Identity Tracking

6.1r1

Aug 2008

www.novell.com

SENTINEL® SOLUTION OVERVIEW

Novell®

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. 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 a list of 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

1 Introduction

This Novell Sentinel® Solution Overview will get you started with understanding the Identity Tracking Solution Pack provided by Novell and how it can help you solve your business needs by leveraging Sentinel's Solution framework and unmatched integration and remediation functionality. @PLUGDESC@

1.1 Audience

This guide is intended to introduce customers and partners to the features provided by the Identity Tracking Solution Pack and related Sentinel features.

1.2 Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product, as well as requests for other Sentinel content. Please submit all comments and suggestions via the web form at

http://support.novell.com/products/sentinel/secure/survey.html

1.3 Documentation Updates

For the most recent version of this Sentinel Solution Overview, visit the Sentinel Plugin website at:

http://support.novell.com/products/sentinel/index.html

and select the links to your version of Sentinel at the bottom of the webpage.

1.4 Additional Documentation

For additional documentation about the Sentinel platform, please view the Sentinel Product Documentation:

http://www.novell.com/documentation/sentinel61/index.html

2 Solution Overview

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, this Solution integrates data from Novell and third-party applications to give unprecedented visibility into user activities and identity/account management.

This Solution sits atop of a coordinated suite of applications called the Novell Compliance Management Platform which have been tailored and improved to work tightly together to solve your business needs. The core products of this platform include:

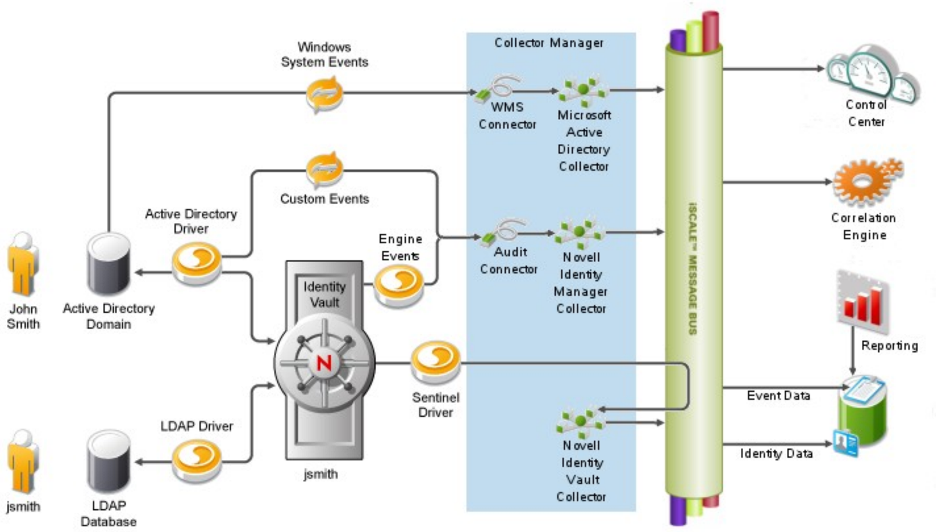
- **Novell Identity Manager** – provides full control over the user identity lifecycle including account provisioning and termination, role management, and password management.
- **Novell Access Manager** – provides local and remote access management to enterprise applications, including SSL-VPN services and identity-based access control.
- **Novell Sentinel** – provides security information and event management, specifically designed to leverage data from the preceding Novell applications to enhance the usefulness of that information and speed remediation times.

Major improvements have been made in each component in this suite of products to support this integrated platform. A brief list of improvements to Sentinel include:

2.1.1 Identity Framework

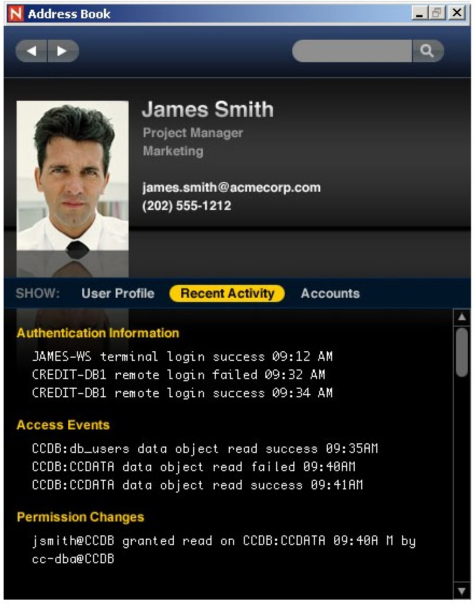
Sentinel now includes the ability to correlate and report at the user identity level, across multiple accounts held by that user. Identity information is loaded into the Sentinel database, inserted into incoming events, and available for lookup from the Sentinel Control Center interface.

