page (http://download.novell.com/index.jsp).
- ❑ Install and configure Identity Manager. For more information, see the *Identity Manager Framework Installation Guide* (http://www.novell.com/documentation/idm401/idm_framework_install/?page=/documentation/idm401/idm_framework_install/data/front.html).
- ❑ Install and configure the Identity Manager Roles Based Provisioning Module. For more information, see the *Identity Manager Roles Based Provisioning Module Installation Guide* (http://www.novell.com/documentation/idm401/install/?page=/documentation/idm401/install/data/front.html).

- Install Designer 4.0. For more information, see the *Designer for Identity Manager Administration Guide* (http://www.novell.com/documentation/idm401/designer_admin/?page=/documentation/idm401/designer_admin/data/front.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 for the Identity Manager Collector with Identify Manager, see the *Identity Manager Reporting Guide for Sentinel* (http://www.novell.com/documentation/idm401/idm_sentinel/?page=/documentation/idm401/idm_sentinel/data/bookinfo.html).
- You have a copy of the `Rogue_Administration_Activity.xml` file. It is located in the Novell User Application CMP Extension Package. The `Rogue_Administration_Activity.xml` file contains the rogue administration workflow that must be imported to complete this scenario.
- Install and configure the Sentinel driver and Identity Vault Collector. For more information, see the *Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

2.2 Using the Identity Tracking Solution Pack

The Identity Tracking 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.

The Identity Tracking Solution Pack provides high-level, identity-based controls that can help solve management and security problems within even the largest enterprises. Leveraging Novell's years of industry experience in Identity and Access Management, the solution pack integrates data from Novell and third-party applications to give unprecedented visibility into user activities and identity/account management.

2.2.1 Overview of the Identity Tracking Solution Pack

This section provides a brief overview of the components within the Identity Tracking Solution Pack.

The solution pack contains the following categories and controls:

Table 2-1 *Solution Pack Controls*

Category	Control	Description
Solution Pack Controls	Dashboard Status	Provides an overview of the rollout status of the Solution as a whole.
	Implementation Audit Trail	Monitors for state changes for controls in this Solution, with alerting and summary reports that show who changed the state of which controls.
Identity Management Controls	Identity Provisioning	Provides a set of reports to monitor common identity provisioning actions within the enterprise.
	Identity De-Provisioning	Provides a set of reports and rules to monitor common identity de-provisioning and access violation actions within the enterprise.

Category	Control	Description
Suspicious Activity Controls	Suspicious Activity Overview	Presents an overview of suspicious activity within the enterprise. It summarizes the other controls for monitoring suspicious activity, not including Rogue Administration.
	Authentication Failures	Provides details about identity-based authentication failures across the enterprise.
	Access Denials	Provides details about identity-based access denials, for example failures when accessing files or database tables, across all integrated systems. These users may be attempting to access sensitive data to which they have not been granted access.
	Privilege Escalation Denials	Provides details about privilege escalation denials across all integrated systems. These users may be attempting to gain a higher level of privilege without authorization.
	Affected By Exploits	Provides details about users accessing assets that are likely to have been exploited by attackers detected by Sentinel's Exploit Detection service. These users may be at risk for having their account information stolen by the attacker that has exploited the asset, which may in turn enable the attacker to compromise other systems.
	Privilege Recipients	Provides details about users who have seen growth in their privileges by being granted additional ACLs or being added to new groups. These users may have been granted too broad access to sensitive information.
	Rogue Administration	Monitors for attempts to modify or manage accounts outside the control of the Identity Management system.

Category	Control	Description
Account Usage Management Controls	Account Usage	Provides a set of reports to monitor the usage of accounts for each identity. Specifically, the associated report should be run regularly to detect unused accounts that should be disabled or deleted.
Password Management Controls	Password Changes	Provides a set of reports related to password management for accounts.
Recent Activity Controls	Recent Activity	Provides a set of reports to monitor the activity performed by the users in the recent past within the enterprise.

The content provided with the Identity Tracking Solution Pack includes several correlation rules, actions, integrators, and reports.

The reports are described below:

Table 2-2 *Solution Pack Reports*

Report	Description
Account Usage	Summarizes account usage for each user in the selected department for last 120 days. Accounts that have not been used for over 90 days are considered inactive and should be disabled; non-usage for over 60 days will be flagged with a warning. Note that the data scanned covers 120 days total, so accounts unused for that entire time period or for which Sentinel is not collecting data at all will not be displayed.
Affected by Exploit Activity Overview	Shows an overview of identities accessing assets that are likely to have been exploited by attackers based on Sentinel's Exploit Detection service. These users may be at risk for having their account information stolen by the attacker that has exploited the asset, which may in turn enable the attacker to compromise other systems.
Authentication Failure Activity Overview	Shows an overview of authentication failures across all integrated systems. These users may be attempting to log in to accounts that are disabled or that they do not own.
Employee Termination Violation	Presents any attempts to access enterprise resources by terminated employees within the selected date range, grouped by the incident status.
Identity Provisioning Overview	Displays provisioning information for identities.

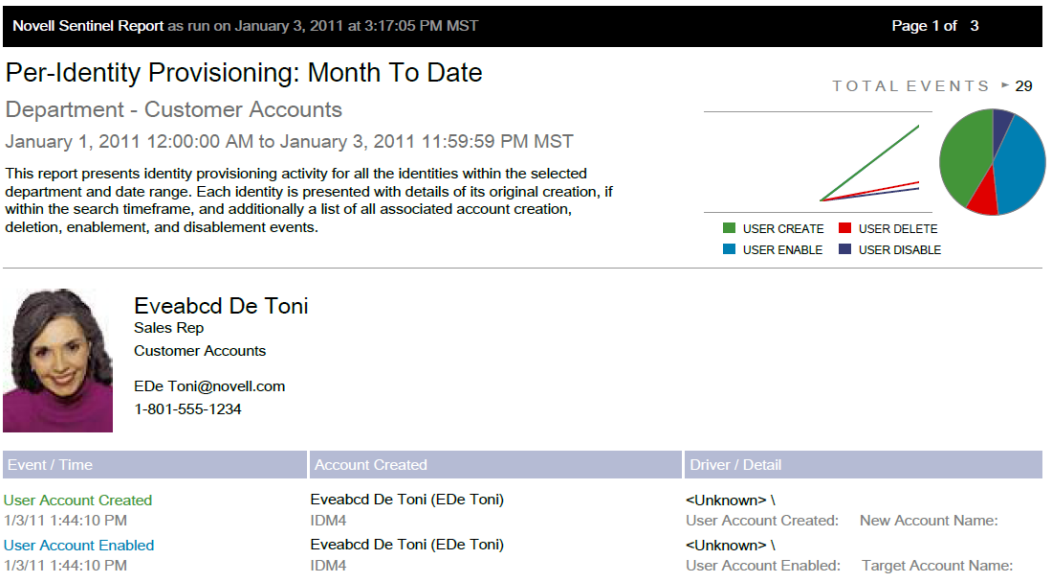
Report	Description
Password Changes	Summarizes password change activity for each user in the selected department for last 120 days. If a password is not changed for 90 days it is assumed to be expired and should be reset; passwords over 60 days old will be flagged as old. Note that the data scanned covers 120 days total, so passwords that are not changed for that entire time period or for which Sentinel is not collecting data at all will not be displayed.
Per Identity Account Management	Presents account management activity for an Identity within the selected date range, grouped by the domain within which each account exists and the account name.
Per Identity Affected by Exploit Activity	Shows details for a specific identity, who attempt to access the assets that are likely to have been exploited by attackers based on Sentinel's Exploit Detection service. The details are grouped by the target asset (hostname - IP) against which the attempt was made. These users may be at risk for having their account information stolen by the attacker that has exploited the asset, which may in turn enable the attacker to compromise other systems.
Per Identity Authentication Failure Activity	Lists all the authentication failures for a specific identity across all integrated systems, grouped by the domain within which each account exists. These users may be attempting to log in to accounts that are disabled or that they do not own.
Per Department Authentication Failure Activity	Allows the report administrator to run an authentication failure report for either a single department, or all departments.
Per Identity Provisioning	Presents identity provisioning activity for all the identities within the selected department and date range. Each identity is presented with details of its original creation, if within the search time frame, and additionally a list of all associated account creation, deletion, enablement, and disablement events.
Recent Activity	Summarizes the recent activity for each user in the selected department for the last week, grouped by the event category.
Rogue Administration Attempts	Shows attempts to manage user accounts outside of the approved Identity Management channels. The security system has attempted to disable the rogue administrator and has started an Identity Management workflow to respond to this attempt.
Solution Pack Audit Trail	Shows state changes to all controls in this Solution Pack for the selected date range, grouped by control.

