Novell®

Workflow und Identity Management - Genehmigungsprozesse, Role Mining, Role Design und Compliance Management

Stefan Stiehl
Senior Technology Sales Specialist
Identity Security Management

sstiehl@novell.com

Novell®

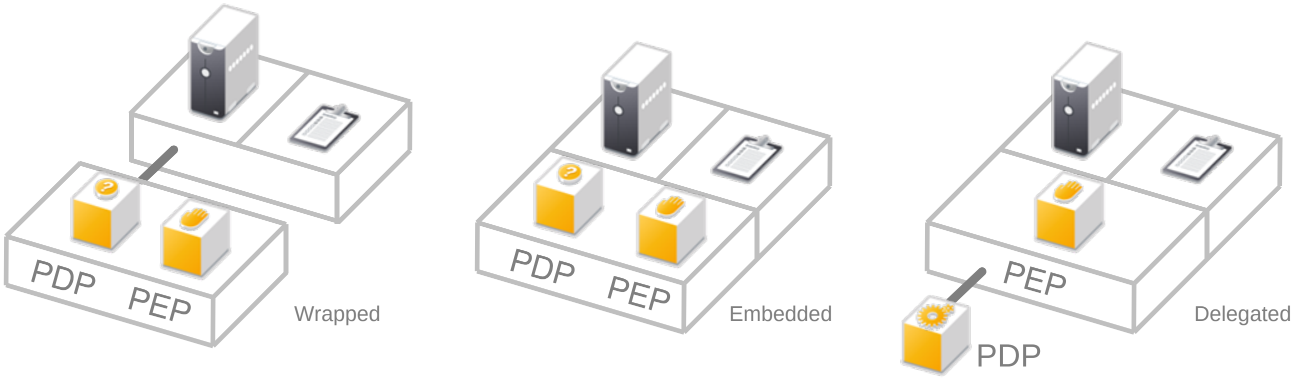
Compliance Management Models

- Compliance
  with is in-process assurance that the right work is done in the right way by the right entities

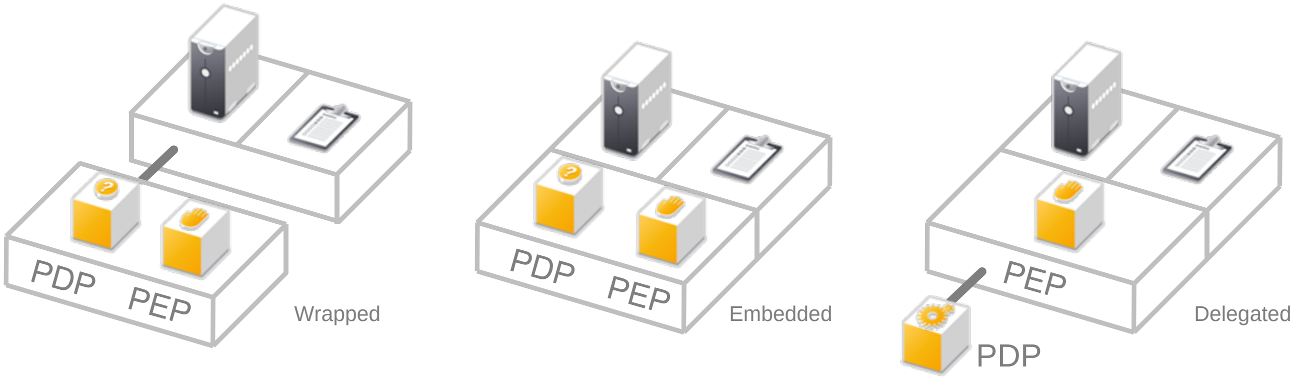
- Policy
  that expands to cover more services, applications and plattforms with increased flexibility and automation, providing simplified, authoritative, resource and access management

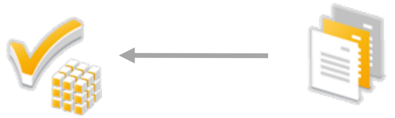
- Identity
  allows policy engines to reason about parts of the system