The Identity Framework is enabled by integration with Identity Manager, which uses a combination of a Identity Manager Sentinel driver and Sentinel Identity Vault Collector to gather and store identity and account information for use by Sentinel.



2.1.2 Identity Browser

If identity information is populated into the Sentinel database, the Identity Browser provides the ability to look up any identity and view information about accounts held by that identity and recent actions taken by that user (such as the last 10 authentications). This information can be accessed by searching for a particular user or by right-clicking an event that references a particular user.



James Smith
Project Manager
Marketing

james.smith@acmecorp.com
(202) 555-1212

Authentication Information

```
JAMES-WS terminal login success 09:12 AM
CREDIT-DB1 remote login failed 09:32 AM
CREDIT-DB1 remote login success 09:34 AM
```

Access Events

```
CCDB:db_users data object read success 09:35AM
CCDB:CCDATA data object read failed 09:40AM
CCDB:CCDATA data object read success 09:41AM
```

Permission Changes

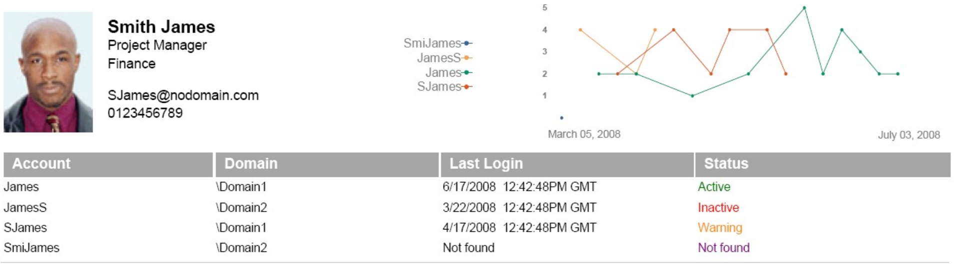
```
jsmith@CCDB granted read on CCDB:CCDATA 09:40A M by
cc-dba@CCDB
```

2.1.3 Database Extensions

New tables have been added for the Account, Identity, and Trust information (the Trust tables are reserved for future expansion). Additional fields have been added to the database for custom and reserved information.

2.1.4 Identity Enhanced Reporting

Sentinel reports have been enhanced to take advantage of user identity information through integration with an identity management system. For example, the report below shows that James Smith, a Project Manager in Finance, has four accounts that he has access to. Only one of these seems to be in active use, the other three have not been used for over 60 day, over 90 days, and apparently never, respectively.



Smith James
Project Manager
Finance

SJames@nodomain.com
0123456789

Account	Domain	Last Login	Status
James	\Domain1	6/17/2008 12:42:48PM GMT	Active
JamesS	\Domain2	3/22/2008 12:42:48PM GMT	Inactive
SJames	\Domain1	4/17/2008 12:42:48PM GMT	Warning
SmiJames	\Domain2	Not found	Not found

2.1.5 Enhanced Integration with Novell Identity Manager

Identity integration with Novell Identity Manager is provided by the Integration Pack for Novell Compliance Management Platform. Some of the pieces of this optional package include a Novell Identity Manager Sentinel driver and the Sentinel Identity Vault Collector that work together to synchronize identity information from the Identity Manager Identity Vault to the Sentinel Database.

2.1.6 Action Framework Changes

Event Menu Actions and Correlation Actions have been moved to the Tools menu. These actions can now be written in JavaScript and treated as plugins, simplifying management. The JavaScript option replaces the existing Execute Command option, which is now only available in the context of existing Execute Command actions. Actions can further leverage Integrators (see below) for access to external systems.