Report	Description
Solution Pack Status Dashboard	Shows the overall deployment status of the Solution Pack. The pie chart shows the percentage of controls in each state for the Pack as a whole, and the horizontal bar chart shows the status of controls in each category.
Suspicious Activity Overview	Shows a global view of suspicious activity.

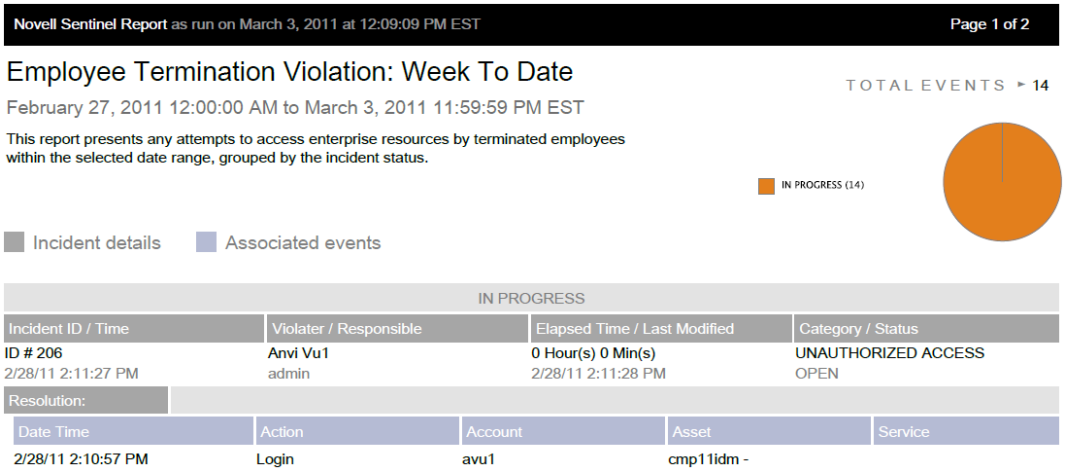
2.2.2 Solution Samples

This section displays some sample results from the Solution Pack controls. Note that in the customer environment results will vary depending on the local configuration of event sources and control parameters.

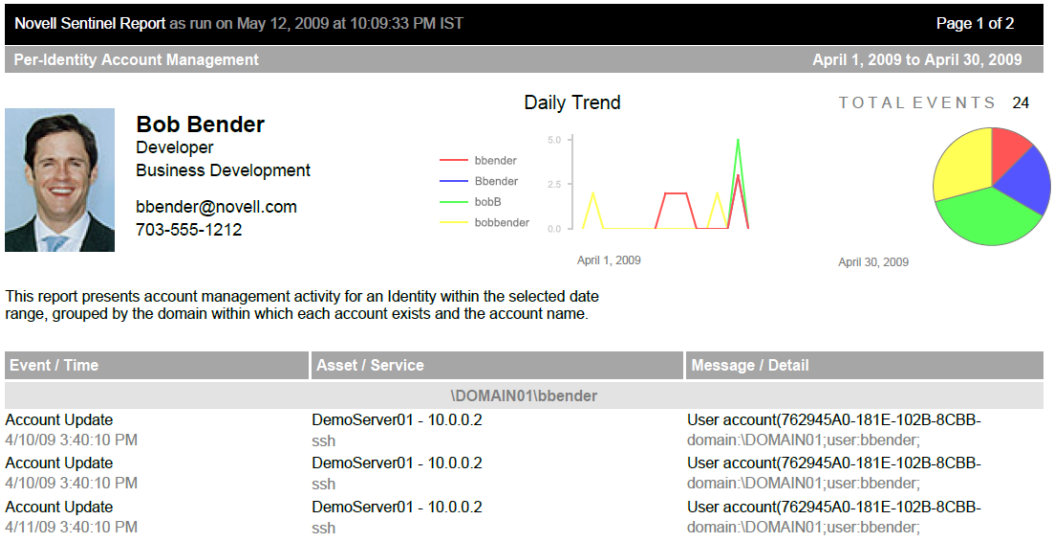
- The *Per-Identity Provisioning* report presents identity provisioning activity for all the identities within the selected department and date range:



- The *Employee Termination Violation* report presents any attempts to access enterprise resources by terminated employees within the selected date range, grouped by the incident status:



- The *Per-Identity Account Management* report presents account management activity for an Identity within the selected date range, grouped by the domain within which each account exists and the account name:

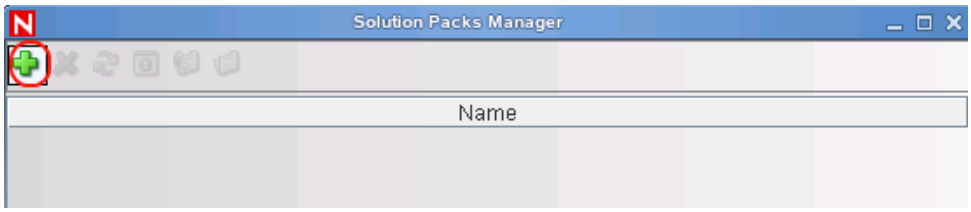


2.2.3 Installing the Identity Tracking Solution Pack

To install the Identity Tracking Solution Pack:

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

   The Solution Manager option must be selected for the user, under *Permissions* > *Solution Pack*.
2. Select *Tools* > *Solution Packs* 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_6.1r4.spz.zip`.

6 Review the Solution Pack directory, then click *Next*.

7 Review the Solution Pack details, then click *Finish*.

2.2.4 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. The configuration information is contained in the Identity Tracking Solution Pack.