Compliance Management Models

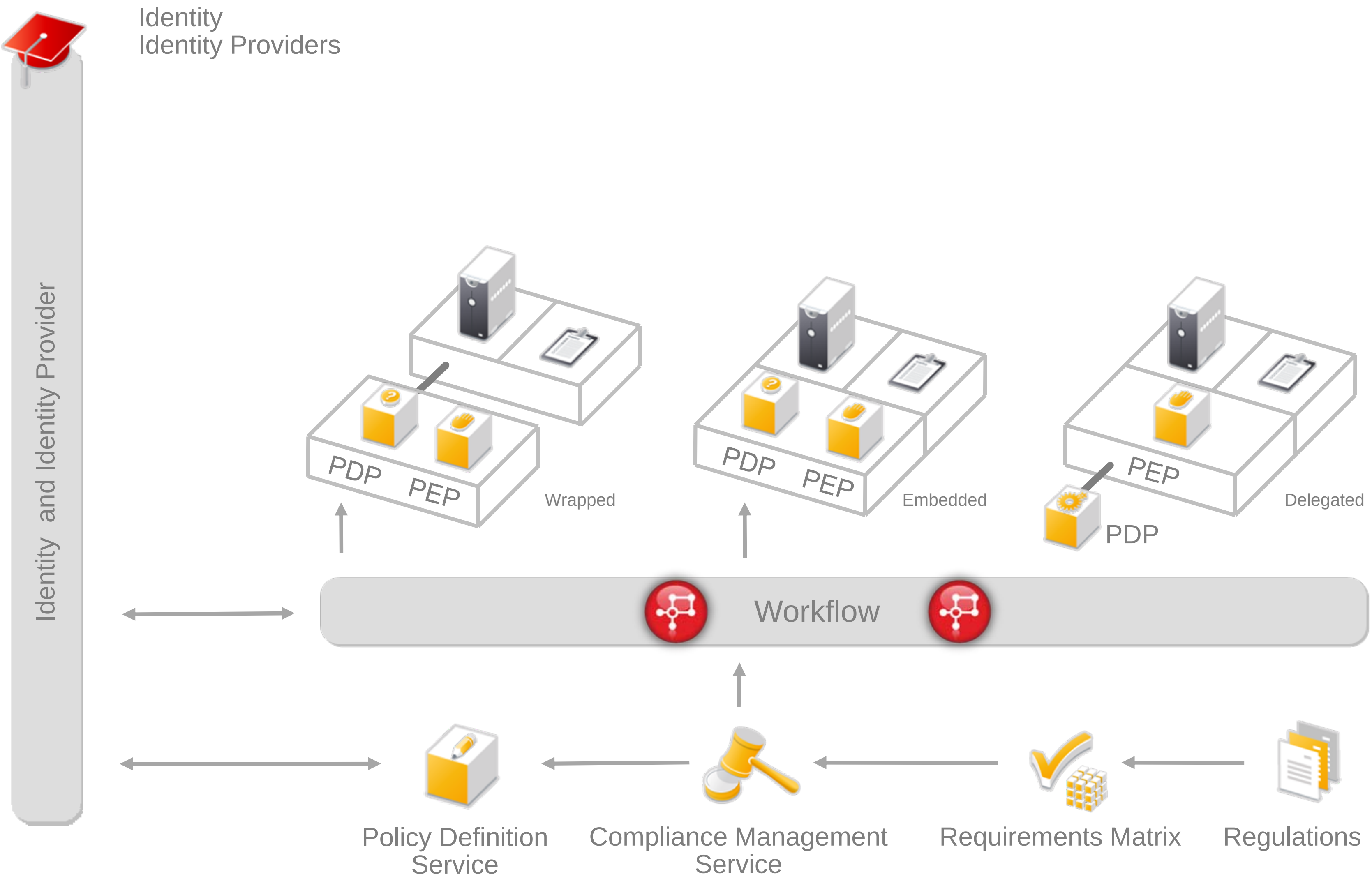


Compliance Management Models

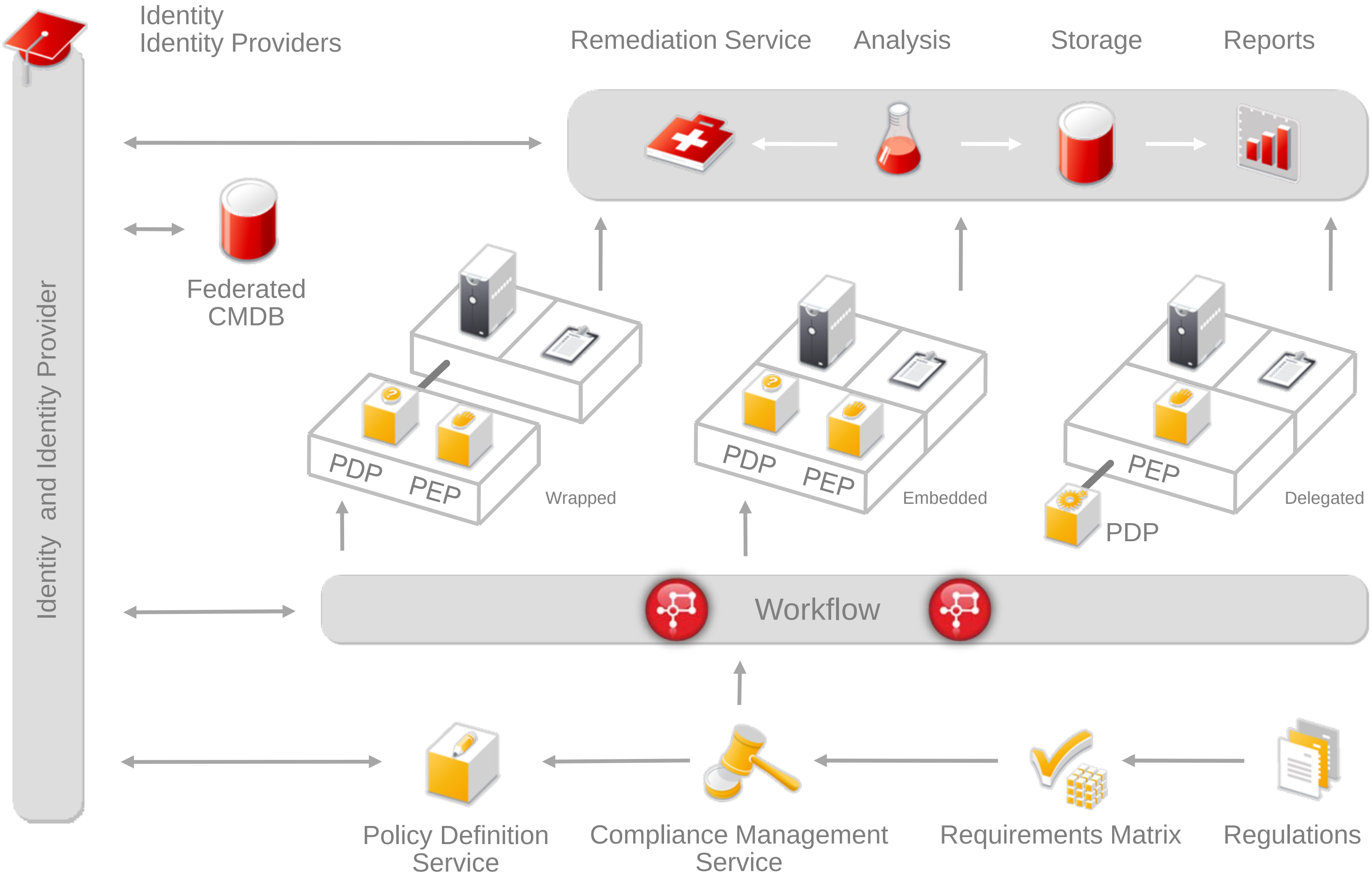




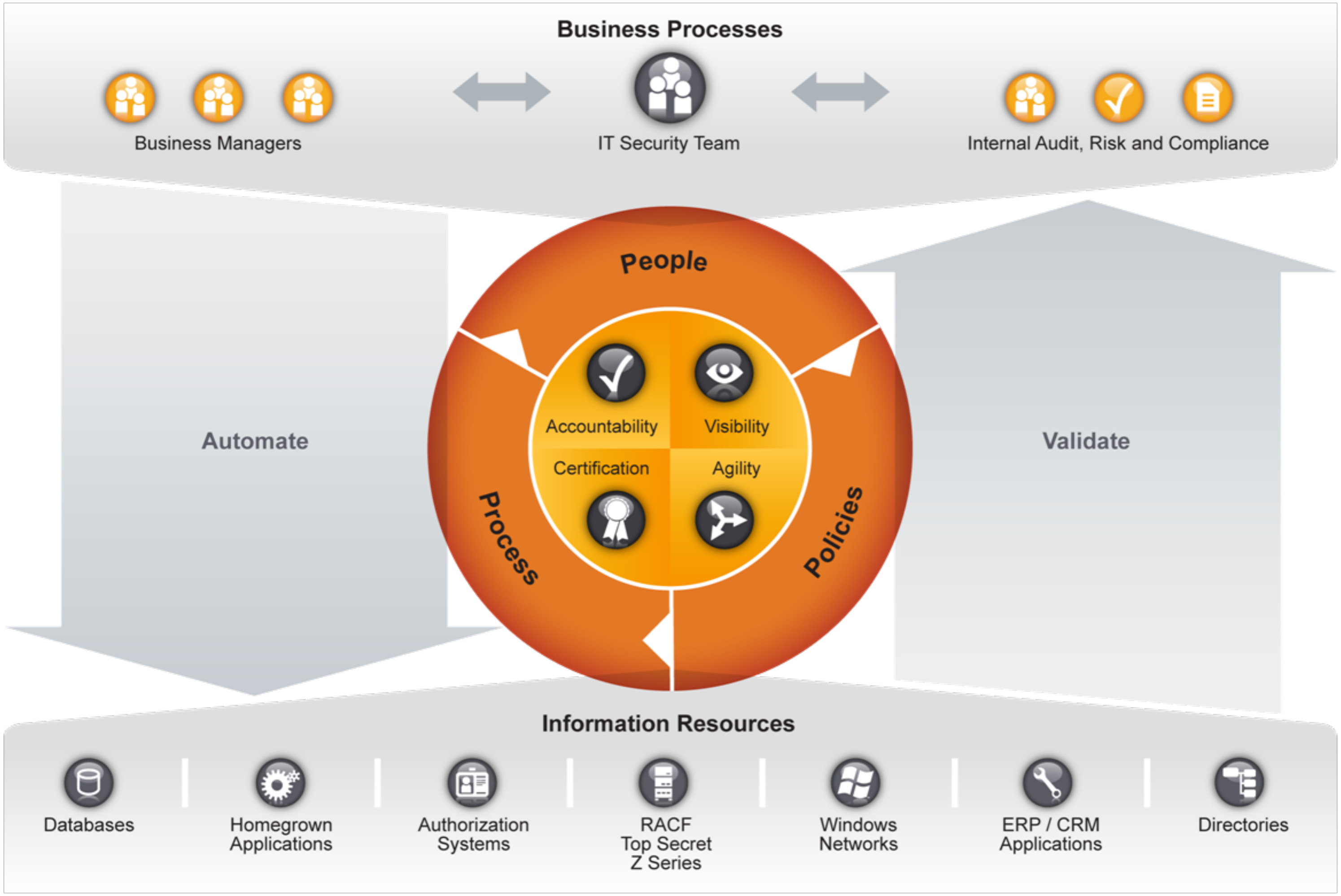
Compliance Management Models



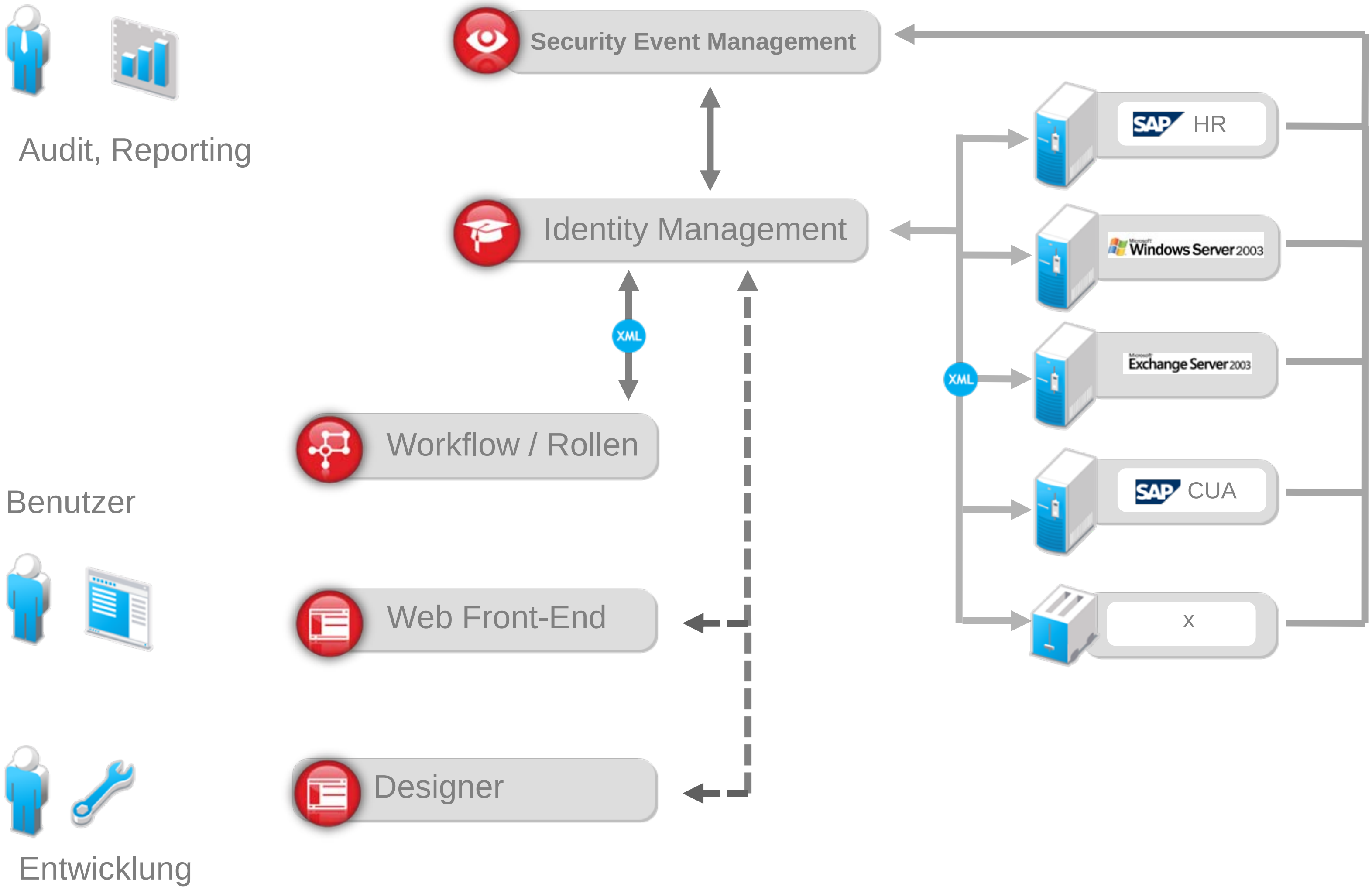
Compliance Management Models



Compliance Automation and Validation

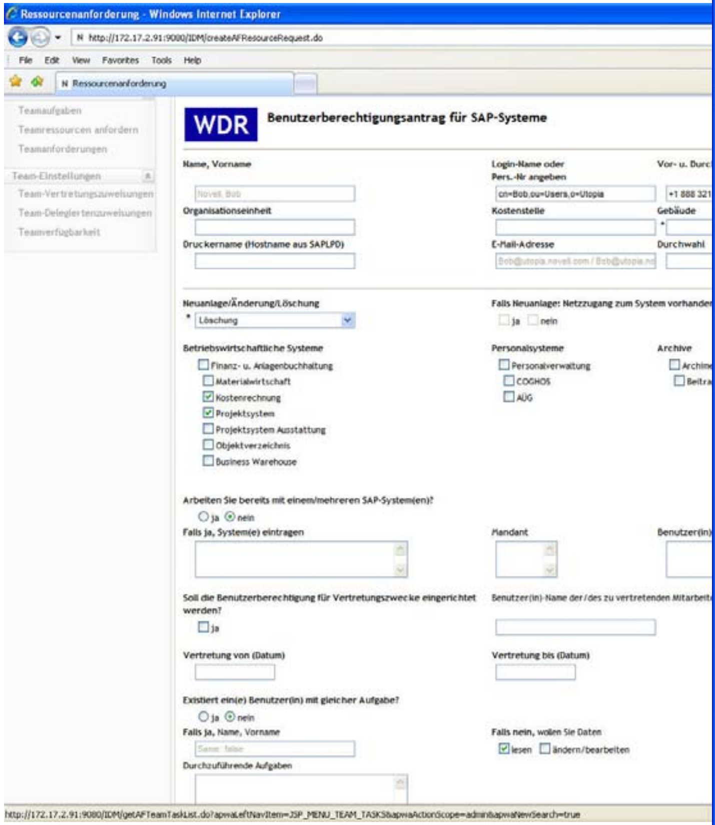


Compliance Management



Compliance Management

Workflows….


Ressourcenanforderung - Windows Internet Explorer
http://172.17.2.91:9080/IDM/createAFResourceRequest.do
File Edit View Favorites Tools Help
Ressourcenanforderung
Teamaufgaben
Teamressourcen anfordern
Teamanforderungen
Team-Einstellungen
Team-Vertretungszuweisungen
Team-Delegiertenzuweisungen
Teamverfügbarkeit

WDR Benutzerberechtigungsantrag für SAP-Systeme

Name, Vorname: Novell, Bob

Login-Name oder Pers.-Nr angeben: cn=Bob,ou=Users,o=Utopia

Vor- u. Durc[hwahl]: +1 888 321

Organisationseinheit

Kostenstelle

Gebäude *

Druckername (Hostname aus SAPLPD)

E-Mail-Adresse: Bob@utopia.novell.com / Bob@utopia.n

Durchwahl

Neuanlage/Änderung/Löschung: * Löschung