2.1.7 New Integrator Plugins for External Connectivity

Integrators provide connectivity to external systems to execute actions that are initiated by a triggered correlation rule or by the selection of a right-click menu tool in the Sentinel Control Center. The following integrators are preloaded in the Sentinel system:

- **SOAP Integrator**: used to initiate actions using calls to a SOAP server

- **LDAP Integrator**: used to set or change attributes in an LDAP directory
- **SMTP Integrator**: used for all e-mail messages sent by Sentinel

2.1.8 JavaScript Collectors

Collectors can be written in the industry-standard JavaScript* language in addition to the proprietary (legacy) Novell collector scripting language. Collector Managers run both types of collectors simultaneously. The Sentinel 6.1 release includes an SDK for writing JavaScript collectors.

JavaScript Collectors provides richer data manipulation functionality, efficiency, and the ability to process double-byte/Unicode* data.

2.1.9 Naming and Taxonomy Changes to Conform with XDAS

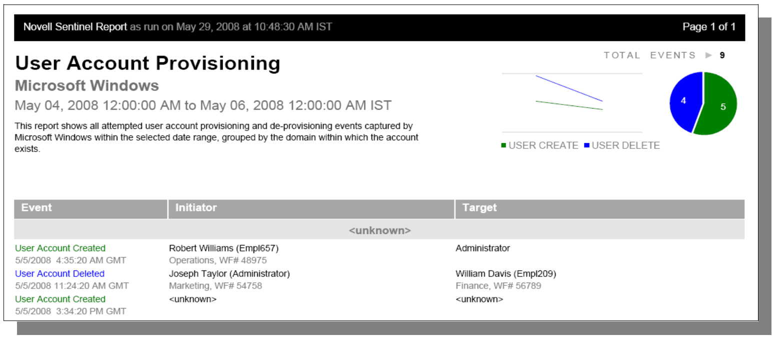
Sentinel uses a hierarchical event taxonomy to categorize and classify events from a wide variety of event sources. This feature simplifies analysis, correlation, and reporting on distributed events by ensuring that common activities are expressed consistently regardless of which platform they came from.

With Sentinel 6.1, the legacy taxonomy is aligned with an emerging open standard called XDAS. XDAS is a standard maintained by The Open Group (http://www.opengroup.org/) in partnership with MITRE (http://www.mitre.org/).

2.1.10 Upgrades to Novell Application Collectors

Existing Collectors for Novell Applications have been updated to conform to the new Sentinel 6.1 schema and taxonomy and to support the new identity-injection features. Each Collector now includes a Collector Pack that provides control-based operation management for that Collector and enhanced visibility into data from that Collector.

For example, the Novell eDirectory Collector Pack now includes reports to show event trends for data from that Collector; account management events from eDirectory including account creation, modification, and password changes; trust and generic object management reports, and authentication reports. A few samples are presented below:



Novell Sentinel Report as run on May 29, 2008 at 10:48:30 AM IST Page 1 of 1

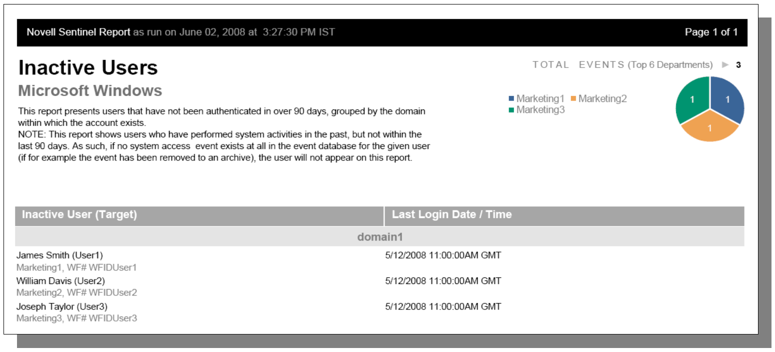
User Account Provisioning

Microsoft Windows

May 04, 2008 12:00:00 AM to May 06, 2008 12:00:00 AM IST

This report shows all attempted user account provisioning and de-provisioning events captured by Microsoft Windows within the selected date range, grouped by the domain within which the account exists.

