COMVERSE
UNIVERSITY

Unified Platform Manager (UPM) Security

Lesson Objectives

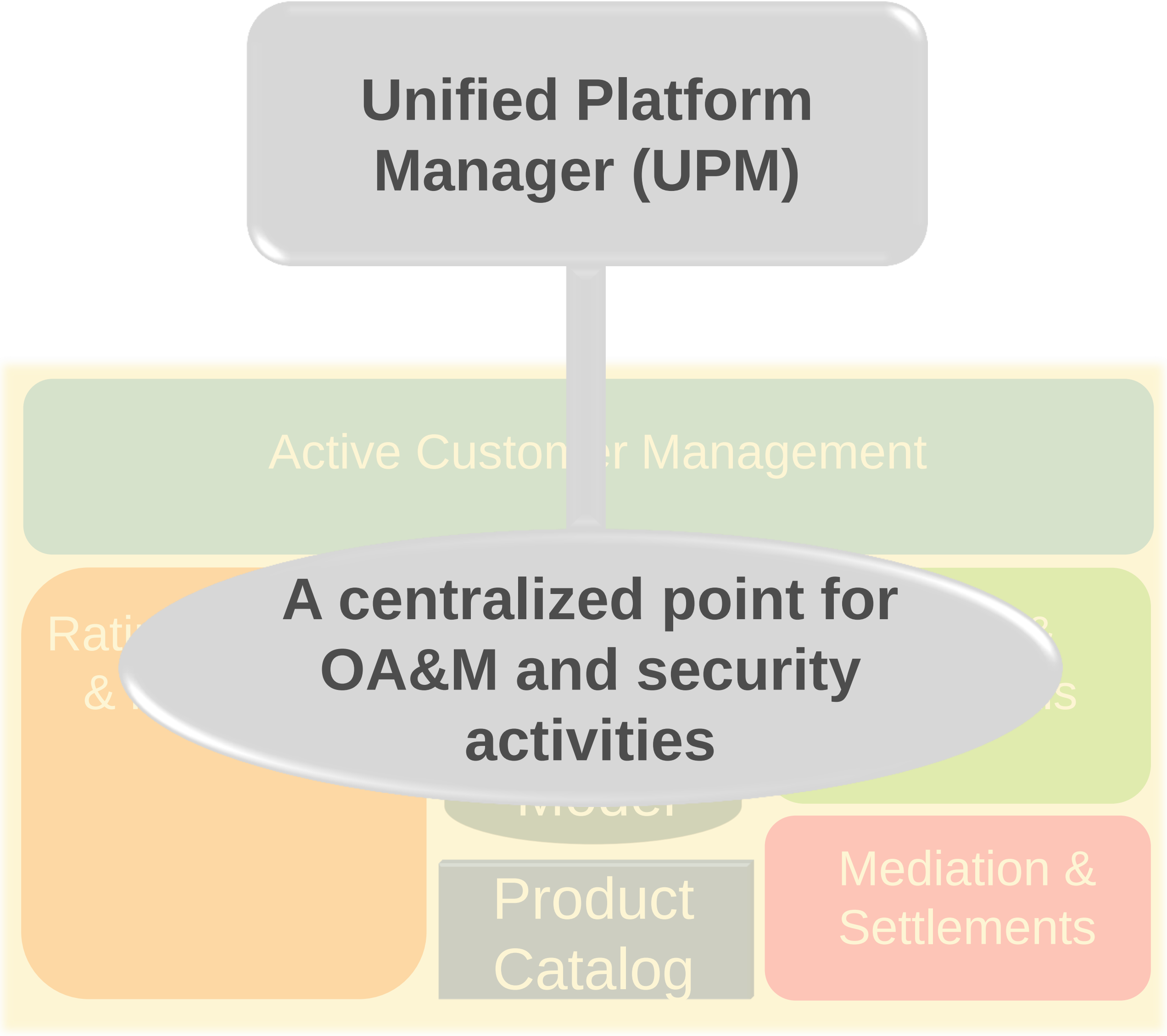
By the end of this lesson you will be able to describe the security capabilities of the UPM:

- Identity management
- Policy management
- Auditing
- Credentials
- Encryption keys

Agenda

- The Unified Platform
- Security Overview
- Using the Unified Platform Manager
- Identity Management
- Policy Management
- Key and Credential Management
- Accounting and Audit

What Is the Unified Platform Manager (UPM)?



Unified Platform Manager (UPM)