Falls Neuanlage: Netzzugang zum System vorhanden: □ ja □ nein

Betriebswirtschaftliche Systeme
- □ Finanz- u. Anlagenbuchhaltung
- □ Materialwirtschaft
- ☑ Kostenrechnung
- ☑ Projektsystem
- □ Projektsystem Ausstattung
- □ Objektverzeichnis
- □ Business Warehouse

Personalsysteme
- □ Personalverwaltung
- □ COGHOS
- □ AÜG

Archive
- □ Archime
- □ Beitra

Arbeiten Sie bereits mit einem/mehreren SAP-System(en)? ○ ja ● nein

Falls ja, System(e) eintragen

Mandant

Benutzer(in)

Soll die Benutzerberechtigung für Vertretungszwecke eingerichtet werden? □ ja

Benutzer(in)-Name der/des zu vertretenden Mitarbeit

Vertretung von (Datum)

Vertretung bis (Datum)

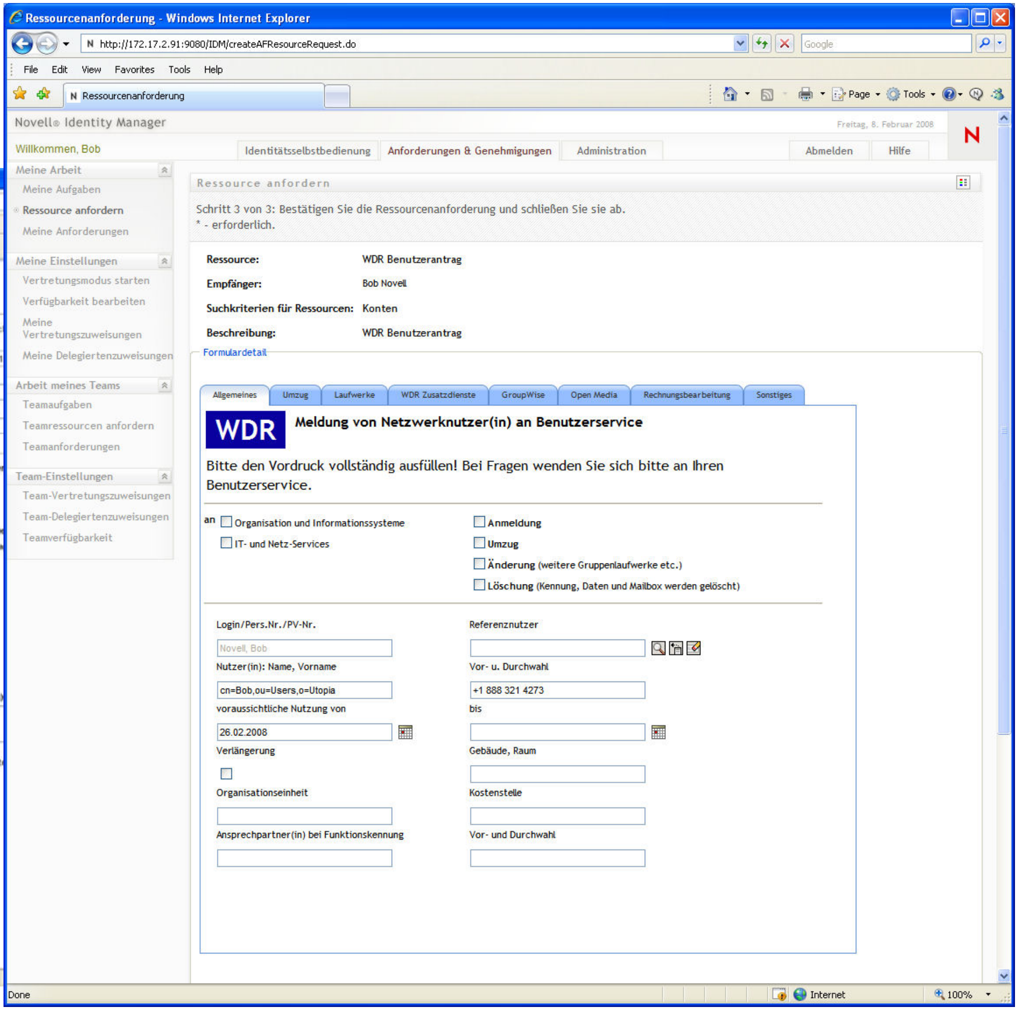
Existiert ein(e) Benutzer(in) mit gleicher Aufgabe? ○ ja ● nein

Falls ja, Name, Vorname: Same: false

Falls nein, wollen Sie Daten ☑ lesen □ ändern/bearbeiten

Durchzuführende Aufgaben

http://172.17.2.91:9080/IDM/getAFTeamTaskList.do?apwaLeftNavItem=JSP_MENU_TEAM_TASKS&apwaActionScope=admin&apwaNewSearch=true



Ressource anfordern

Schritt 3 von 3: Bestätigen Sie die Ressourcenanforderung und schließen Sie sie ab.
* - erforderlich.