Event	Initiator	Target
<unknown>		
User Account Created 5/5/2008 4:35:20 AM GMT	Robert Williams (Empl657) Operations, WF# 48975	Administrator
User Account Deleted 5/5/2008 11:24:20 AM GMT	Joseph Taylor (Administrator) Marketing, WF# 54758	William Davis (Empl209) Finance, WF# 56789
User Account Created 5/5/2008 3:34:20 PM GMT	<unknown>	<unknown>



Novell Sentinel Report as run on June 02, 2008 at 3:27:30 PM IST Page 1 of 1

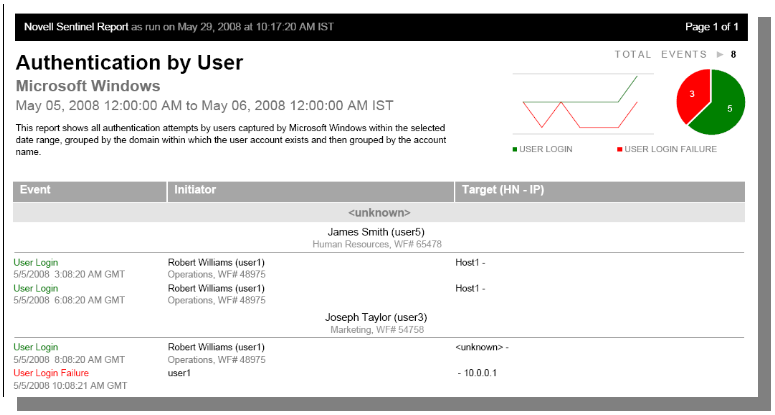
Inactive Users

Microsoft Windows

This report presents users that have not been authenticated in over 90 days, grouped by the domain within which the account exists.
NOTE: This report shows users who have performed system activities in the past, but not within the last 90 days. As such, if no system access event exists at all in the event database for the given user (if for example the event has been removed to an archive), the user will not appear on this report.

TOTAL EVENTS (Top 6 Departments) ▶ 3
■ Marketing1 ■ Marketing2
■ Marketing3
1
1
1

Inactive User (Target)	Last Login Date / Time
domain1	
James Smith (User1) Marketing1, WF# WFIDUser1	5/12/2008 11:00:00AM GMT
William Davis (User2) Marketing2, WF# WFIDUser2	5/12/2008 11:00:00AM GMT
Joseph Taylor (User3) Marketing3, WF# WFIDUser3	5/12/2008 11:00:00AM GMT



Novell Sentinel Report as run on May 29, 2008 at 10:17:20 AM IST — **Page 1 of 1**

Authentication by User

Microsoft Windows

May 05, 2008 12:00:00 AM to May 06, 2008 12:00:00 AM IST

This report shows all authentication attempts by users captured by Microsoft Windows within the selected date range, grouped by the domain within which the user account exists and then grouped by the account name.

Event	Initiator	Target (HN - IP)
<unknown>		
James Smith (user5) Human Resources, WF# 65478		
User Login 5/5/2008 3:08:20 AM GMT	Robert Williams (user1) Operations, WF# 48975	Host1 -
User Login 5/5/2008 6:08:20 AM GMT	Robert Williams (user1) Operations, WF# 48975	Host1 -
Joseph Taylor (user3) Marketing, WF# 54758		
User Login 5/5/2008 8:08:20 AM GMT	Robert Williams (user1) Operations, WF# 48975	<unknown> -
User Login Failure 5/5/2008 10:08:21 AM GMT	user1	- 10.0.0.1

2.1.11 Upgrades to Third-Party Application Collectors

Existing Collectors for third-party Applications have been updated to conform to the new schema and taxonomy as well, starting with Microsoft Active Directory. These new Collectors include the same basic reports provided for Novell applications (above) and are fully enabled for identity injection if paired with the corresponding Identity Manager driver.

2.1.12 New Identity Vault Collector

A new Collector is provided to support collecting identity data from Identity Manager so that it can be injected into events and reports. This Collector works in partnership with the Identity Manager Sentinel driver to collect and store a complete set of identity information along with information about associated accounts.

2.2 Recommended Configuration

The following simple two-server configuration is a good starting point for the Novell Sentinel portion of the Novell Compliance Management Platform. This configuration should be sufficient to handle approximately 500 events per second.