Active Custon er Management

Rati &

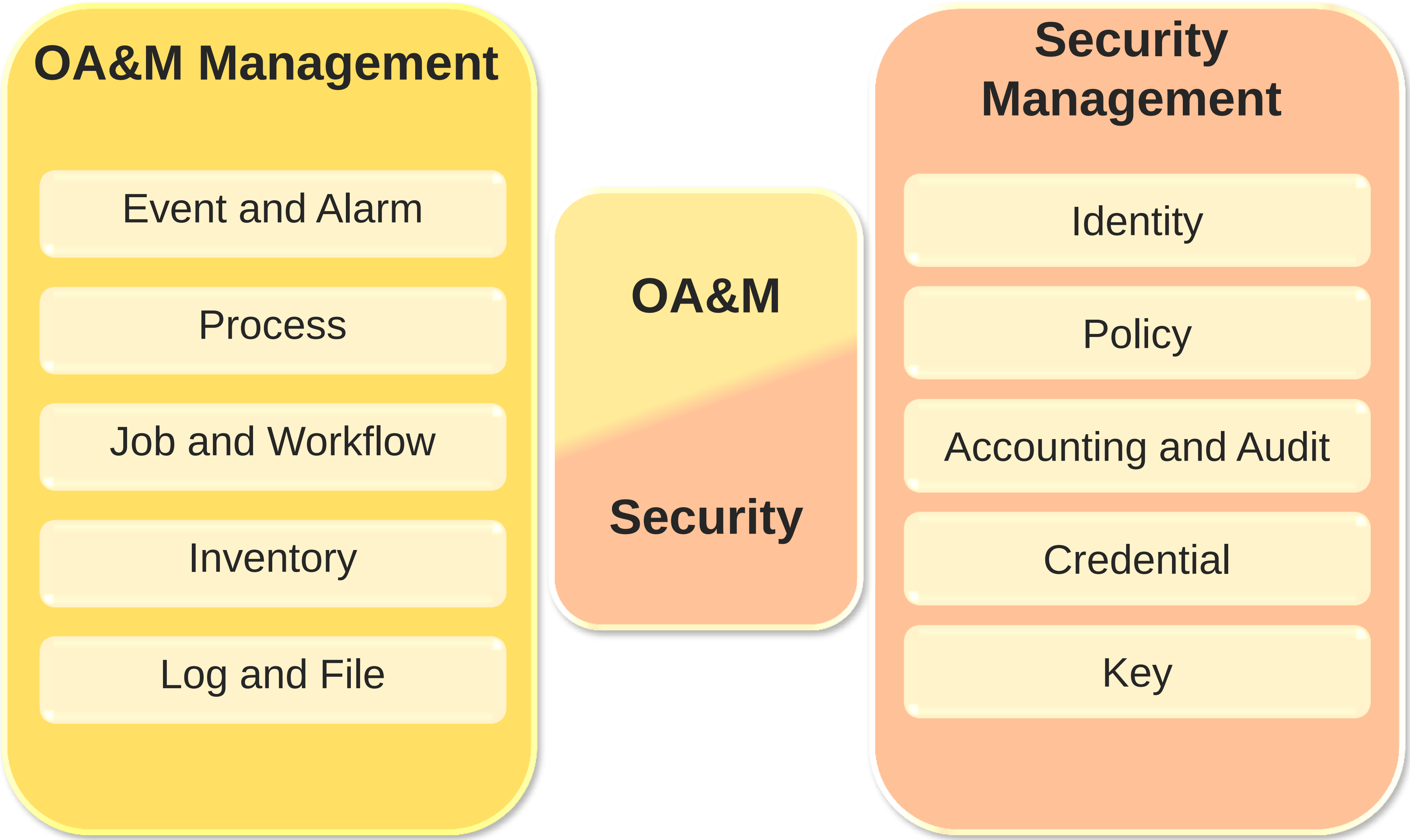
Model

Product Catalog

Mediation & Settlements

A centralized point for OA&M and security activities

Security Management



OA&M Management

- Event and Alarm
- Process
- Job and Workflow
- Inventory
- Log and File

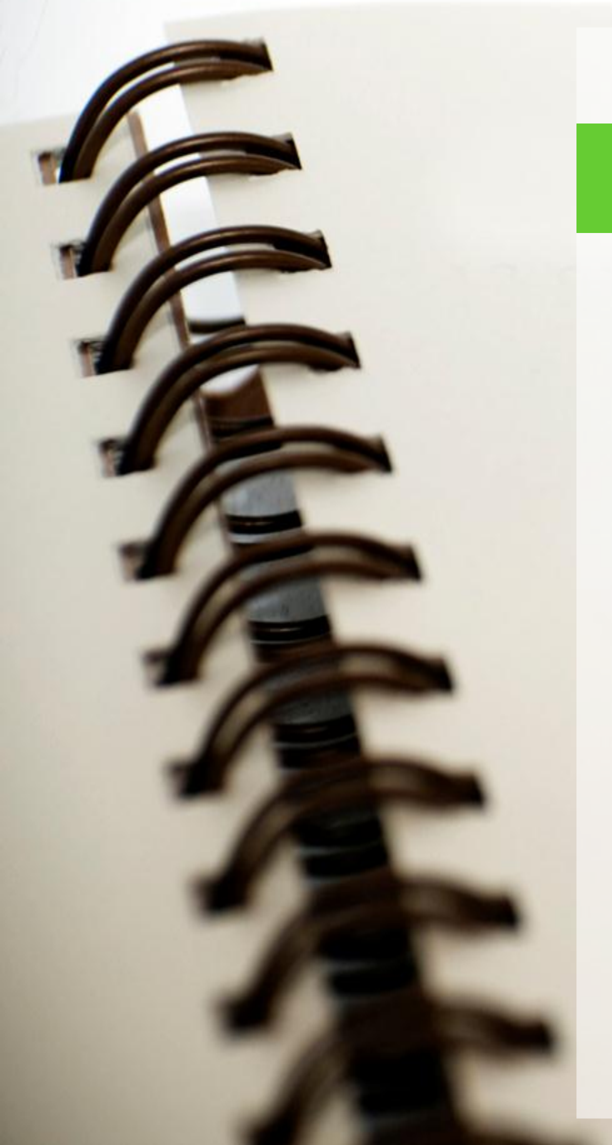
OA&M

Security

Security Management

- Identity
- Policy
- Accounting and Audit
- Credential