Ressource:	WDR Benutzerantrag
Empfänger:	Bob Novell
Suchkriterien für Ressourcen:	Konten
Beschreibung:	WDR Benutzerantrag

Formulardetail

WDR Meldung von Netzwerknutzer(in) an Benutzerservice

Bitte den Vordruck vollständig ausfüllen! Bei Fragen wenden Sie sich bitte an Ihren Benutzerservice.

an □ Organisation und Informationssysteme
□ IT- und Netz-Services

□ Anmeldung
□ Umzug
□ Änderung (weitere Gruppenlaufwerke etc.)
□ Löschung (Kennung, Daten und Mailbox werden gelöscht)

Login/Pers.Nr./PV-Nr.: Novell, Bob

Referenznutzer

Nutzer(in): Name, Vorname: cn=Bob,ou=Users,o=Utopia

Vor- u. Durchwahl: +1 888 321 4273

voraussichtliche Nutzung von: 26.02.2008

bis

Verlängerung □

Gebäude, Raum

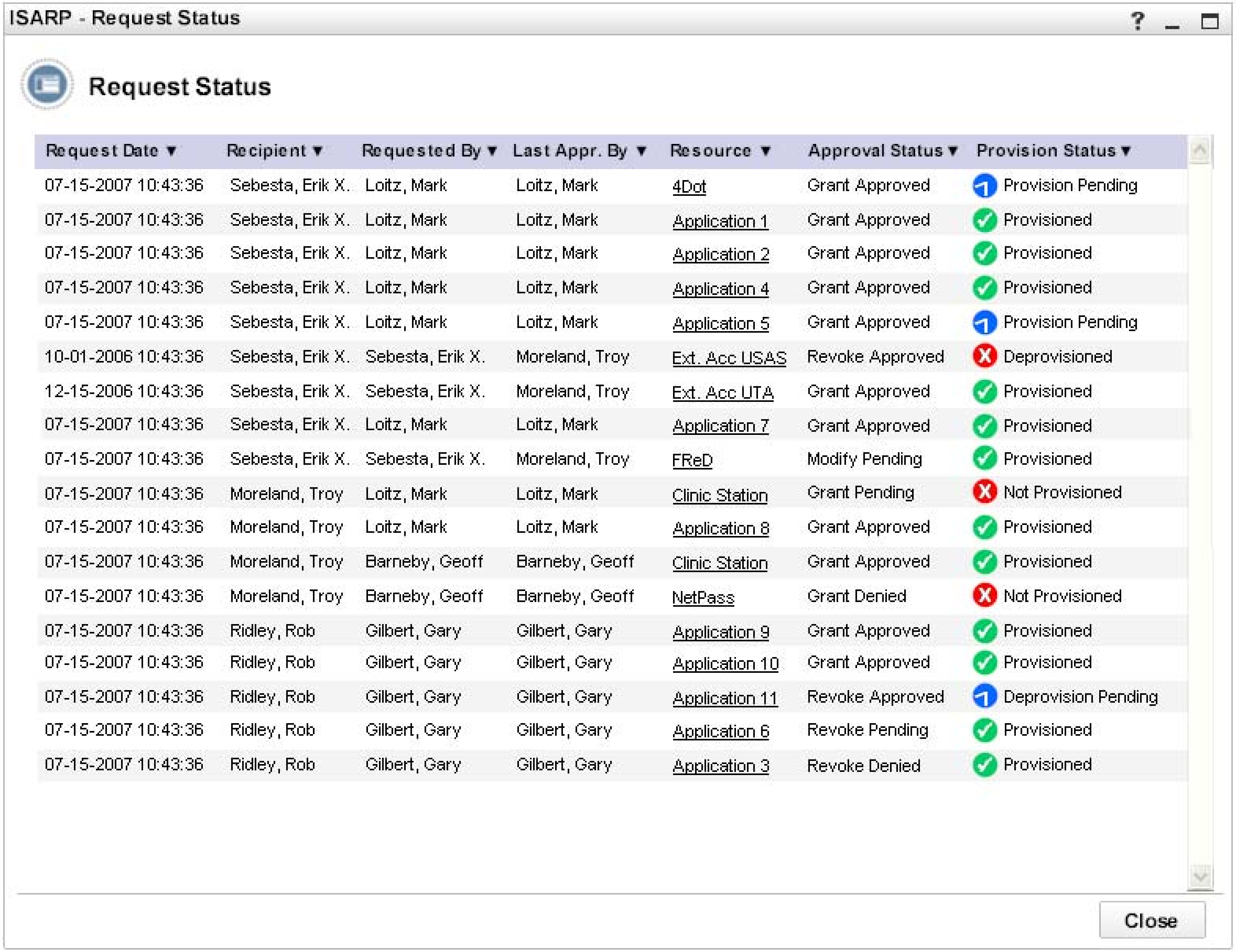
Organisationseinheit

Kostenstelle

Ansprechpartner(in) bei Funktionskennung

Vor- und Durchwahl

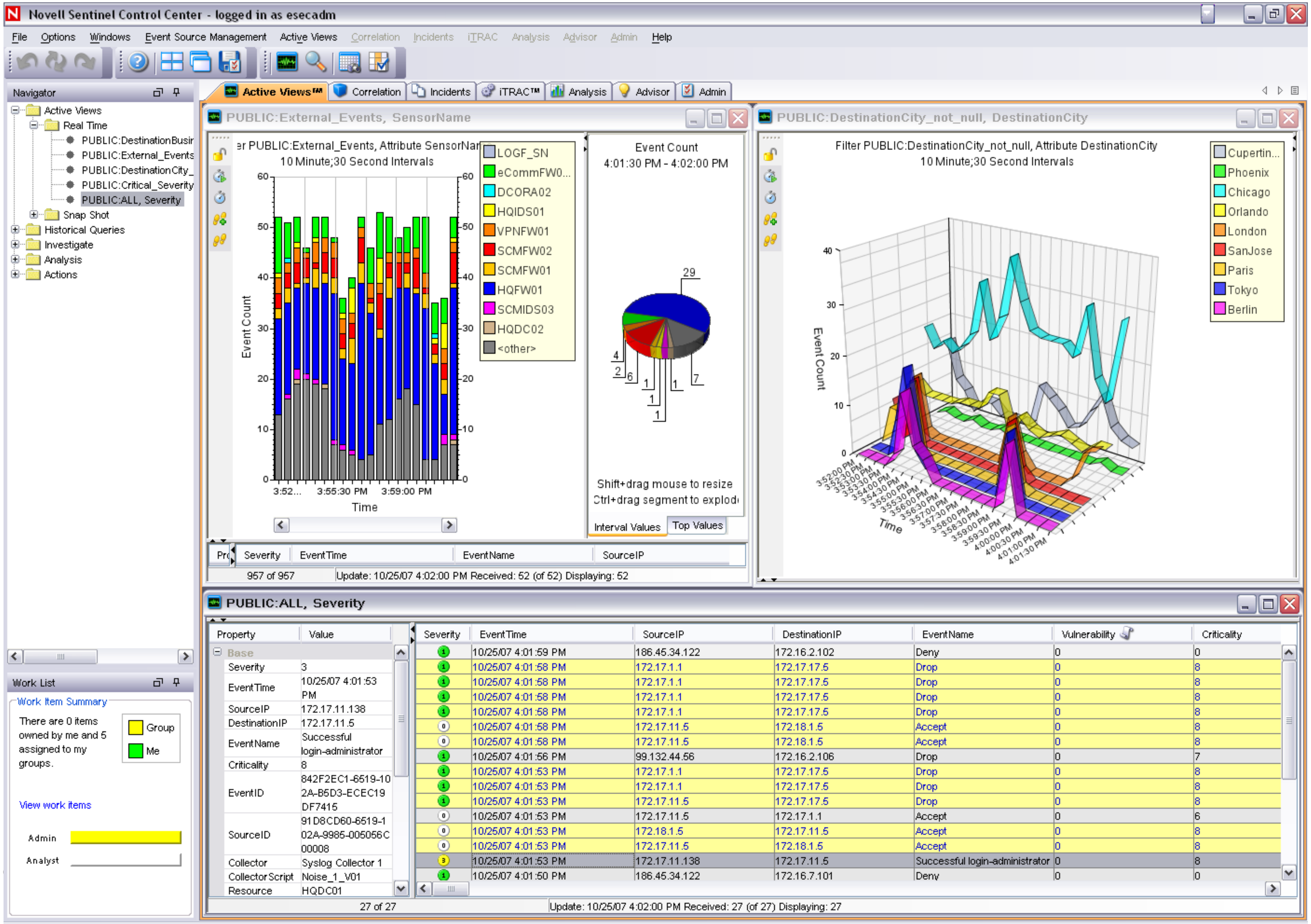
Audits and Dashboards



Request Status

Request Date ▼	Recipient ▼	Requested By ▼	Last Appr. By ▼	Resource ▼	Approval Status ▼	Provision Status ▼
07-15-2007 10:43:36	Sebesta, Erik X.	Loitz, Mark	Loitz, Mark	4Dot	Grant Approved	Provision Pending
07-15-2007 10:43:36	Sebesta, Erik X.	Loitz, Mark	Loitz, Mark	Application 1	Grant Approved	Provisioned
07-15-2007 10:43:36	Sebesta, Erik X.	Loitz, Mark	Loitz, Mark	Application 2	Grant Approved	Provisioned
07-15-2007 10:43:36	Sebesta, Erik X.	Loitz, Mark	Loitz, Mark	Application 4	Grant Approved	Provisioned
07-15-2007 10:43:36	Sebesta, Erik X.	Loitz, Mark	Loitz, Mark	Application 5	Grant Approved	Provision Pending
10-01-2006 10:43:36	Sebesta, Erik X.	Sebesta, Erik X.	Moreland, Troy	Ext. Acc USAS	Revoke Approved	Deprovisioned
12-15-2006 10:43:36	Sebesta, Erik X.	Sebesta, Erik X.	Moreland, Troy	Ext. Acc UTA	Grant Approved	Provisioned
07-15-2007 10:43:36	Sebesta, Erik X.	Loitz, Mark	Loitz, Mark	Application 7	Grant Approved	Provisioned
07-15-2007 10:43:36	Sebesta, Erik X.	Sebesta, Erik X.	Moreland, Troy	FReD	Modify Pending	Provisioned
07-15-2007 10:43:36	Moreland, Troy	Loitz, Mark	Loitz, Mark	Clinic Station	Grant Pending	Not Provisioned
07-15-2007 10:43:36	Moreland, Troy	Loitz, Mark	Loitz, Mark	Application 8	Grant Approved	Provisioned
07-15-2007 10:43:36	Moreland, Troy	Barneby, Geoff	Barneby, Geoff	Clinic Station	Grant Approved	Provisioned
07-15-2007 10:43:36	Moreland, Troy	Barneby, Geoff	Barneby, Geoff	NetPass	Grant Denied	Not Provisioned
07-15-2007 10:43:36	Ridley, Rob	Gilbert, Gary	Gilbert, Gary	Application 9	Grant Approved	Provisioned
07-15-2007 10:43:36	Ridley, Rob	Gilbert, Gary	Gilbert, Gary	Application 10	Grant Approved	Provisioned
07-15-2007 10:43:36	Ridley, Rob	Gilbert, Gary	Gilbert, Gary	Application 11	Revoke Approved	Deprovision Pending
07-15-2007 10:43:36	Ridley, Rob	Gilbert, Gary	Gilbert, Gary	Application 6	Revoke Pending	Provisioned
07-15-2007 10:43:36	Ridley, Rob	Gilbert, Gary	Gilbert, Gary	Application 3	Revoke Denied	Provisioned