In some situations, a different configuration may be recommended. Sentinel can be implemented on Linux or Solaris with an Oracle database, or the system can be distributed to additional machines to handle higher event rates. For more information, work with Novell Consulting or see the Sentinel Installation Guide at the Novell Documentation site (http://www.novell.com/documentation/sentinel61).

2.2.1 Sentinel Server and Database

Recommended Hardware:

- 2 x Quad Core Intel® Xeon® E5430, 2x6MB Cache, 2.66GHz, 1333MHz FSB
- 16 GB memory
- 6 x 500GB 7200 RPM SATA drives configured with hardware RAID 5

Recommended Software:

- Windows 2003 SP1, Standard Edition (64-bit)
- Microsoft SQL Server 2005 SP2, Standard Edition (64-bit)

You should check with the respective vendors for security updates and patches. These hotfixes and security patches typically have no impact on Sentinel operations and are therefore supported. Since major or minor releases of a database or operating system typically involve more substantial changes, only the versions above are supported for this release.

2.2.2 Reporting Server

The supported reporting server, BusinessObjects Crystal Reports Server XI R2 SP3, requires a web server and a Central Management Server (CMS) database for operation, in addition to the Sentinel database.

The following hardware is recommended for the Crystal Reports Server:

- 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)
- 4 GB RAM
- 20GB disk space

The following software is recommended on the Crystal Reports Server machine:

- Windows 2003 SP1 Server, Standard Edition (32-bit)
- Crystal Reports Server XI R2 SP3
- Microsoft SQL Server 2005 for the Crystal CMS database
- Microsoft IIS with .NET

The Crystal service packs can be downloaded from the Download section of the SAP web site at

https://www.sdn.sap.com/irj/sdn/businessobjects-downloads

See the vendor documentation for additional detail about system requirements, supported version numbers, and known issues for these platforms.

2.3 Solution Summary Details

The Identity Tracking Solution Pack includes the following categories and controls:

2.3.1 Control Summary

- **Solution Pack Controls** – *Controls related to the management of the Pack itself*
  - **Dashboard Status** – *Provides an overview of the rollout status of the Solution as a whole*
  - **Implementation Audit Trail** – *Monitors for state changes to controls in this Solution, with alerting and summary reports which show who changed the state of which controls*
- **Identity Management Controls** – *This control area consists of controls to manage the creation, deletion, and modification of identities and their associated accounts within the enterprise.*
  - **Identity Provisioning** – *This control provides a set of reports to monitor common identity provisioning actions within the enterprise.*
  - **Identity De-Provisioning** – *This control provides a set of reports and rules to monitor common identity de-provisioning and access violation actions within the enterprise.*
- **Suspicious Activity Controls** – *This control area consists of several controls to help you monitor suspicious activity within the enterprise.*
  - **Suspicious Activity Overview** – *This control presents an overview of suspicious activity within the enterprise. It summarizes the succeeding six categories of suspicious activity, not including Rogue Administration.*
  - **Authentication Failures** – *This control provides details about Identity-based authentication failures across the enterprise.*
  - **Access Denials** – *This control 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** – *This control 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** – *This control 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.*
  - **Impersonators** – *This control provides details about users who after logging in with their own identity then attempted to log in to other assets under an account associated with a different identity. Best practices dictate that users should only know credentials for accounts associated with their identity, and use privilege escalation to access administrative accounts.*
  - **Privilege Recipients** – *This control 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** – *This control monitors for attempts to modify or manage accounts outside the control of the Identity Management system.*
- **Account Usage Management Controls** – *This control area provides information about how accounts are being used within the enterprise.*
  - **Account Usage** – *This control 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** - *This control area provides monitoring of password management within the enterprise.*
  - **Password Changes** – *This control provides a set of reports related to the password management of accounts.*
- **Recent Activity Controls** – *This control area provides details about an individual's enterprise activity.*
  - **Recent Activity** – *This control provides a set of reports to monitor the activity performed by the users in recent past within the enterprise.*