- Key

Agenda



The Unified Platform

Security Overview

Using the Unified Platform Manager

Identity Management

Policy Management

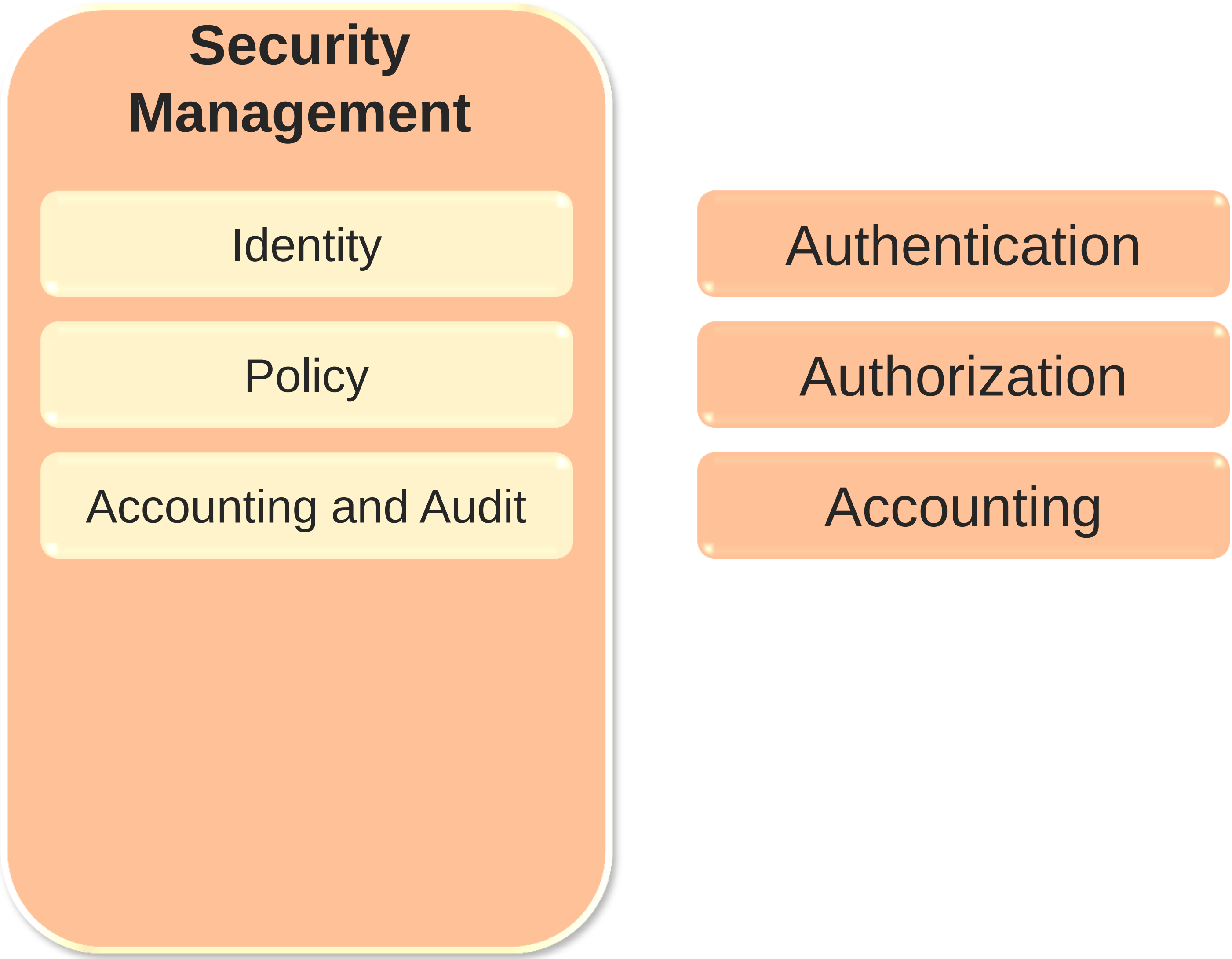
Key and Credential Management

Accounting and Audit

Security Functionalities

Authentication	Identifies the user, through login and password security credentials
Authorization	Grant access to authenticated users
Accounting	Tracks the activities of users