Audits and Dashboards



Pri	Severity	EventTime	EventName	SourceIP

957 of 957 Update: 10/25/07 4:02:00 PM Received: 52 (of 52) Displaying: 52

Work Item Summary

There are 0 items owned by me and 5 assigned to my groups.

View work items

PUBLIC:ALL, Severity

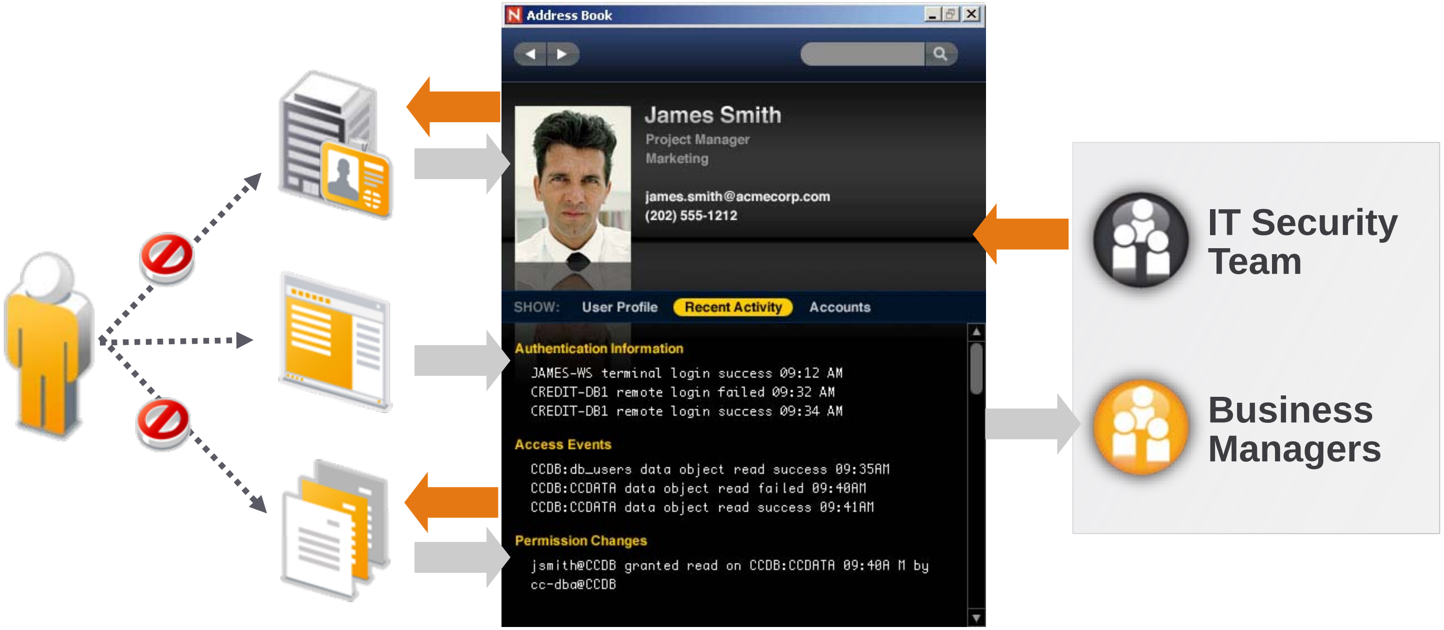
Property	Value
Base	
Severity	3
EventTime	10/25/07 4:01:53 PM
SourceIP	172.17.11.138
DestinationIP	172.17.11.5
EventName	Successful login-administrator
Criticality	8
EventID	842F2EC1-6519-102A-B5D3-ECEC19DF7415
SourceID	91D8CD60-6519-102A-9985-005056C00008
Collector	Syslog Collector 1
CollectorScript	Noise_1_V01
Resource	HQDC01

27 of 27

Severity	EventTime	SourceIP	DestinationIP	EventName	Vulnerability	Criticality
1	10/25/07 4:01:59 PM	186.45.34.122	172.16.2.102	Deny	0	0
1	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
1	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
1	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
1	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
0	10/25/07 4:01:58 PM	172.17.11.5	172.18.1.5	Accept	0	8
0	10/25/07 4:01:58 PM	172.17.11.5	172.18.1.5	Accept	0	8
1	10/25/07 4:01:56 PM	99.132.44.56	172.16.2.106	Drop	0	7
1	10/25/07 4:01:53 PM	172.17.1.1	172.17.17.5	Drop	0	8
1	10/25/07 4:01:53 PM	172.17.1.1	172.17.17.5	Drop	0	8
1	10/25/07 4:01:53 PM	172.17.11.5	172.17.17.5	Drop	0	8
0	10/25/07 4:01:53 PM	172.17.11.5	172.17.1.1	Accept	0	6
0	10/25/07 4:01:53 PM	172.18.1.5	172.17.11.5	Accept	0	8
0	10/25/07 4:01:53 PM	172.17.11.5	172.18.1.5	Accept	0	8
3	10/25/07 4:01:53 PM	172.17.11.138	172.17.11.5	Successful login-administrator	0	8
1	10/25/07 4:01:50 PM	186.45.34.122	172.16.7.101	Deny	0	0