If you have completed these global configuration task for another use case, you can skip the following sections:

- “Accessing the Global Setup Configuration” on page 21
- “Installing the Controls” on page 22
- “Configuring the Sentinel Data Field” on page 22
- “Adding SQL Indexes to Speed Up Queries” on page 23

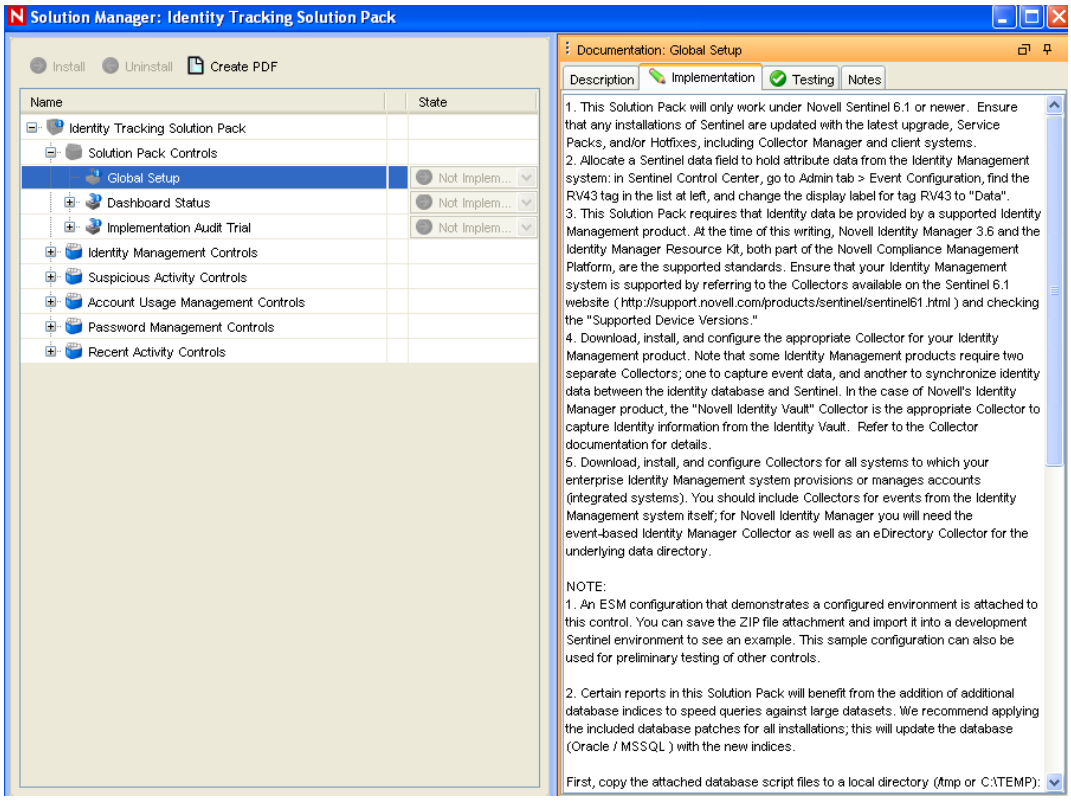
Accessing the Global Setup Configuration

To access the Global Setup configuration information:

1 In the Sentinel Control Center tool bar, click *Tools* > *Solution Packs*.

2 Double-click the Identity Tracking Solution Pack entry in the Solution Packs Manager.

3 In the left pane, select *Identity Tracking Solution Pack* > *Solution Pack Controls* > *Global Setup*, then click the *Implementation* tab in the right pane.

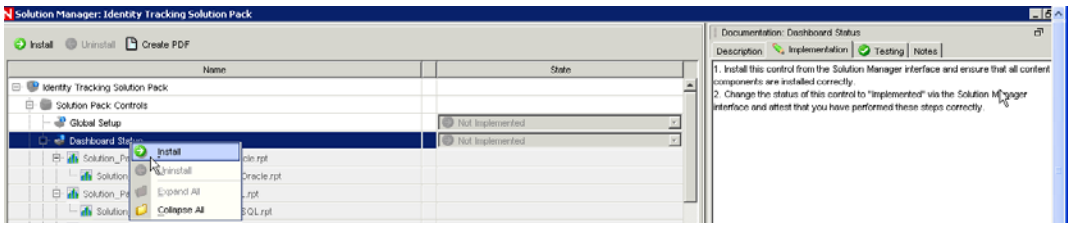


Installing the Controls

To install the controls included with the solution pack:

1 Right-click a control (such as Dashboard Status) in the list displayed under Solution Pack Controls.

2 Click *Install* from the pop-up menu.

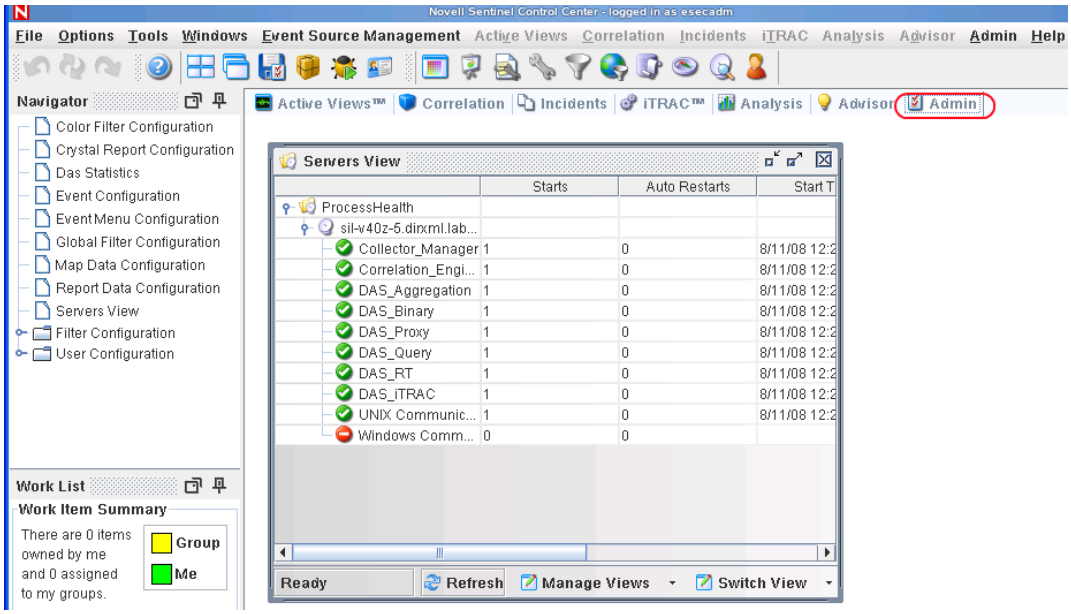


You need to do this for each control you plan to use.

Configuring the Sentinel Data Field

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 tool bar

3 In the left pane, locate the rv43 variable, which may have already been labeled *ReservedVar43* or *DataValue43*.

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

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

Adding SQL Indexes to Speed Up Queries

The performance of queries for certain reports in the Identity Tracking Solution Pack is increased if you add indexes to the database. These indexes increase the speed of queries against the large database. The Identity Tracking Solution Pack provides instructions on how to add the indexes.

2.3 Configuring Sentinel Link to use Sentinel as the Sender and EAS as the Receiver

CMP 1.1 allows you to forward event data from the Sentinel repository to the EAS repository. To configure event forwarding from Sentinel to EAS, you need to configure some components on both the Sentinel and EAS servers.

For CMP 1.1, a new utility has been provided for creating the Sentinel Link Server in EAS. This utility is called the EAS Sentinel Link Configuration Utility.

In order for the Sentinel server to receive events, a Link Connector must be configured. The Sentinel documentation provides information about creating a Link Connector. For background information on creating a Link Connector, see the *Sentinel Link Solution Guide* (http://support.novell.com/products/sentinel/zip/utilities/Sentinel-Link_Solution_6.1r4.pdf).

IMPORTANT: The EAS Sentinel Link Configuration Utility removes the need to perform the steps in Section 2 of the Sentinel Link Solution Guide.

2.3.1 Working with the EAS Sentinel Link Configuration Utility

To configure event forwarding from Sentinel to EAS, you need to have the EAS Sentinel Link Configuration Utility (`eas_link_configure`). You can download the EAS Sentinel Link Configuration ZIP file (`eas_link_configure.zip` file) from the Novell Downloads page (http://download.novell.com/index.jsp).

This utility creates a Sentinel Link Server in the EAS server environment. The Connector and Collector are automatically created after a restart of EAS, when events begin being sent.