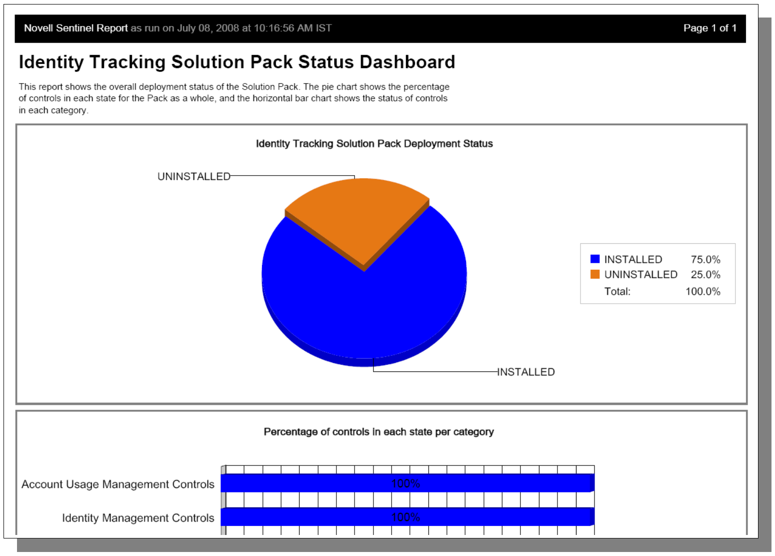
2.3.2 Content Summary

#	Type
24	*Reports*
8	*Correlation Rules*
1	*Workflows*
8	*Actions*
2	*Integrators*

2.4 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 *Solution Pack Status Dashboard* shows an overview of the rollout status of the Solution as a whole:



Novell Sentinel Report as run on July 08, 2008 at 10:16:56 AM IST Page 1 of 1

Identity Tracking Solution Pack Status Dashboard

This report 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.

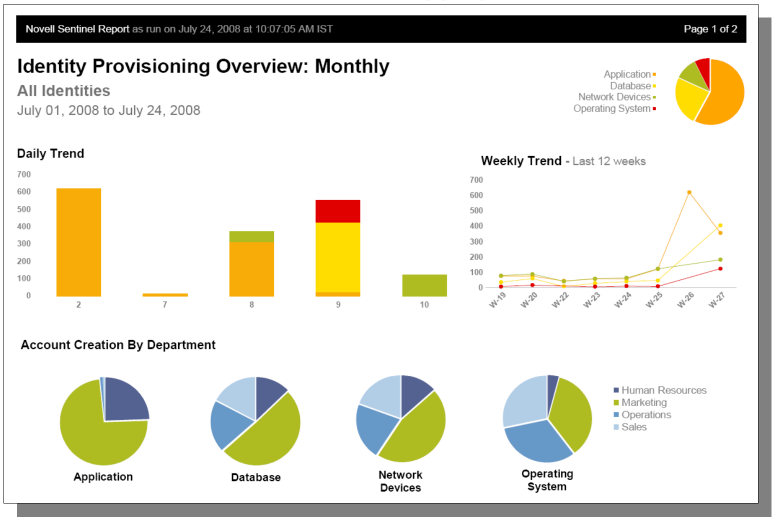
Identity Tracking Solution Pack Deployment Status

🟦	INSTALLED	75.0%
🟧	UNINSTALLED	25.0%
	Total:	100.0%

Percentage of controls in each state per category

UNINSTALLED
INSTALLED
Account Usage Management Controls
100%
Identity Management Controls
100%

- The *Identity Provisioning Overview* report presents an overview of account management activity in the enterprise and ties it back to individual identities where appropriate.



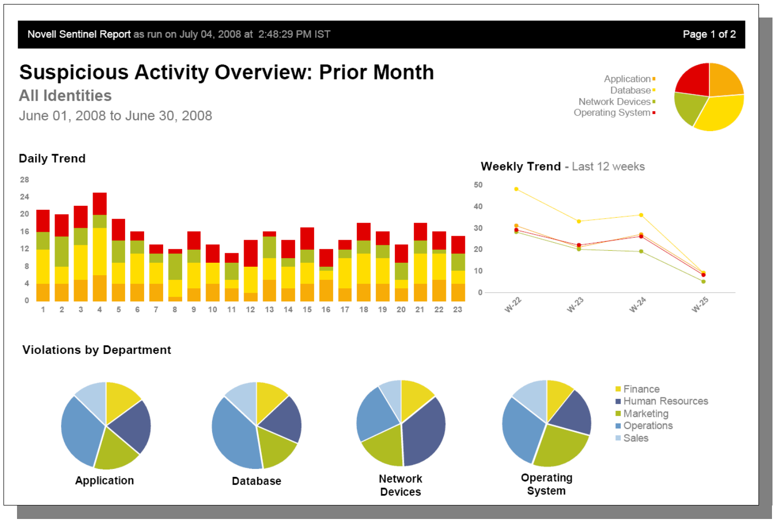
Novell Sentinel Report as run on July 24, 2008 at 10:07:05 AM IST Page 1 of 2