Security Management Functional Areas



Security Management

Identity

Policy

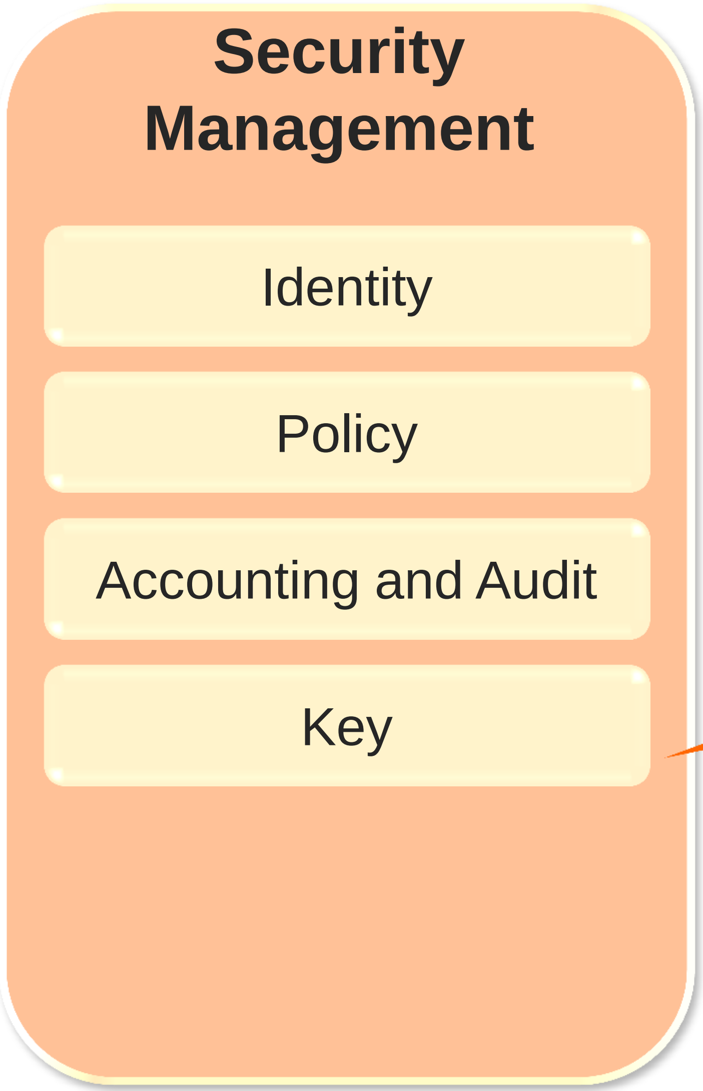
Accounting and Audit

Authentication

Authorization

Accounting

Data Encryption and Credentials Management



Security Management

Identity

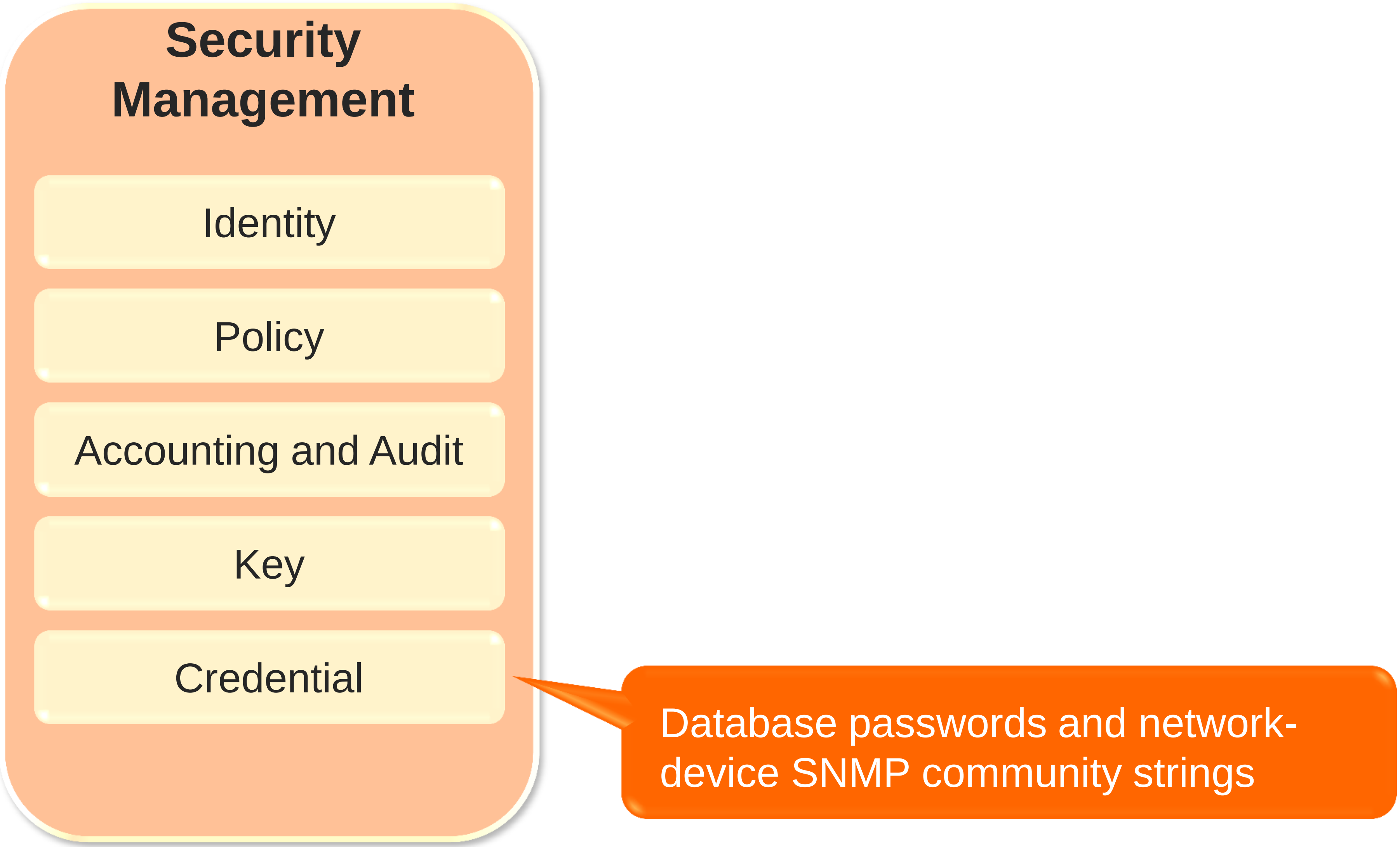
Policy

Accounting and Audit

Key

Encryption keys for data encryption
For example – encryption for credit card information