The eas_link_configure utility takes the following values as arguments on the command line:

- The password for dbauser
- An Action, which is one of the following values:
  - **create:** Creates and establishes a new Sentinel Link Server
  - **remove:** Removes an existing Sentinel Link Server
  - **update:** Modifies an existing Sentinel Link Server name or port
  - **list:** Lists any existing Sentinel Link Servers that are configured

After running the `eas_link_configure` utility, you must restart the EAS server in order for the changes to take effect.

To get help with the utility, you can run this command: `eas_sentinel_link help`

Help will give you the following usage information: Usage: `eas_link_configure.sh password { create | remove | update | list }`

2.3.2 Configuring EAS to Receive Events

To configure EAS to receive events, you need to create a Sentinel Server in EAS. This section provides instructions for doing this.

To configure EAS to receive events:

1. Disable history in the shell in order to avoid retention in the shell history of the password specified on the command line.
2. Unzip `eas_link_configure.zip`.
3. Change directory to the unzipped utility.
4. Modify `db_connnection.properties` to reflect values for your EAS PostgreSQL database:
   - server=PostgreSQL
   - hostname=localhost
   - portnum=15432
   - database=SIEM
   - username=dbauser
5. Modify `eas_link_configure.properties` to specify the name of the Sentinel Link Server and the port it will listen on:
   - sentinelLinkName=Sentinel Link Server ALL:1290
   - sentinelLinkPort=1290

6 Optionally, set the ESM_UTIL_ROOT property. The value of ESM_UTIL_ROOT is set to the current directory by default. You may also set it to an explicit value.

7 Set the JAVA_HOME variable to point to the JDK home directory.

8 Run the `eas_link_configure` utility with a command that follows this format:

```
eas_link_configure dbauser_password <Action>
```

9 Examine the `eas_link_configure.log` file. All information and error output is written to the `eas_link_configure.log` file. View the log file for further details on the information or the errors.

- The `eas_link_configure.sh` script will report if errors are found. After correcting the errors reported in the `eas_link_configure.log`, run the `eas_link_configure` utility again.
- If no errors are reported for create, update, and delete actions, restart EAS in order for the changes to take effect.

10 To verify that the server has been successfully created:

1. Go to the Sentinel Link Integrator in Sentinel RD Control Center and use the *Test* button to confirm success of the EAS Sentinel Link Server.
2. Verify that events are arriving in EAS by generating a report.
3. Query the events table in the EAS database to verify events are being forwarded successfully. Here a sample SQL query that uses a time range to verify the events:

```
select * from EVENTS where EVT_TIME > '2011-01-13 09:00' AND EVT_TIME
< '2011-01-13 10:00';
```

11 If the events are not being forward properly, check the EAS log files for errors.

12 If history is not disabled in your shell, then you are strongly advised to clear the history now in order to avoid retention of the PostgreSQL password in any history contents.

2.3.3 Configuring Sentinel to Send Events

This section provides instructions for configuring a Sentinel server to send events to EAS. These instructions describe the approach Novell recommends for an initial setup.

NOTE: If you use a different method to configure a Sentinel server to send events to EAS, you need to be sure that all events are sent. If you do not send all events, your Identity Manager reports will not run successfully.

Detailed steps for configuring a Sentinel server to send events to another Sentinel system are provided in Section 3 of the *Sentinel Link Solution Guide* (http://support.novell.com/products/sentinel/zip/utilities/Sentinel-Link_Solution_6.1r4.pdf). If you want to refine your configuration after performing the steps below, you should refer to this document for additional information.

To configure a Sentinel server to send events to EAS:

1 Log in to your Sentinel server as user “novell”.

Set a password for user “novell” if you have not done so already. The Sentinel installer creates the user “novell” without password credentials.

2 Download the Sentinel Link Solution (June 2010 6.1r4) from *Sentinel Link Solution Downloads* (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

3 Unzip the downloaded Sentinel Link Solution package.

4 Start Sentinel Control Center.

5 Import the new Integrator for the Sentinel Link Solution:

5a In the Novell Sentinel Control Center, select *Tools > Integrator Manager*. The Integrator Manager window displays.

5b Click *Manage Plug-Ins*.

5c Click the *Import* (plus sign) icon in the Integrator Plugin Manager window.

The Plugin Import Type window displays.

5d Select *Import an Integrator plugin file (.zip)*, then click *Next*.

The Choose Plugin Package File window displays.

5e Click *Browse* to locate the `slink_integrator.zip` file and click *Next*.

5f Click *Finish*.

5g Dismiss the dialogs.

6 From the Integrator Manager interface, configure an Integrator:

6a Click the *Add Integrator* icon in the bottom left corner.

6b Choose *Sentinel Link Integrator* from the *Select Integrator* drop down

6c Specify a name for your Integrator, such as “Sentinel Link Integrator to EAS”.

6d Specify a new *Service Category*, such as “SL - Sentinel Link”.

6e Provide a description for the Integrator in the *Description* field.

6f Click *Next*.

6g Specify the IP address of the EAS Server in the *Host Name* text field.

6h Specify the port number for the Sentinel Link configured on EAS. The default is 1290.

6i Click *Next* on each of the remaining dialogs.

6j Click *Finish*.

7 Import the Action plugin:

7a In the Sentinel Control Center, select *Tools > Action Manager*.

7b In the Action Manager window, click *Manage Plugins*.

7c In the Action Plugin Manager, click the *Import* (plus sign) icon.

7d In the Import Plugin wizard, select *Import an Action plugin file (zip,inz)*, then click *Next*.

7e Click *Browse* to locate the `Sentinel-Link_6.1r3.acz.zip` file and click *Next*.

7f Click *Next*.

7g Click *Finish*.

8 Create a new Action:

8a In Action Manager, click the *Add* (plus-sign) icon.

8b Specify an *Action Name* (for example, “SLinkEAS”).

8c Choose *Sentinel Link* from the *Action* drop down

8d Choose your Sentinel Link Integrator.

8e Click *Save*.

8f Dismiss the Action Manager dialog.

9 Create the Global Filters:

9a In the Sentinel Control Center, click on the *Admin* tab.

9b In the left navigation bar, select *Global Filter Configuration*.

9c Click *Add*.

9d Click the button under *Filter Name*. Perform the steps below for each of the following product names (note that some of the products have more than one name):

- Novell Identity Manager
- Novell eDirectory and EDIRECTORY
- Identity Vault
- Novell Modular Authentication
- Novell iManager

9d1 Click *Add*.

1. Specify a *Filter Name*.
2. Set *Property* to `ProductName`.
3. Set *Operator* to the equals sign (`=`).
4. Set *Value* to one of the product names listed above.

9d2 Click *Save*.

9e From the Global Filter Configuration dialog, perform these steps for each of the Filter Names you just created:

9e1 Click *Add*.

9e2 Select your newly created filter.

9e3 Check the *Active* check box.

9e4 Set *Action* to the Sentinel Link action configured earlier (“SLinkEAS”, in this example).

9f Set *Default Action* to database.

9g Click *Save*.

2.4 Using the IDM Driver for Sentinel and the Identity Vault Collector

The Sentinel driver and the Identity Vault Collector seamlessly integrate Identity Manager and Sentinel to track user account information. A user account can have one or more identities per system connected to the Identity Vault. The Sentinel driver and the Identity Vault Collector are used together to track each account identity and the status of the account. For more information, see the *Identity Manager Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide* (http://www.novell.com/documentation/ncmp11/ncmp_sentinel_driver/?page=/documentation/ncmp11/ncmp_sentinel_driver/data/bookinfo.html).

2.5 Sending Alerts When Rogue Administration Occurs

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. It sets the user's 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.