Identity Provisioning Overview: Monthly

All Identities

July 01, 2008 to July 24, 2008

- The *Suspicious Activity Overview* report presents summaries of six different types of suspicious activity that could occur in the enterprise. It leverages Identity information to tie that activity back to the actual person that caused the suspicious activity to occur.



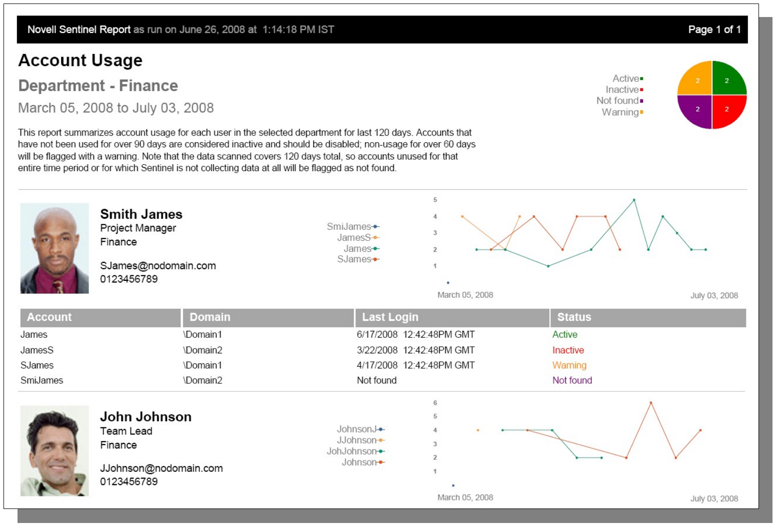
Novell Sentinel Report as run on July 04, 2008 at 2:48:29 PM IST — **Page 1 of 2**

Suspicious Activity Overview: Prior Month

All Identities

June 01, 2008 to June 30, 2008

- The *Account Usage* report 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 to be inactive.



Novell Sentinel Report as run on June 26, 2008 at 1:14:18 PM IST — **Page 1 of 1**

Account Usage

Department - Finance

March 05, 2008 to July 03, 2008

This report 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 be flagged as not found.

Smith James
Project Manager
Finance

SJames@nodomain.com
0123456789

Account	Domain	Last Login	Status
James	\Domain1	6/17/2008 12:42:48PM GMT	Active
JamesS	\Domain2	3/22/2008 12:42:48PM GMT	Inactive
SJames	\Domain1	4/17/2008 12:42:48PM GMT	Warning
SmiJames	\Domain2	Not found	Not found

John Johnson
Team Lead
Finance

JJohnson@nodomain.com
0123456789

3 Quickstart

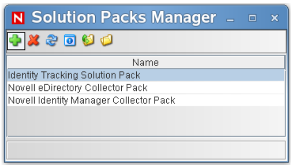
To get started on using this Solution Pack:

1. Download the latest version from the Novell Sentinel Plugin website:

   http://support.novell.com/products/sentinel/sentinel61.html

   NOTE: In some cases, the Solution Pack is an add-on that requires an additional license to be purchased before you will be entitled to download the Plugin.

2. Start the Sentinel Control Center and log in as a user with rights to manage Solution Packs (*Permissions* > *Solution Pack* > *Solution Manager* must be checked).
3. Start the Solution Pack Manager via the menu *Tools* > *Solution Packs*.
4. Select the green *Add* button to start the import wizard.
5. Browse to select the Plugin file you just downloaded, then select *Next*.
6. Review the Plugin details and select *Next* to import the Plugin. The new Plugin should appear in the Solution Packs Manager list.