Data Encryption and Credentials Management



Security Management

Identity

Policy

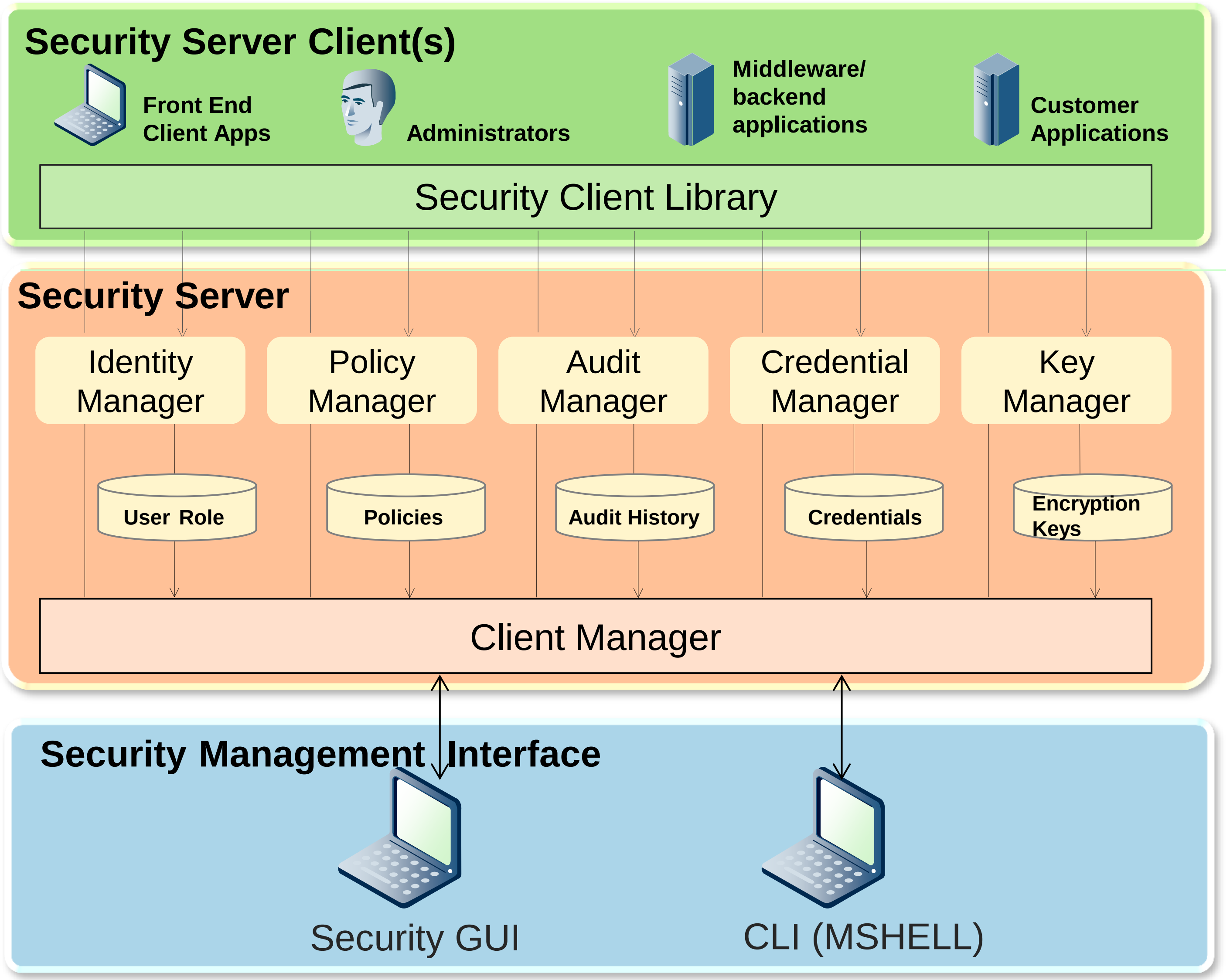
Accounting and Audit

Key

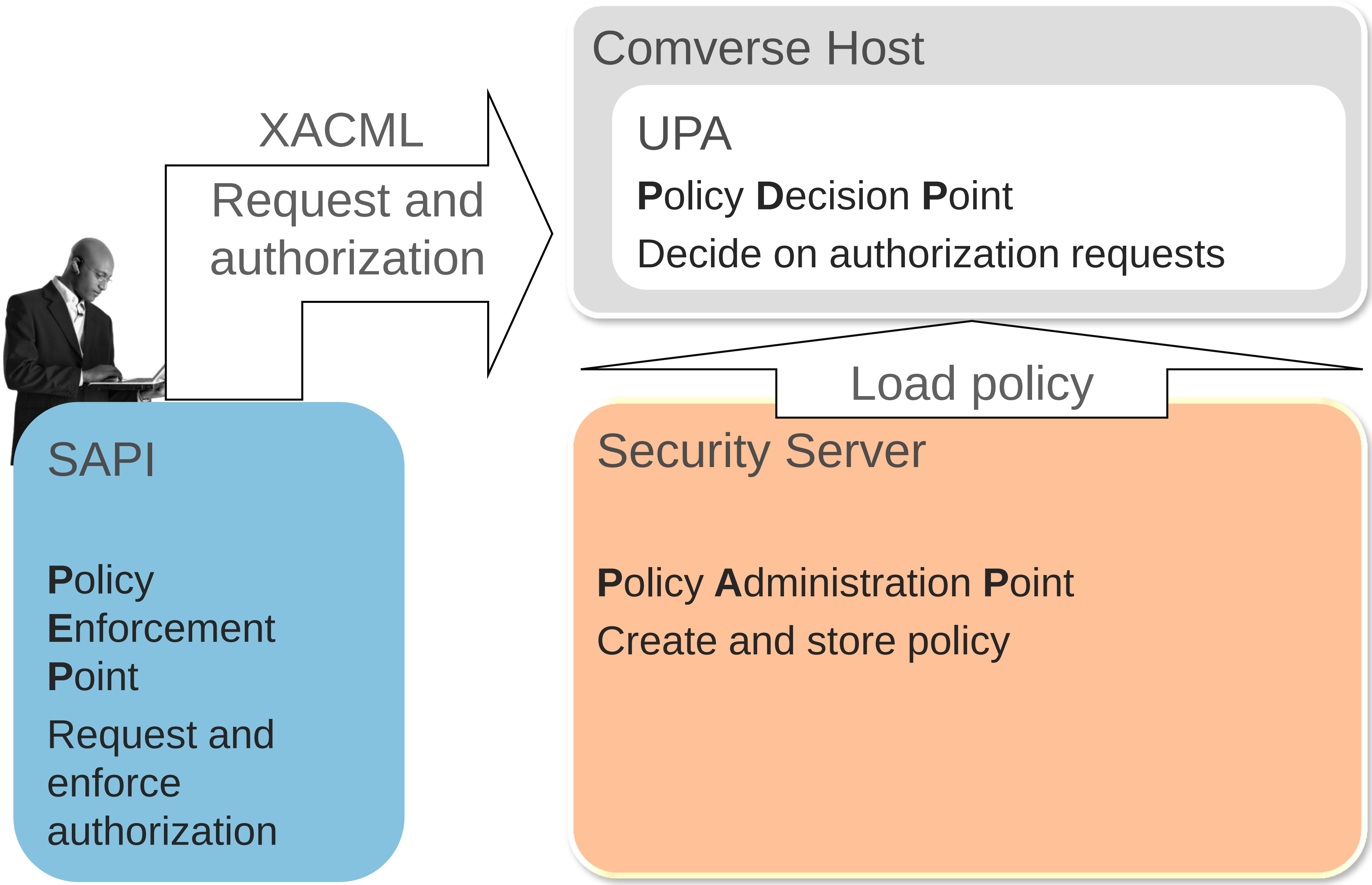
Credential

Database passwords and network-device SNMP community strings

Comverse ONE – Security Architecture



Organization for the Advancement of Structured Information Standards (OASIS) - Security Points