2.5.1 Assumptions

The steps for this scenario assume the following:

- ❑ Install and configure the latest available version of Sentinel 6.1 or Sentinel 6.1 RD. For more information, see the *Sentinel 6.1 Installation Guide* (http://www.novell.com/documentation/sentinel61/s61_install/data/) or the *Sentinel 6.1 Rapid Deployment Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/).
- ❑ 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/sentinelplugins.html).
- ❑ Install and configure event Collectors for all integrated systems that are part of the Identity Manager solution. For example, if you are synchronizing 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/sentinelplugins.html).
- ❑ Download the Identity Tracking Solution Pack from the Sentinel Solution Pack Download Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

- ❑ Install and configure Identity Manager 4.0.1 Advanced Edition and the Roles Based Provisioning Module. For more information, see the *Identity Manager 4.0.1 Integrated Installation Guide* (http://www.novell.com/documentation/idm401/idm_integrated_install/?page=/documentation/idm401/idm_integrated_install/data/front.html).
- ❑ Install Designer 4.0.1. For more information, see the *Designer for Identity Manager 4.0.1 Administration Guide* (http://www.novell.com/documentation/idm401/designer_admin/?page=/documentation/idm401/designer_admin/data/front.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/sentinelplugins.html). For configuration documentation for the Identity Manager Collector with Identity Manager, see the *Identity Manager 4.0.1 Reporting Guide for Novell Sentinel* (http://www.novell.com/documentation/idm401/idm_sentinel/?page=/documentation/idm401/idm_sentinel/data/bookinfo.html).
- ❑ Install and configure the Sentinel driver and Identity Vault Collector. For more information, see the *Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

2.5.2 Installing the Identity Tracking Solution Pack

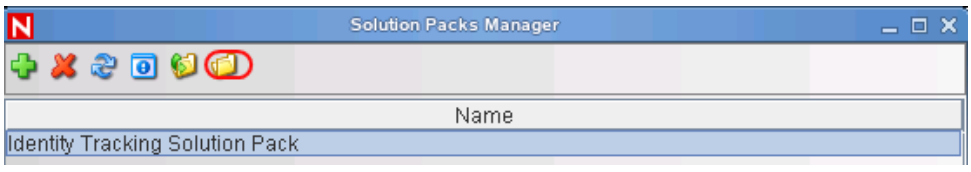
If you have already installed the Identity Tracking Solution Pack, skip this section and proceed directly to Section 2.5.4, “Installing the Rogue Administration Control,” on page 29. If not, see Section 2.2.3, “Installing the Identity Tracking Solution Pack,” on page 20 for instructions on installing the solution pack.

2.5.3 Configuring the Global Setup

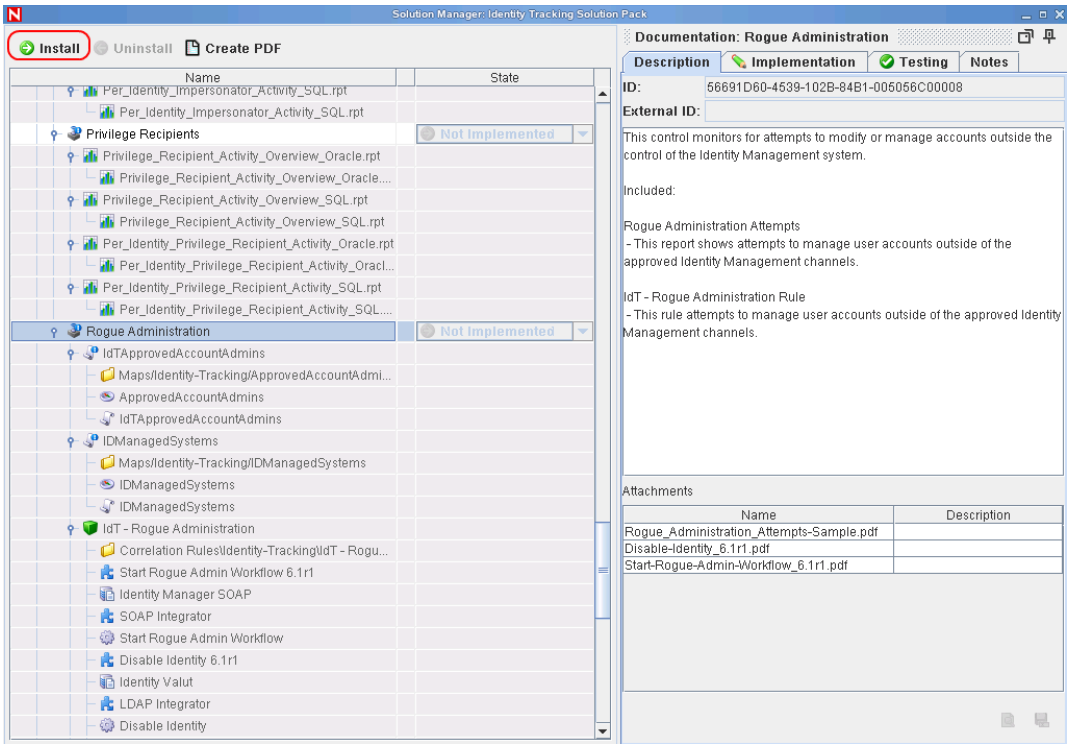
The Identity Tracking Solution Pack requires some global configuration that must be completed. This configuration needs to be completed before any additional configuration. The configuration information is contained in the Identity Tracking Solution Pack. For details on configuring the global setup, see Section 2.2.4, “Configuring the Global Setup,” on page 21.

2.5.4 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*.



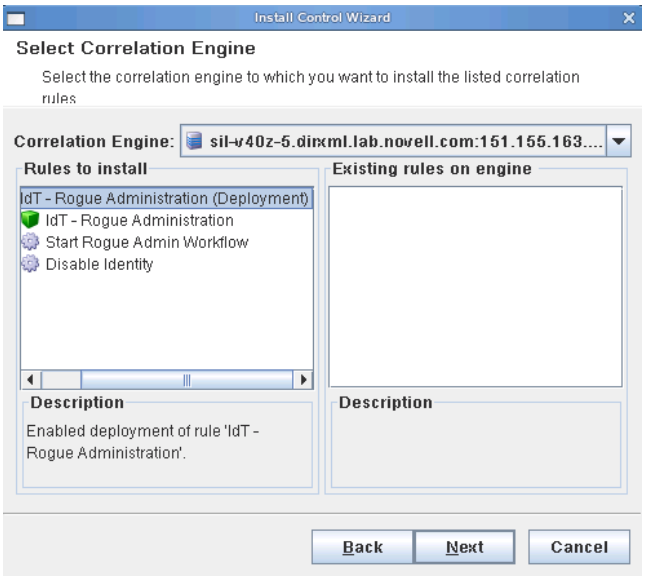
3. Select Rogue Administration in the left pane of the Solution Manager, then click *Install*.



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*.



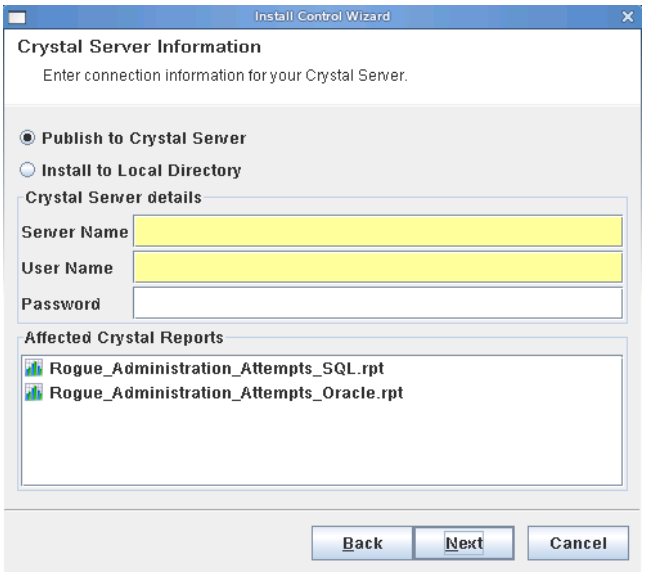
7 Select whether the Crystal server is local or remote by selecting:

- *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*.