Name
Identity Tracking Solution Pack
Novell eDirectory Collector Pack
Novell Identity Manager Collector Pack

7. Select the new Solution Pack from the list, then open it in Solution Manager by selecting the *Open* button.

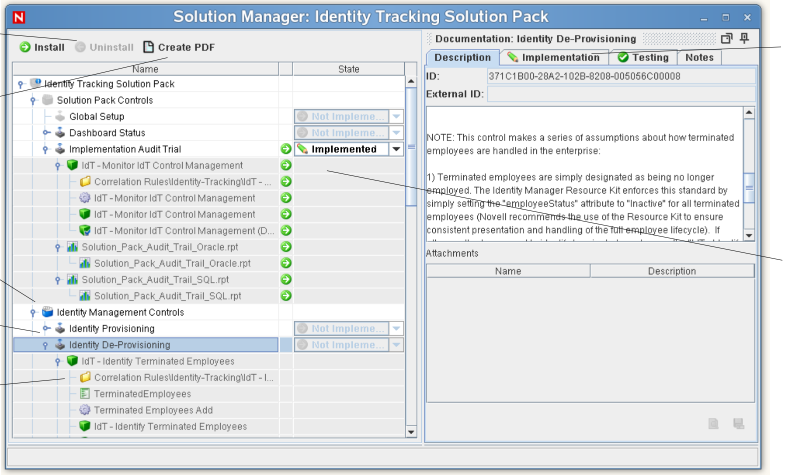
Install/Uninstall
When a control is selected, these buttons will install or uninstall all associated content.

Create PDF
Generates PDF documentation for this Solution.

Categories
Groupings of similar controls.

Controls
Sets of content intended to solve a specific business problem.

Content
The individual reports, rules, workflows, actions, and integrators that make up a given control.


Solution Manager: Identity Tracking Solution Pack
Install
Uninstall
Create PDF
Documentation: Identity De-Provisioning
Description
Implementation
Testing
Notes

Name	State
Identity Tracking Solution Pack	
Solution Pack Controls	
Global Setup	Not Impleme...
Dashboard Status	Not Impleme...
Implementation Audit Trial	Implemented
IdT - Monitor IdT Control Management	
Correlation Rules\Identity-Tracking\IdT - ...	
IdT - Monitor IdT Control Management	
IdT - Monitor IdT Control Management	
IdT - Monitor IdT Control Management (D...	
Solution_Pack_Audit_Trail_Oracle.rpt	
Solution_Pack_Audit_Trail_Oracle.rpt	
Solution_Pack_Audit_Trail_SQL.rpt	
Solution_Pack_Audit_Trail_SQL.rpt	
Identity Management Controls	
Identity Provisioning	Not Impleme...
Identity De-Provisioning	Not Impleme...
IdT - Identify Terminated Employees	
Correlation Rules\Identity-Tracking\IdT - I...	
TerminatedEmployees	
Terminated Employees Add	
IdT - Identify Terminated Employees	

ID: 371C1B00-28A2-102B-8208-005056C00008

External ID:

NOTE: 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 Identity Manager Resource Kit enforces this standard by simply setting the "employeeStatus" attribute to "Inactive" for all terminated employees (Novell recommends the use of the Resource Kit to ensure consistent presentation and handling of the full employee lifecycle). If

Attachments

Name	Description

Documentation
Description, steps for implementation, and steps for testing are all included directly within the Solution Pack.

Status
The current status of each control or content element is indicated here. If the control state is changed, an audit event is generated listing the user who made the change.

8. Select the *Create PDF* button to generate complete, detailed PDF documentation for this Solution Pack, including implementation and testing steps for each control. Note that you have two additional options:
   1. Show Status Information – This adds current status information to the generated PDF, equivalent to what you see in the State column of the Solution Manager interface.
   2. Include Content Nodes – Includes additional details about the individual content elements included within each control. Note that this can add many pages to the produced document.

4 Revision History

Release Notes

6.1r1

- Initial version: core set of controls that demonstrate the power of this solution

Known Issues

- For SQL Server reports, if internal SQL Server statistics are not kept up to date reports may take longer than normal to complete. A script is attached which will help repair SQL Server's internal statistics counters.