XACML

Request and authorization

Comverse Host

UPA

Policy **D**ecision **P**oint

Decide on authorization requests

Load policy

SAPI

Policy **E**nforcement **P**oint

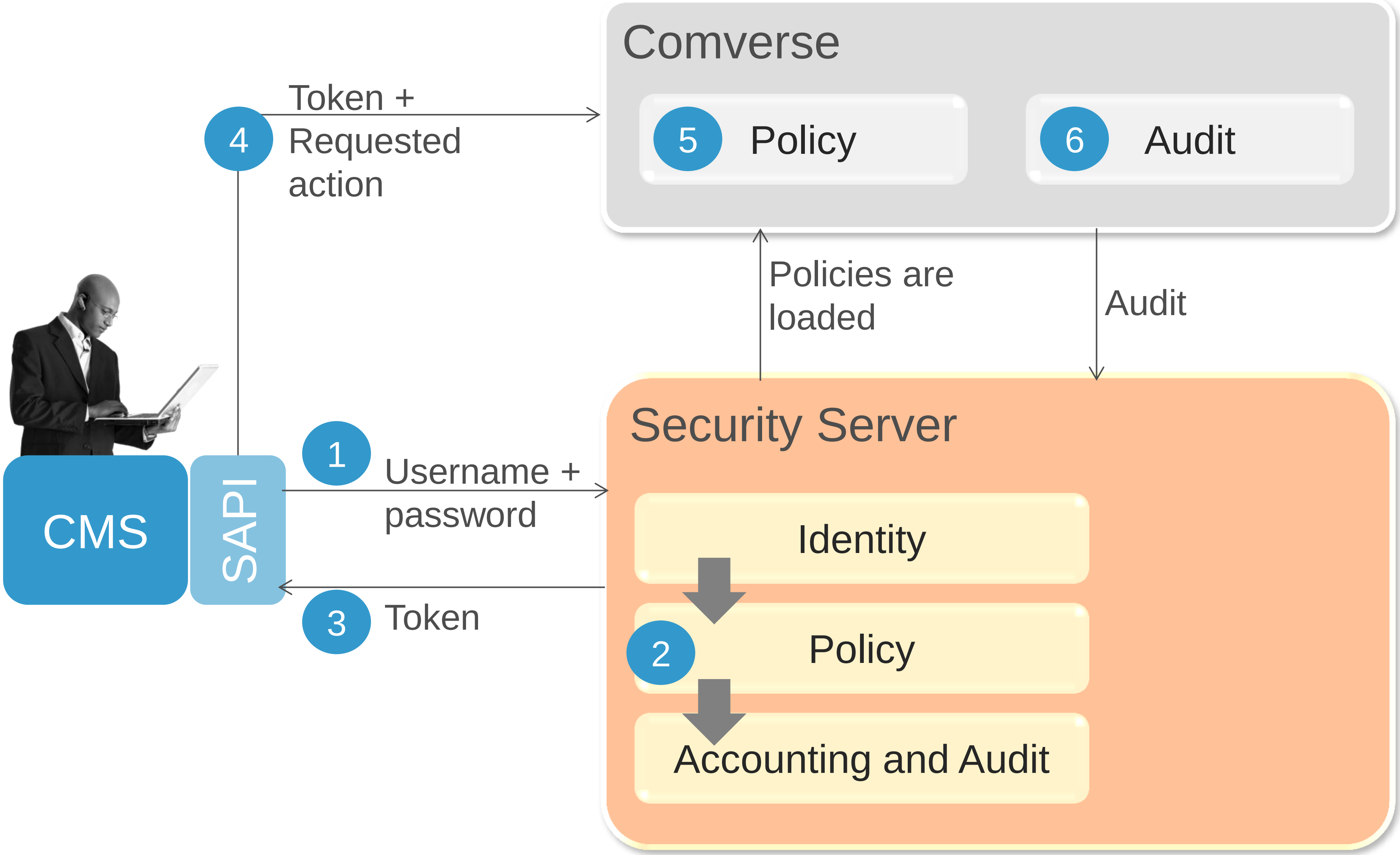
Request and enforce authorization

Security Server

Policy **A**dministration **P**oint

Create and store policy

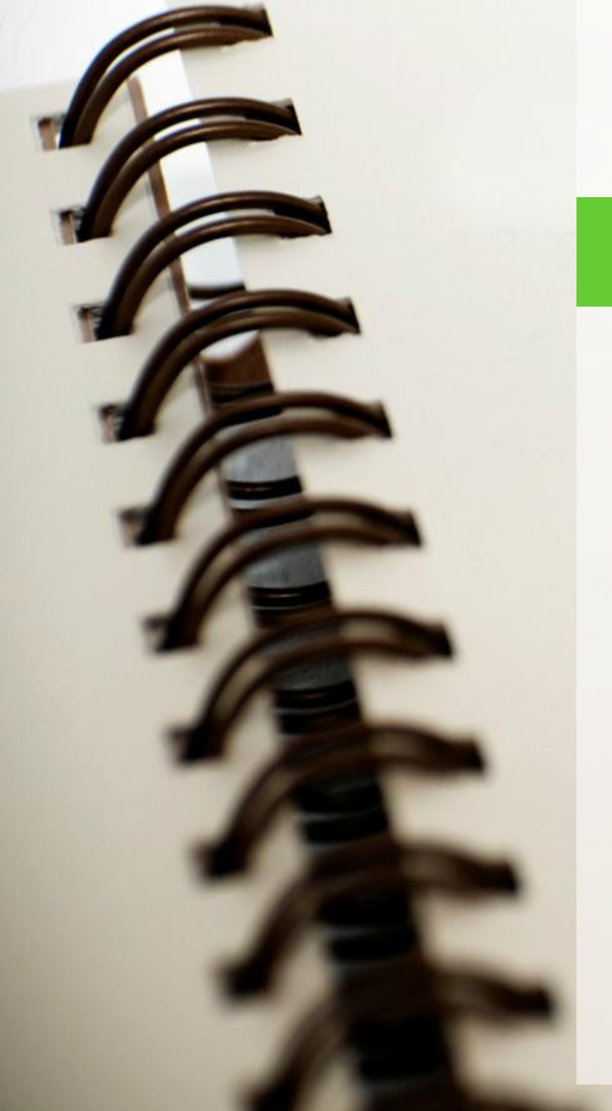
Security Flow



Review Questions

1. What does the Authentication process do?
   a. Identifies the user, through login and password security credentials
   b. Grant access to authenticated users
   c. Tracks the activities of users
   d. All of the above
2. What part of AAA does the Security Policy Manager implement?
   a. Authentication
   b. Authorization
   c. Accounting
3. An application requests services from a Comverse ONE host, using the SAPI. What type of OASIS security point is the application?