2.5.5 Configuring the Rogue Administration Control

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

The following documentation includes instructions for configuring the Disable Identity and Start Rogue Admin Workflow actions. This documentation covers configuration within the Sentinel environment. Additional configuration may be necessary for production environments or if your enterprise is configured in ways that differ from standard installations of integrated systems.

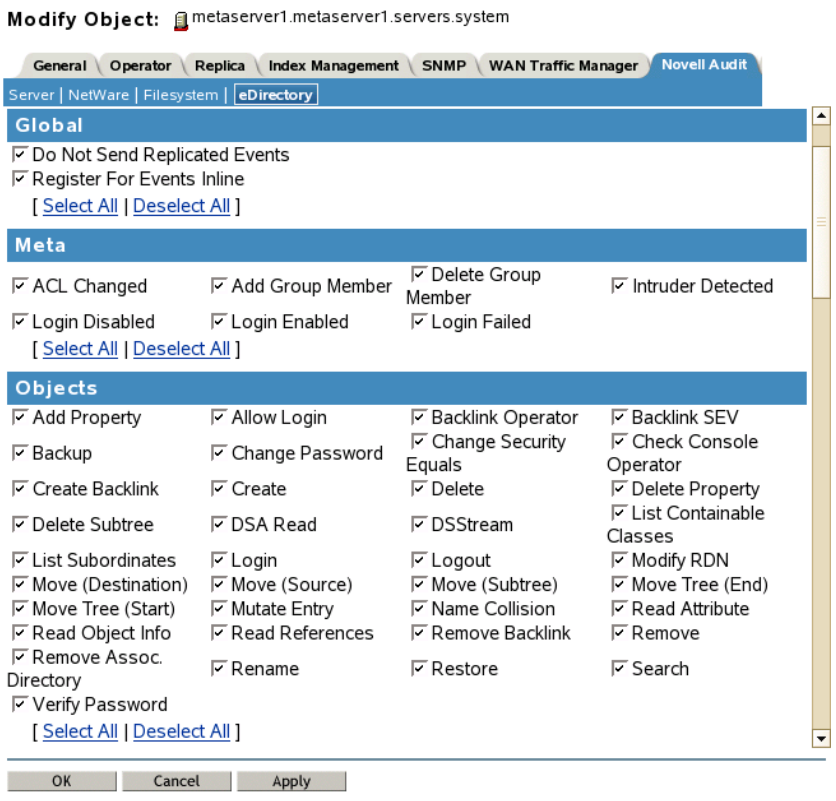
Solution Packs and Action Plugins In many cases, Action Plugins are delivered as part of pre-defined controls within Solution Packs, where they will already be instantiated as Actions, attached to Rules or Menu Tools, and will already be configured to use the appropriate Integrator. This is the case with the Identity Tracking Solution Pack. Installing the Solution Pack control which uses the Action Plugin is sufficient to install all the necessary components. The only configuration you will typically need to perform will be to modify the Integrator configuration to point to the correct integration targets. However, you may need to additionally change some Action parameters that control the Action Plugin.

Enabling Auditing 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. The following figure shows an example of enabling events on the server object.

Figure 2-1 *Enabling Audit Events on eDirectory*

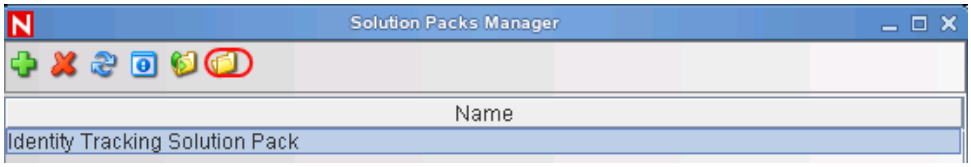


Copying Script Files

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.

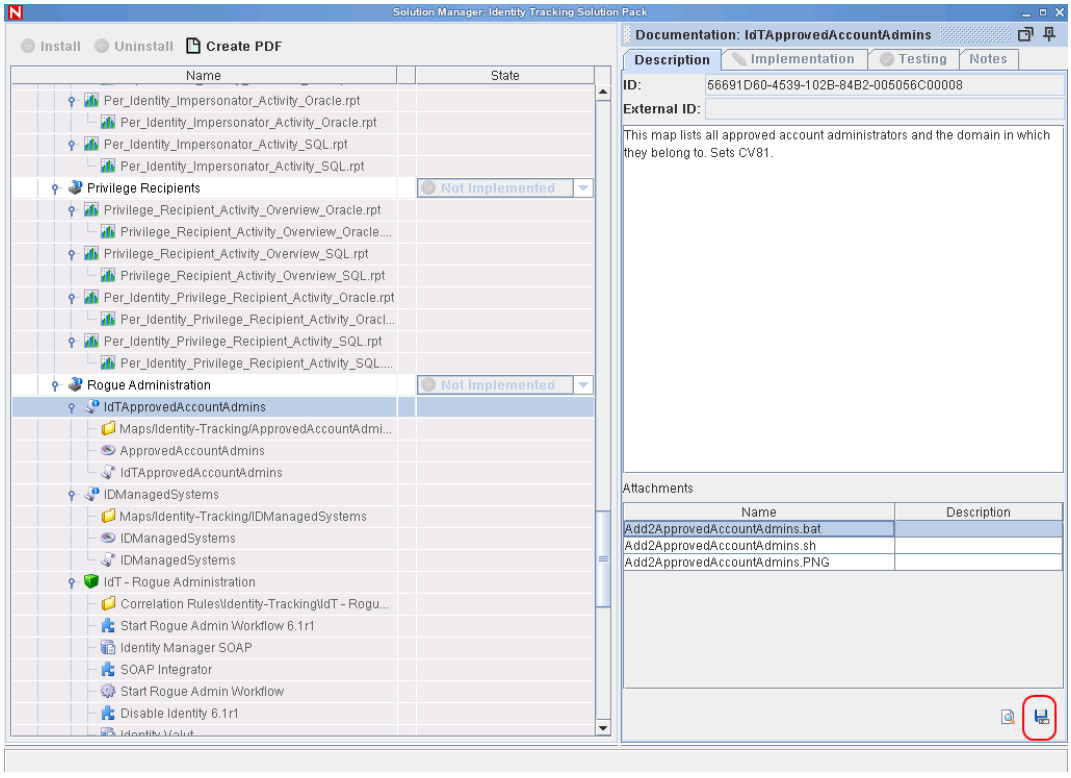
To copy the scripts:

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*.

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. 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.
6. Click *OK* to save the changes.

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*.

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*.

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.

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.

NOTE: The LDAP Integrator is required for the Disable Identity plugin.

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.

Modifying the Sentinel Execution Permissions

Action Plugins run in a protected execution environment that is intended to help protect the system from accidental corruption of the data objects used by Sentinel. The Disable Identity Plugin however, needs to be able to look up information about the identity that it is planning to disable. To allow this, we need to modify the permissions for Action execution.