Update: 10/25/07 4:02:00 PM Received: 27 (of 27) Displaying: 27

Security and Vulnerability Management



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
```

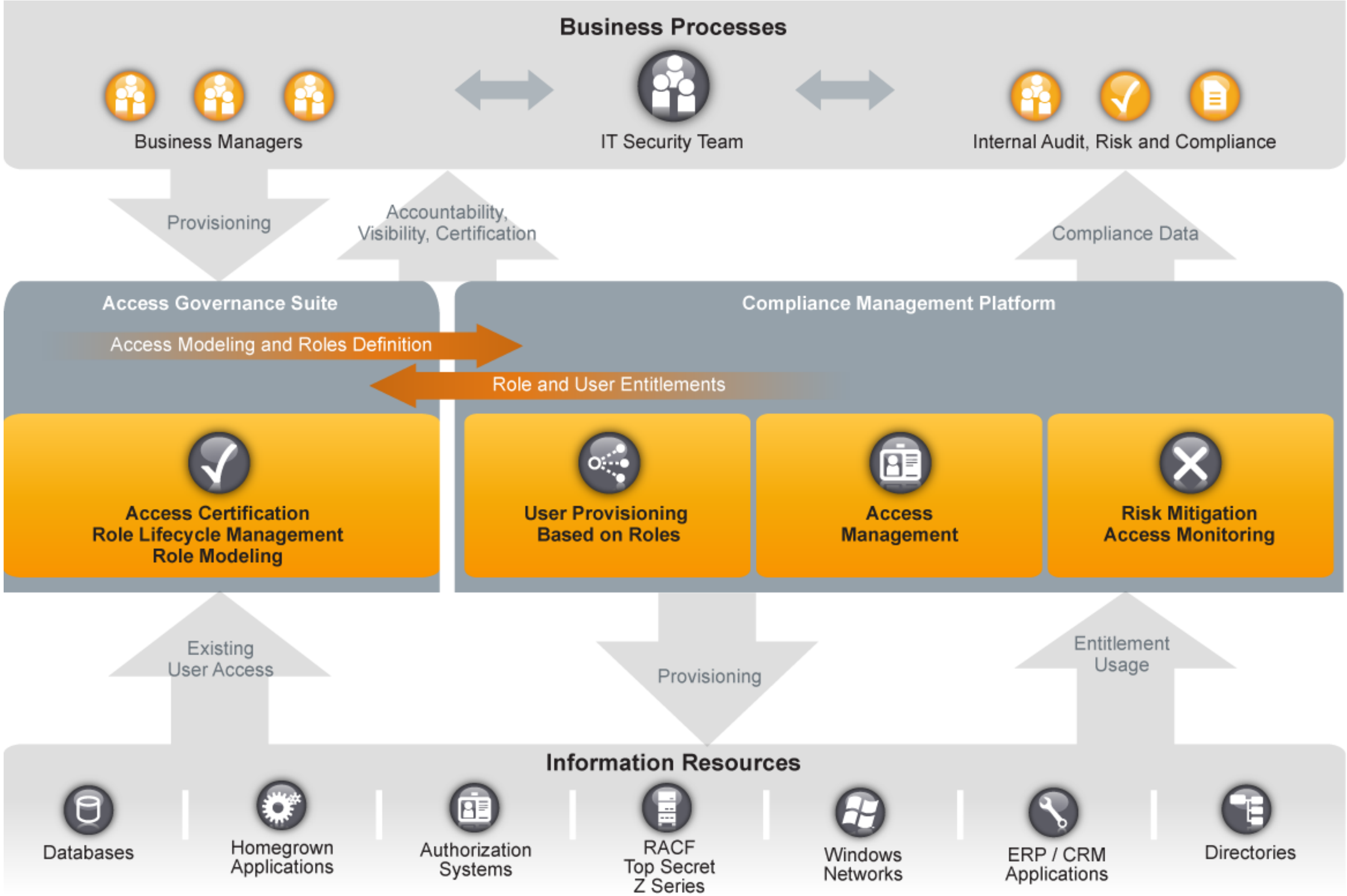
Permission Changes

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

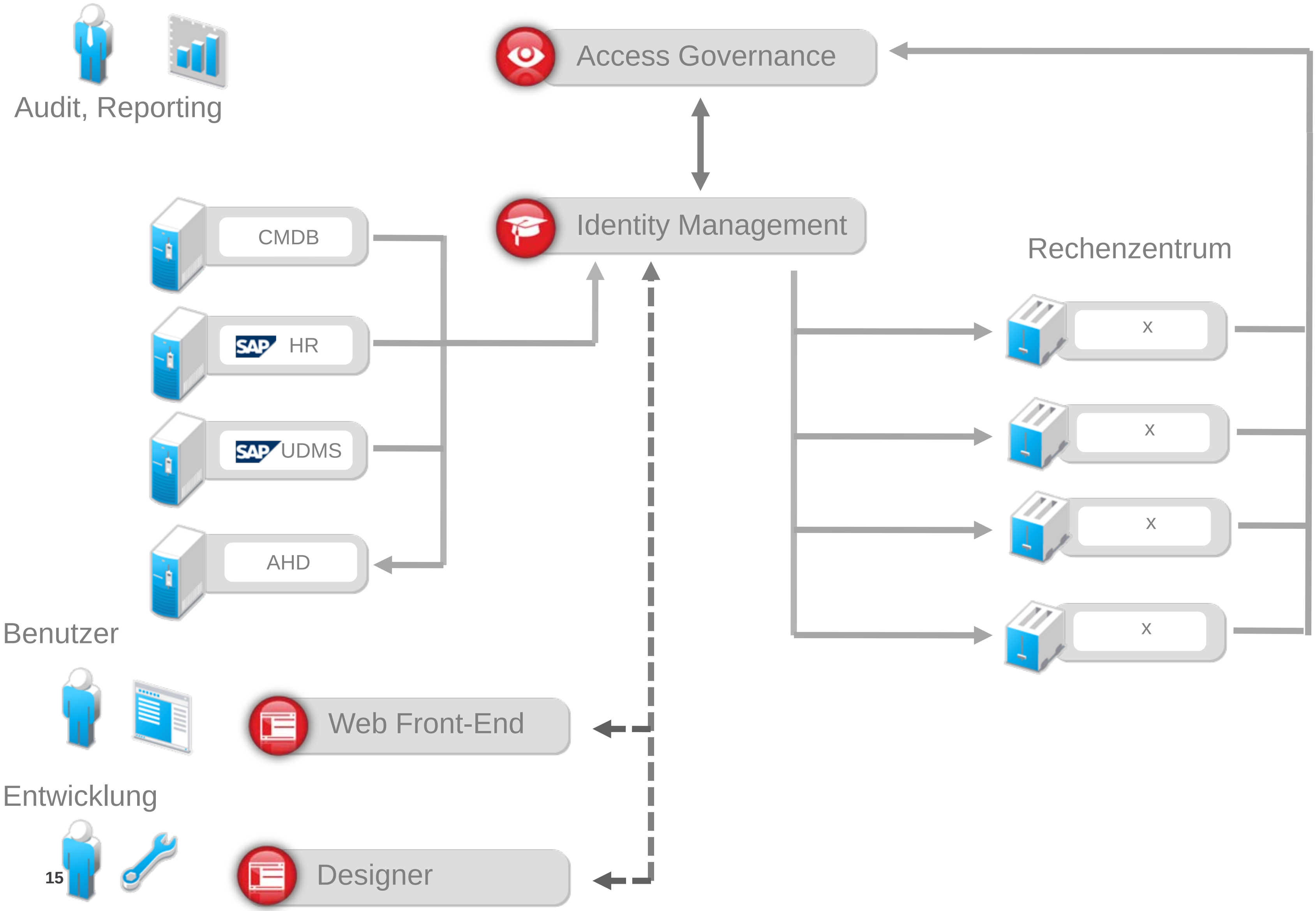
IT Security Team

Business Managers

Access Governance

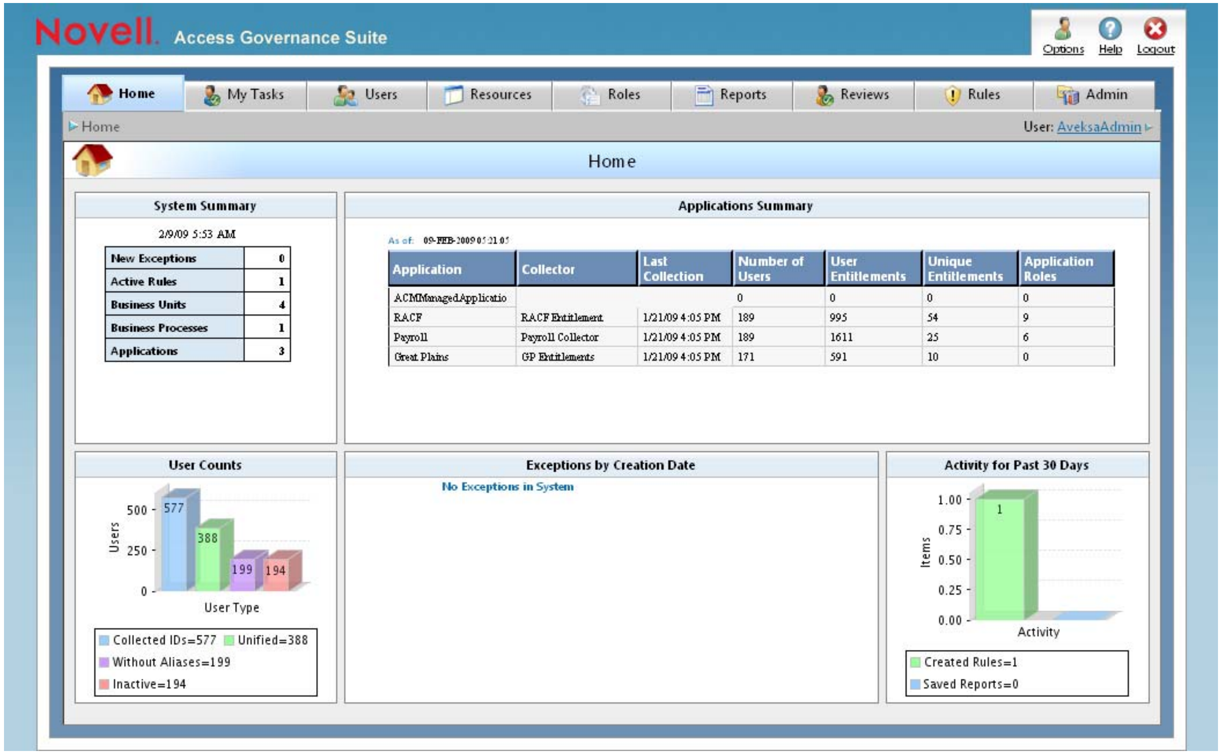


Access Governance



Access Governance

- Automates the processes of mining and managing roles
- Delivers visibility, simplicity and accuracy to the complex process of defining and managing user access



System Summary

2/9/09 5:53 AM

New Exceptions	0
Active Rules	1
Business Units	4
Business Processes	1
Applications	3

Applications Summary

As of: 09-FEB-2009 05:21:05

Application	Collector	Last Collection	Number of Users	User Entitlements	Unique Entitlements	Application Roles
ACMManagedApplicatio			0	0	0	0
RACF	RACF Entitlement	1/21/09 4:05 PM	189	995	54	9
Payroll	Payroll Collector	1/21/09 4:05 PM	189	1611	25	6
Great Plains	GP Entitlements	1/21/09 4:05 PM	171	591	10	0

User Counts

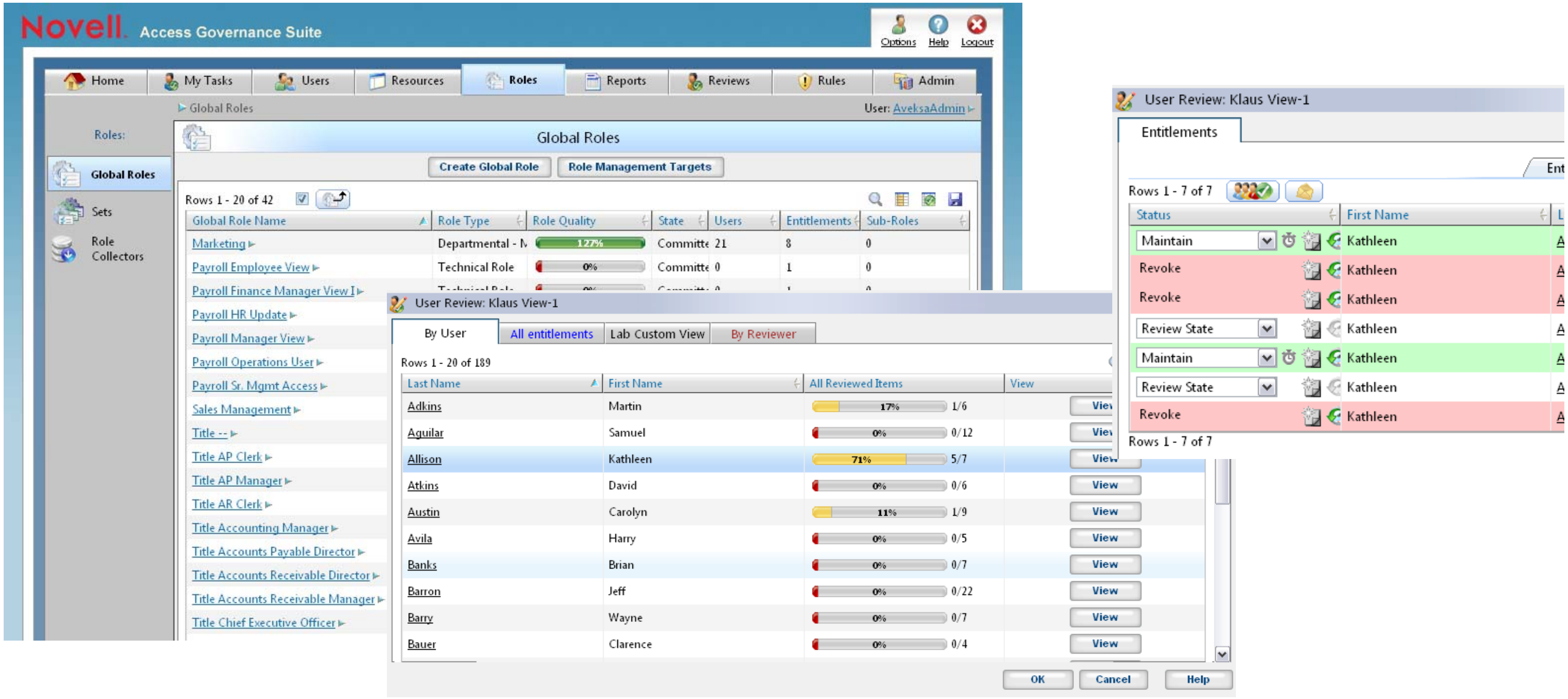
Exceptions by Creation Date

No Exceptions in System

Activity for Past 30 Days

Access Governance

- Enable business managers and application owners to be accountable for meeting the company's compliance requirements.



Global Roles

Rows 1 - 20 of 42

Global Role Name	Role Type	Role Quality	State	Users	Entitlements	Sub-Roles
Marketing	Departmental - N	127%	Committe	21	8	0