   a. PAP - Policy Administration Point
   b. PDP - Policy Decision Point
   c. PEP - Policy Enforcement Point
4. An application sends requests to Comverse ONE. How is the request checked against the security policy?
   a. Every request is forwarded to the security server for approval
   b. A copy of the policy is part of the token given to the application in the authentication process
   c. A copy of the policy is saved on the host, it checks the token against the policy.
   d. After the authentication and authorization process, all requests to the application are approved

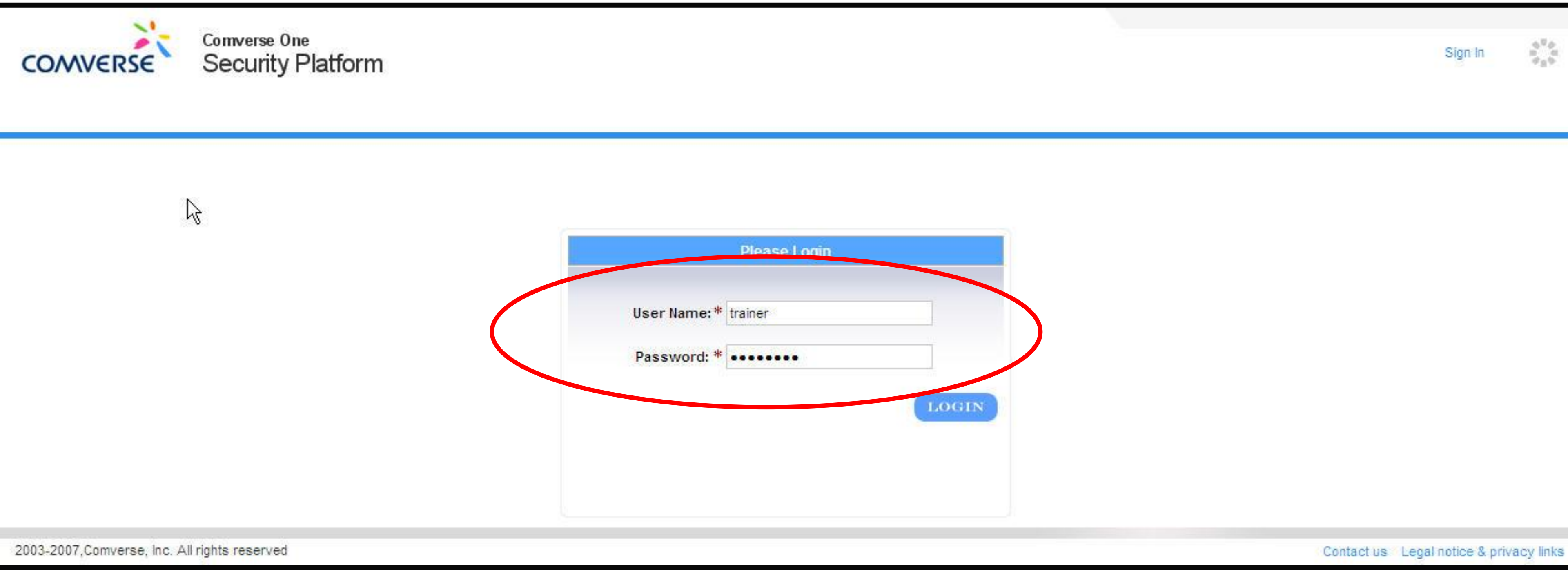
Agenda



- The Unified Platform
- Security Overview
- Using the Unified Platform Manager
- Identity Management
- Policy Management
- Key and Credential Management
- Accounting and Audit