To modify the permissions:

1 Log into the Sentinel Server machine as a user with privileges to edit files in the ESEC_HOME directory.

2 Locate `ESEC_HOME/config/execution.properties` and open it in a file editor.

3 Append the following line to the file:

```
esecurity.execution.script.context.restricted=false
```

4 Save and close the file.

5 Restart Sentinel:

- Windows: Stop and then Start the *Sentinel* service in the Services Control Panel applet.
- Linux: Execute the following commands as root:

```
/etc/rc.d/sentinel stop
/etc/rc.d/sentinel start
```

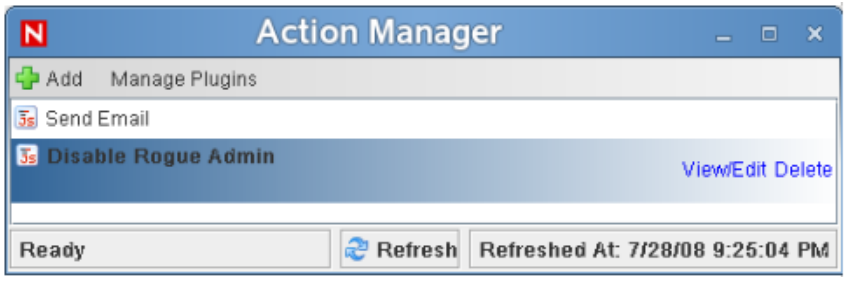
Configuring the Action for Start Rogue Admin Workflow

No changes should be necessary for this Action Plugin as it is included as part of the Identity Tracking Solution Pack. If, however, you have multiple User Applications, you may need to replicate the Integrator configuration and manually configure additional Actions.

1 Log in to the Sentinel Control Center (SCC) as a user with rights to manage Actions (*Permissions* > *Actions* > *Manage Actions*).

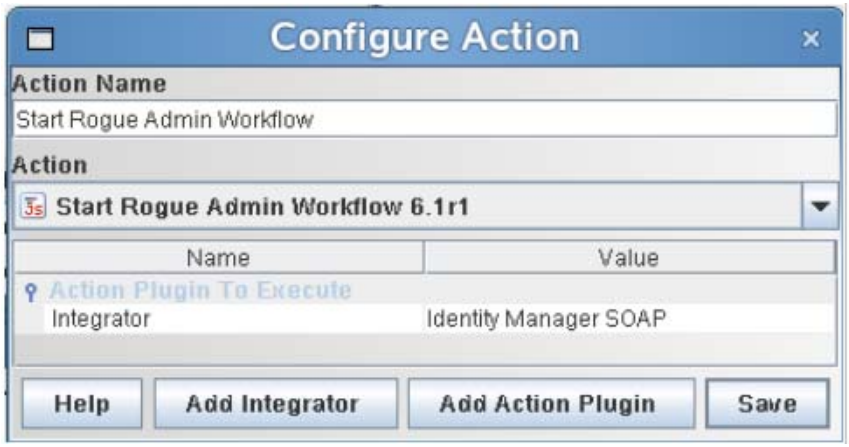
2 Select the menu *Tools* > *Action Manager*.

3 Select the Integrator that was installed as part of this control (this is set as a parameter on the Action if you don't know it) from the list at left.



4 Select the *Add* (plus sign) button to create a new Action.

5 Give the Action a name in the entry box at top.



6 Select the *Add Action Plugin* button at the bottom of the dialog.

7 Use the popup wizard to browse for and install this Action Plugin. Once complete, the name of the Action Plugin should appear in the drop-down list in the Configure Action dialog.

8 Select the plugin name from the drop-down list. The list of configurable parameters for this Plugin should appear.

9 Set the workflow DN for the Rogue Administration Activity workflow that is included as part of the Novell User Application CMP Extension Package. Browse the eDirectory tree and find the User Application container, then locate the workflow definition under that container.

10 Refer to the table below for the parameters that can be configured for this Action Plugin.

Parameter Name	Default Value	Description
Integrator	Identity Manager SOAP	This parameter specifies which Integrator will be used with this Action Plugin. The drop-down list will display all the available configured Integrators.
Workflow DN	CN=Rogue_Administration_Activity,CN=RequestDefs,CN=AppConfig,CN=UserApplication,CN=driverset1,DC=idm,DC=services,DC=system	The LDAP Distinguished Name of the workflow definition – this will be passed to SOAP.

11 Configure the parameters with settings appropriate for your environment.

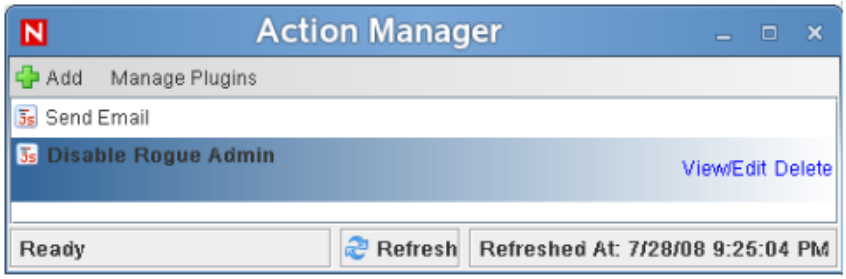
Configuring the Action for Disable Identity

No changes should be necessary for this Action Plugin as it is included as part of the Identity Tracking Solution Pack. If, however, you have multiple Identity Vaults, you may need to replicate the Integrator configuration and manually configure additional Actions.

1 Log in to the Sentinel Control Center (SCC) as a user with rights to manage Actions (*Permissions* > *Actions* > *Manage Actions*).

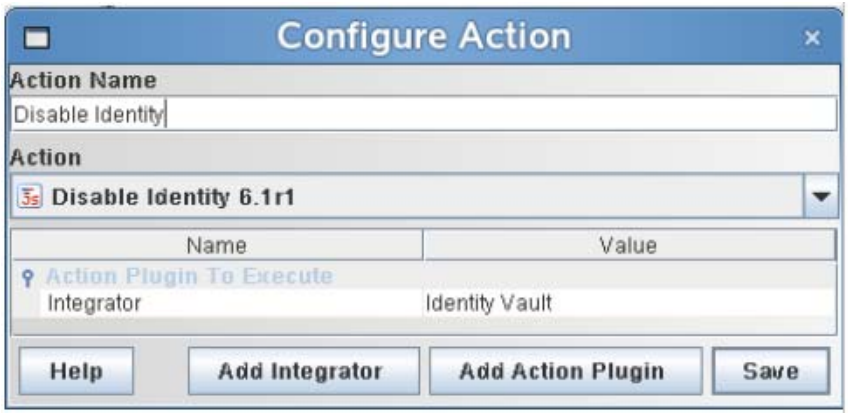
2 Select the menu *Tools* > *Action Manager*.

3 Select the Integrator that was installed as part of this control (this is set as a parameter on the Action if you don't know it) from the list at left.



4 Select the *Add* (plus sign) button to create a new Action.

5 Give the Action a name in the entry box at top.



6 Select the *Add Action Plugin* button at the bottom of the dialog.

7 Use the popup wizard to browse for and install this Action Plugin. Once complete, the name of the Action Plugin should appear in the drop-down list in the Configure Action dialog.

8 Select the plugin name from the drop-down list. The list of configurable parameters for this Plugin should appear.

9 Refer to the table below for the parameters that can be configured for this Action Plugin.

Parameter Name	Default Value	Description
Integrator	Identity Vault	This parameter specifies which Integrator will be used with this Action Plugin. The drop-down list will display all the available configured Integrators.

10 Configure the parameters with settings appropriate for your environment.

2.5.6 Adding the CMP Extension Package to the User Application Driver

Now you need to add the User Application CMP Extension package to the User Application Driver in Designer.