Payroll Employee View	Technical Role	0%	Committe	0	1	0
Payroll Finance Manager View I	Technical Role	0%	Committe	0	1	0
Payroll HR Update						
Payroll Manager View						
Payroll Operations User						
Payroll Sr. Mgmt Access						
Sales Management						
Title --						
Title AP Clerk						
Title AP Manager						
Title AR Clerk						
Title Accounting Manager						
Title Accounts Payable Director						
Title Accounts Receivable Director						
Title Accounts Receivable Manager						
Title Chief Executive Officer						

User Review: Klaus View-1

By User | All entitlements | Lab Custom View | By Reviewer

Rows 1 - 20 of 189

Last Name	First Name	All Reviewed Items		View
Adkins	Martin	17%	1/6	View
Aguilar	Samuel	0%	0/12	View
Allison	Kathleen	71%	5/7	View
Atkins	David	0%	0/6	View
Austin	Carolyn	11%	1/9	View
Avila	Harry	0%	0/5	View
Banks	Brian	0%	0/7	View
Barron	Jeff	0%	0/22	View
Barry	Wayne	0%	0/7	View
Bauer	Clarence	0%	0/4	View

User Review: Klaus View-1

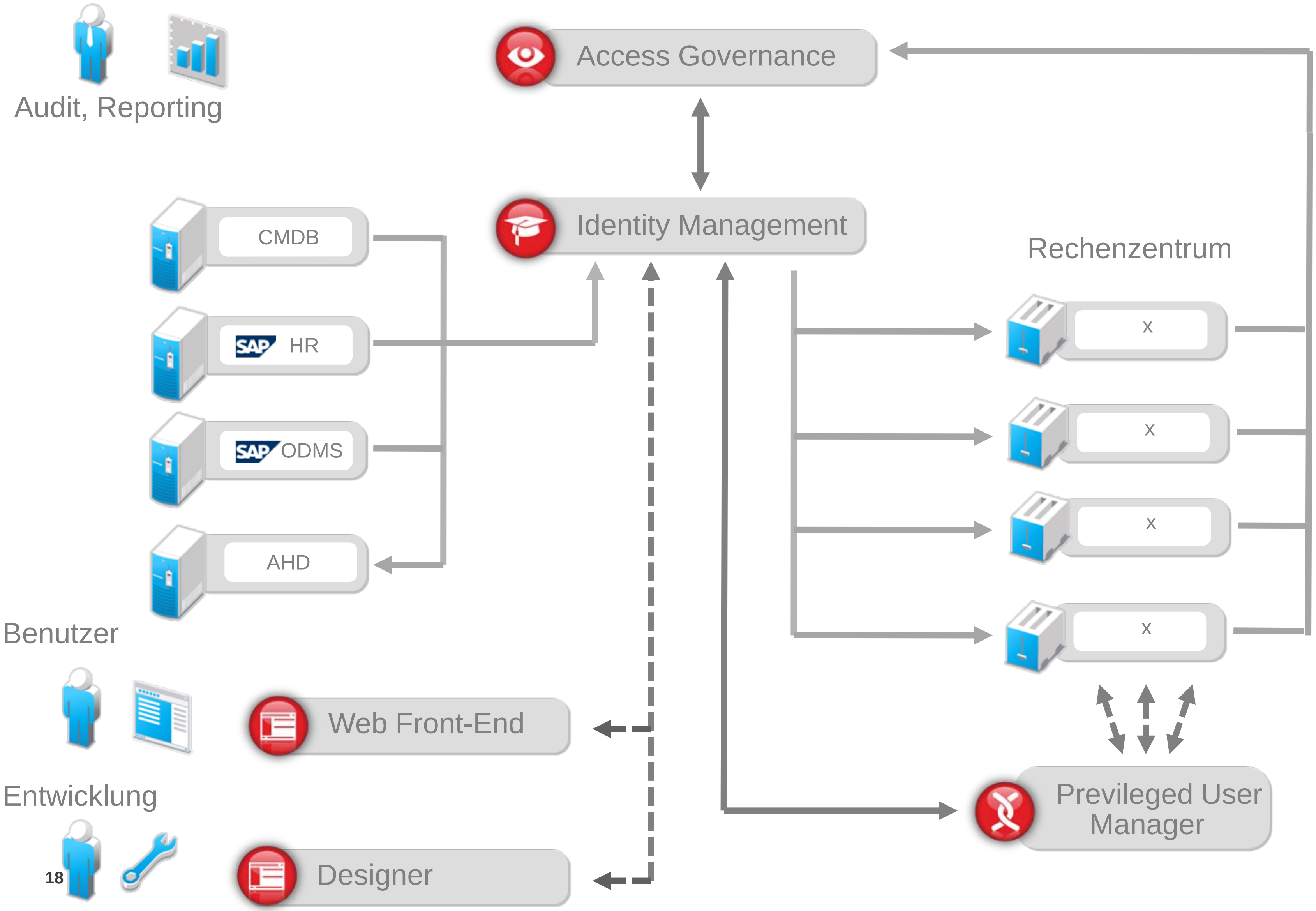
Entitlements

Rows 1 - 7 of 7

Status	First Name	L
Maintain	Kathleen	A
Revoke	Kathleen	A
Revoke	Kathleen	A
Review State	Kathleen	A
Maintain	Kathleen	A
Review State	Kathleen	A
Revoke	Kathleen	A

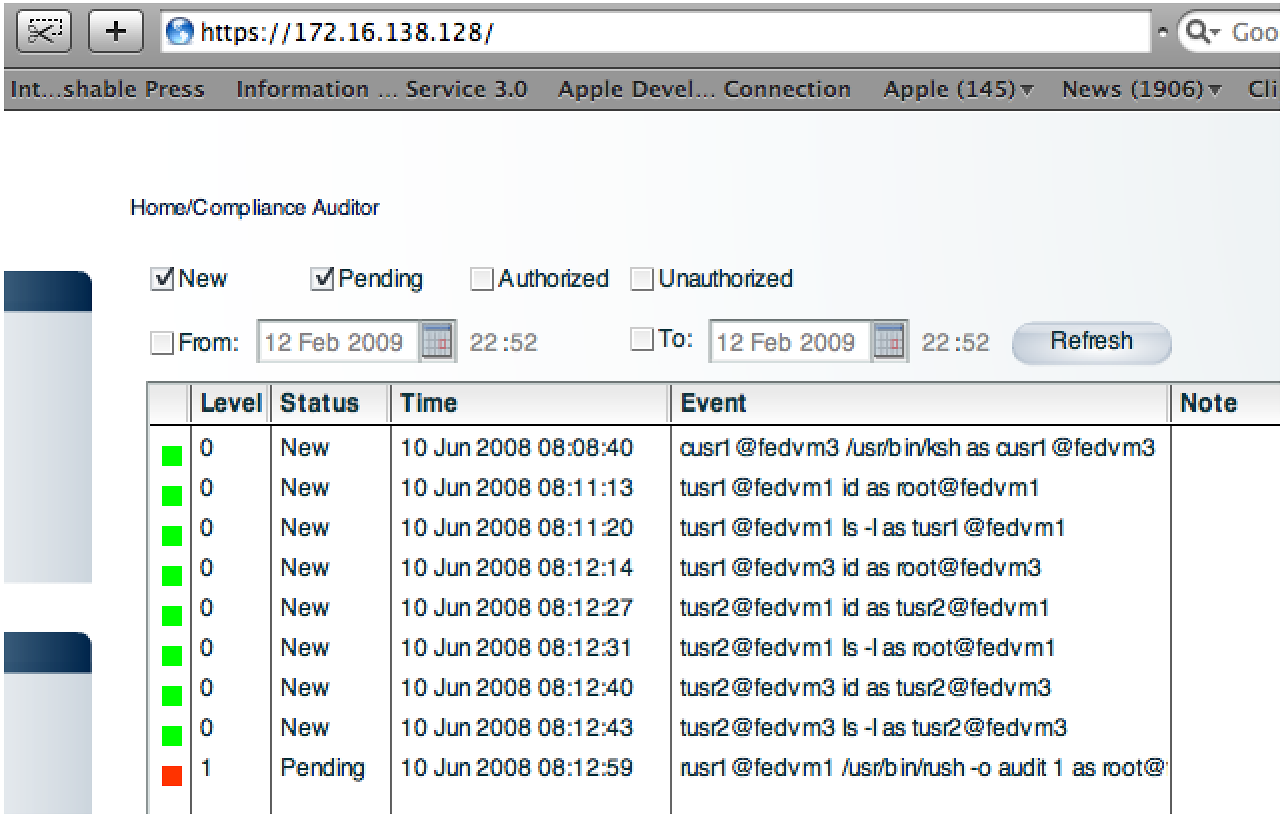
Rows 1 - 7 of 7

Access Governance



Privileged User Management

- Deliver Superuser Privilege Management for all UNIX/Linux



Home/Compliance Auditor

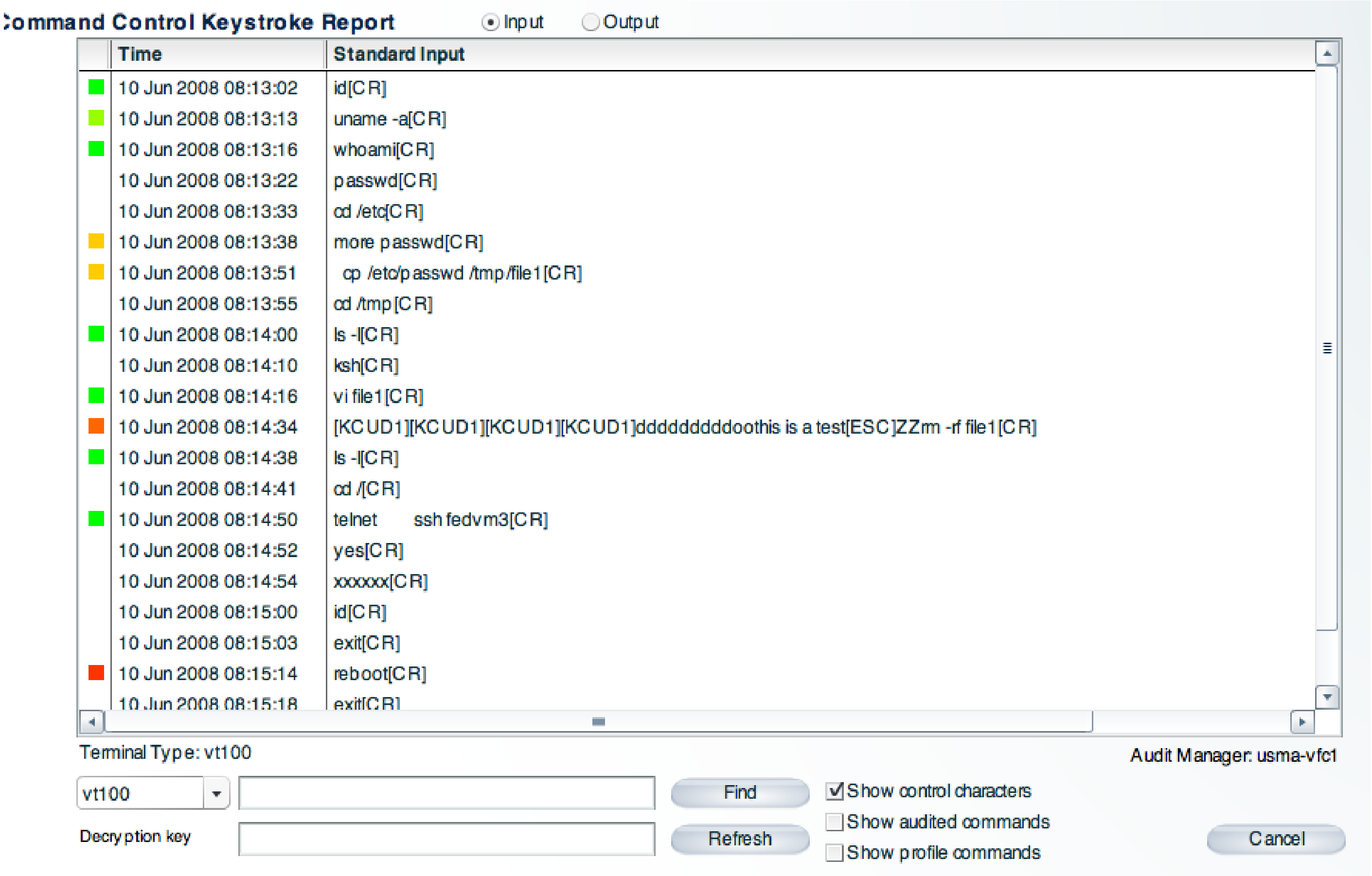
☑ New ☑ Pending □ Authorized □ Unauthorized

□ From: 12 Feb 2009 22 :52 □ To: 12 Feb 2009 22 :52

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

Privileged User Management

- Control and Record “Which Privileged Users Have Access to What”



Command Control Keystroke Report ● Input ○ Output

	Time	Standard Input
🟩	10 Jun 2008 08:13:02	id[CR]
🟩	10 Jun 2008 08:13:13	uname -a[CR]
🟩	10 Jun 2008 08:13:16	whoami[CR]
	10 Jun 2008 08:13:22	passwd[CR]
	10 Jun 2008 08:13:33	cd /etc[CR]
🟨	10 Jun 2008 08:13:38	more passwd[CR]
🟨	10 Jun 2008 08:13:51	cp /etc/passwd /tmp/file1[CR]
	10 Jun 2008 08:13:55	cd /tmp[CR]
🟩	10 Jun 2008 08:14:00	ls -l[CR]
	10 Jun 2008 08:14:10	ksh[CR]
🟩	10 Jun 2008 08:14:16	vi file1[CR]
🟧	10 Jun 2008 08:14:34	[KCUD1][KCUD1][KCUD1][KCUD1]dddddddddoothis is a test[ESC]ZZrm -rf file1[CR]
🟩	10 Jun 2008 08:14:38	ls -l[CR]
	10 Jun 2008 08:14:41	cd /[CR]
🟩	10 Jun 2008 08:14:50	telnet ssh fedvm3[CR]
	10 Jun 2008 08:14:52	yes[CR]
	10 Jun 2008 08:14:54	xxxxxx[CR]
	10 Jun 2008 08:15:00	id[CR]
	10 Jun 2008 08:15:03	exit[CR]
🟥	10 Jun 2008 08:15:14	reboot[CR]
	10 Jun 2008 08:15:18	exit[CR]

Terminal Type: vt100

Audit Manager: usma-vfc1

vt100

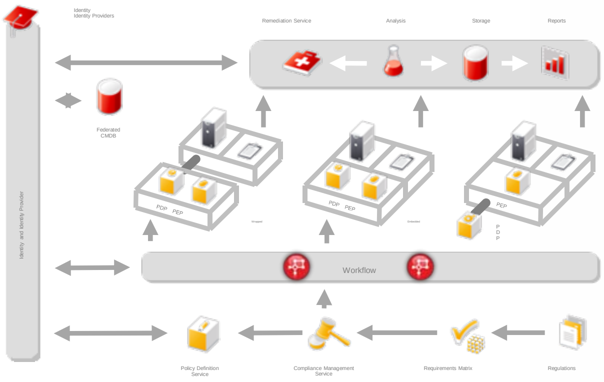
Decryption key

☑ Show control characters

☐ Show audited commands

☐ Show profile commands

Questions?


Identity
Identity Providers
Remediation Service
Analysis
Storage
Reports
Federated CMDB
PDP PEP
Wrapped
PDP PEP
Embedded
PEP
PDP
Workflow
Identity and Identity Provider
Policy Definition Service
Compliance Management Service
Requirements Matrix
Regulations

Novell®

- General Disclaimer

- This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.