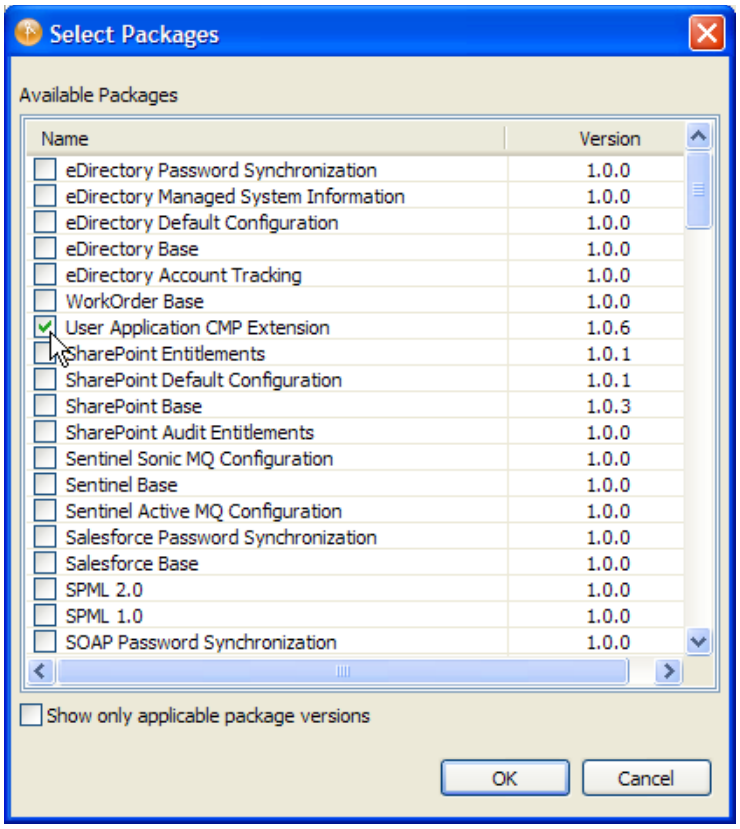
To add the User Application CMP Extension package to the User Application Driver:

1 In the *Developer View*, select the line connecting the User Application Driver to the Identity Vault and click *Properties*.

2 Select *Packages* in the Properties page.

3 Click on the *Add package (+)* symbol in the top right corner.

4 Select the *User Application CMP Extension 1.0.6* package.



5 Click *OK* to install this package.

6 In the Package Installation Wizard, provide values for the following configuration parameters:

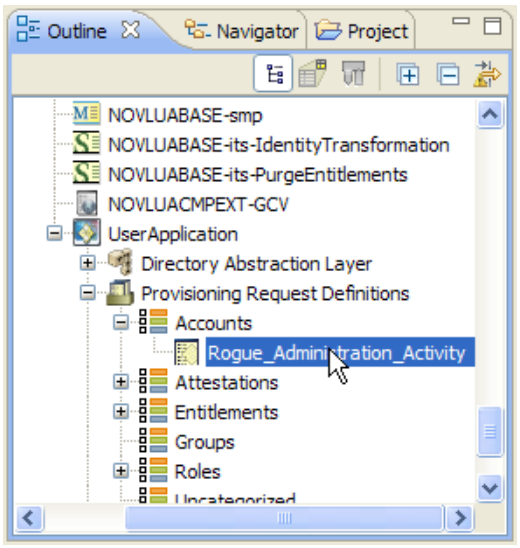
Parameter	Description
Rogue Administration - Security Review Timeout (In Minutes)	Specifies the number of minutes to allow for a security review.
Rogue Administration - Escalation Timeout (In Minutes)	Specifies the number of minutes to allow before an escalation occurs.
Rogue Administration - Escalation Addressee	Specifies the addressee (user) to be notified in the event of an escalation.

These parameters are added as global configuration values (GCVs) on the User Application Driver.

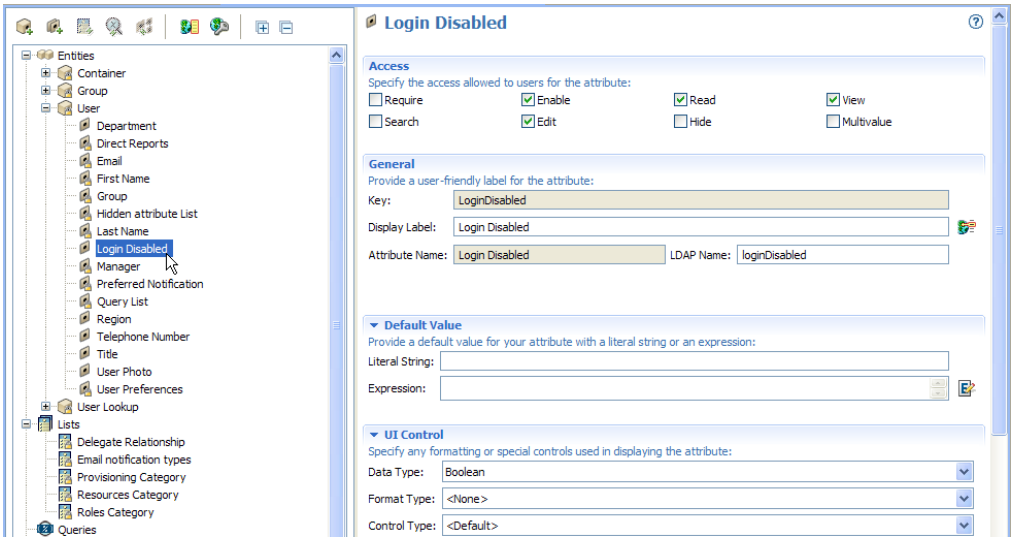
7 Click *Finish*.

8 To verify that the package installation was successful:

8a In the Outline view, look for *Rogue_Administration_Activity* under *Provisioning Request Definitions* > *Accounts* within the driver.



8b Edit the *User* entity in the *Directory Abstraction Layer*, and look for the *Login Disabled* attribute on the entity definition.



9 Deploy the changes to the Identity Vault.

10 Restart the User Application and the User Application driver to apply the changes.

2.6 Configuring the Identity Reporting Module to Work with Novell Access Manager

If you want to integrate Novell Access Manager and the Identity Reporting Module, you need to be aware that Novell does not currently support direct Single Sign On (SSO) between the two products. Instead, one must first access the User Application via Novell Access Manager, and then press the *Access Reporting Module* button on the left-hand navigation menu within the Work Dashboard.

To use this configuration, you need to perform some manual steps to configure the User Application and Novell Access Manager. For details, see the section on "Configuring Reporting to Work With Novell Access Manager" (http://www.novell.com/documentation/idm401/reporting/?page=/documentation/idm401/reporting/data/bobwny3.html#bum94vs) in the *Identity Reporting Module Guide*.

Upgrading from CMP 1.0.1

3

This section describes some steps you will need to take if you upgrading from CMP 1.0.1.

3.1 Upgrading the User Application Driver

When you upgrade to CMP 1.1, you need to create a new User Application Driver using the new package facility provided with Designer. The driver must include the CMP Extension Package. For details on how to create the new driver, see Section 2.5.6, “Adding the CMP Extension Package to the User Application Driver,” on page 39.

3.2 Creating the Sentinel Driver Using Package Manager

When you upgrade to CMP 1.1, you need to create a new Sentinel Driver using the new package management facility provided with Designer. For details on how to create the driver, see “Creating a New Driver” in the *Driver for Sentinel 6.1 and the Identity Vault Collector Implementation Guide*.

3.3 Upgrading the Identity Tracking Solution Pack

If you want to upgrade the Identity Tracking Solution Pack, follow these steps:

1. Uninstall each control in your existing Identity Tracking Solution Pack.
2. Uninstall the existing Identity Tracking Solution Pack.
3. Install the new Identity Tracking Solution Pack for CMP 1.1.