Security GUI Login

http://<IP address of Security Server>:8800/security/

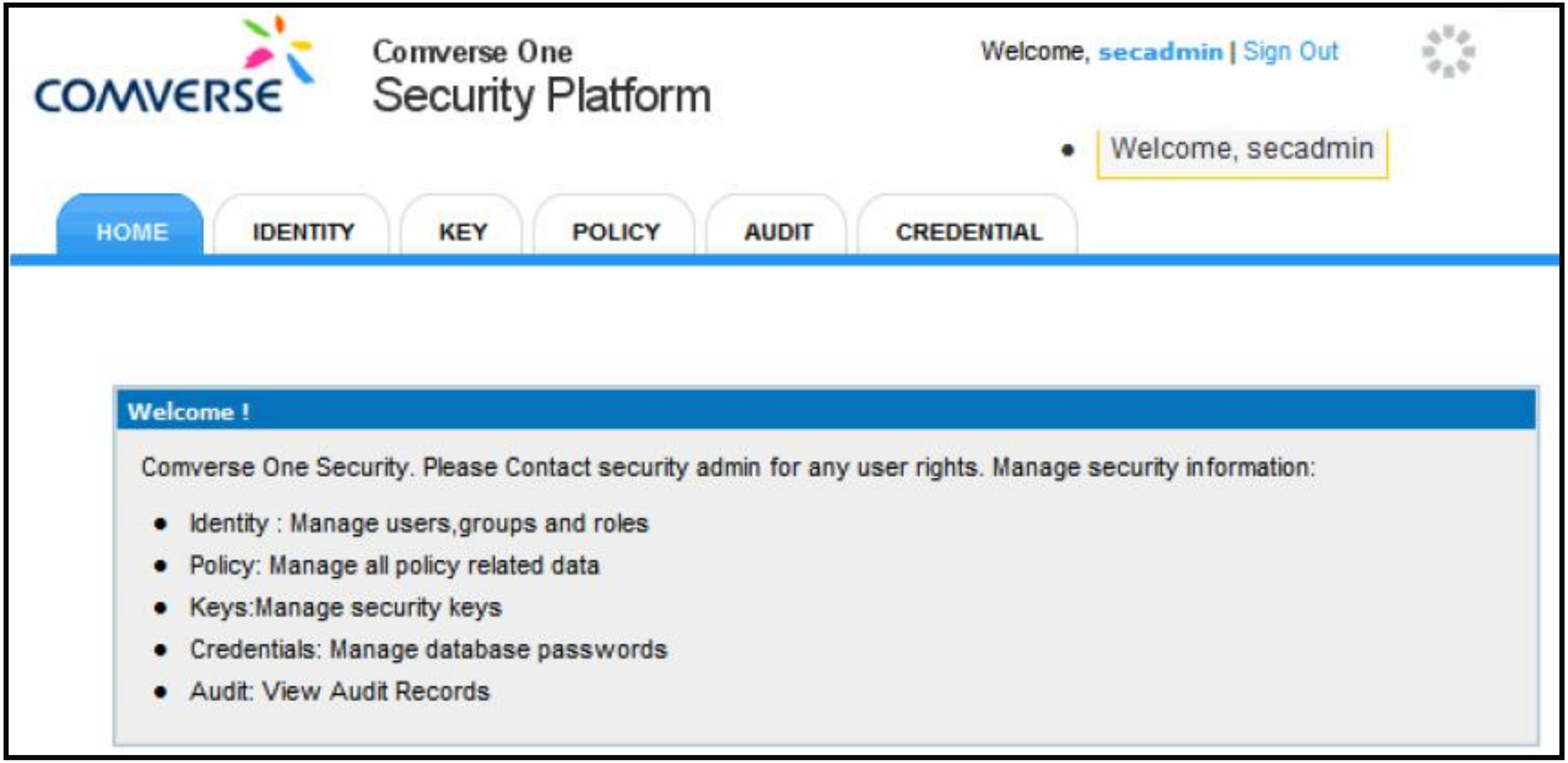


User Name: * trainer

Password: * •••••••••

COMVERSE
Comverse One
Security Platform
Sign In
Please Login
LOGIN
2003-2007,Comverse, Inc. All rights reserved
Contact us
Legal notice & privacy links

Security GUI (2)

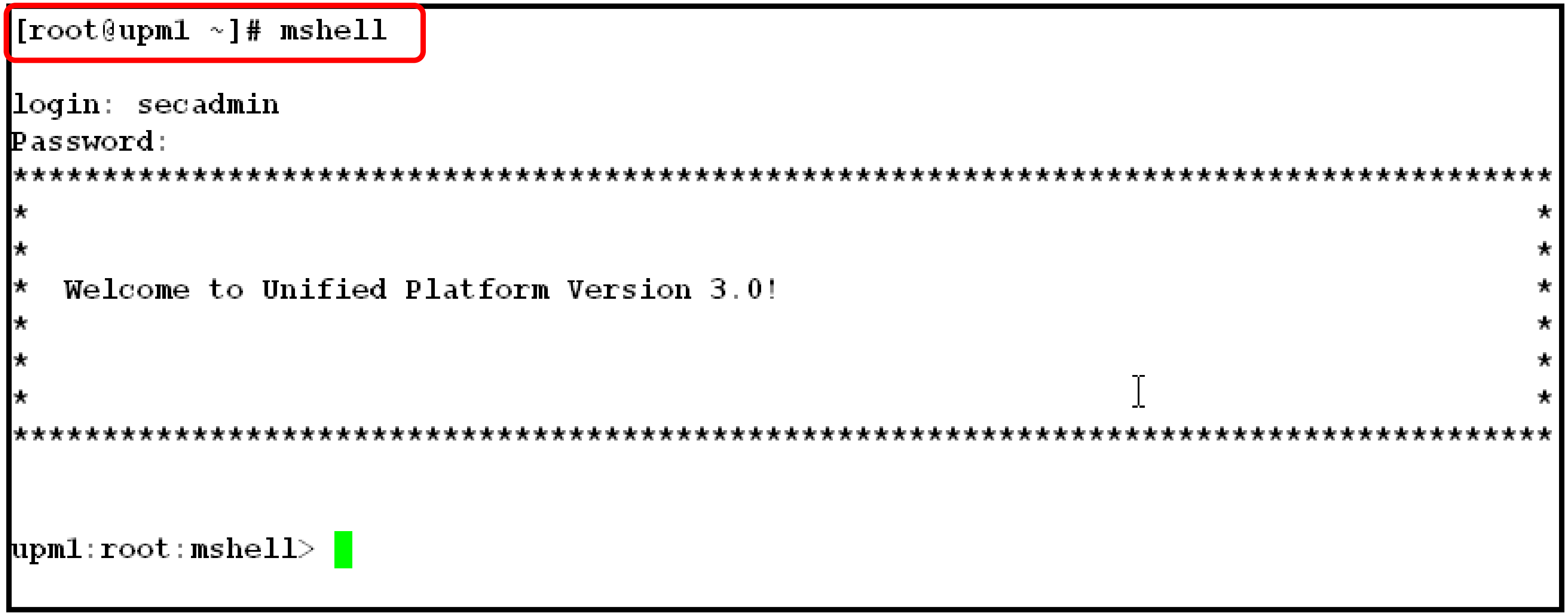


Welcome !

Comverse One Security. Please Contact security admin for any user rights. Manage security information:

- Identity : Manage users,groups and roles
- Policy: Manage all policy related data
- Keys:Manage security keys
- Credentials: Manage database passwords
- Audit: View Audit Records

UPM CLI Access



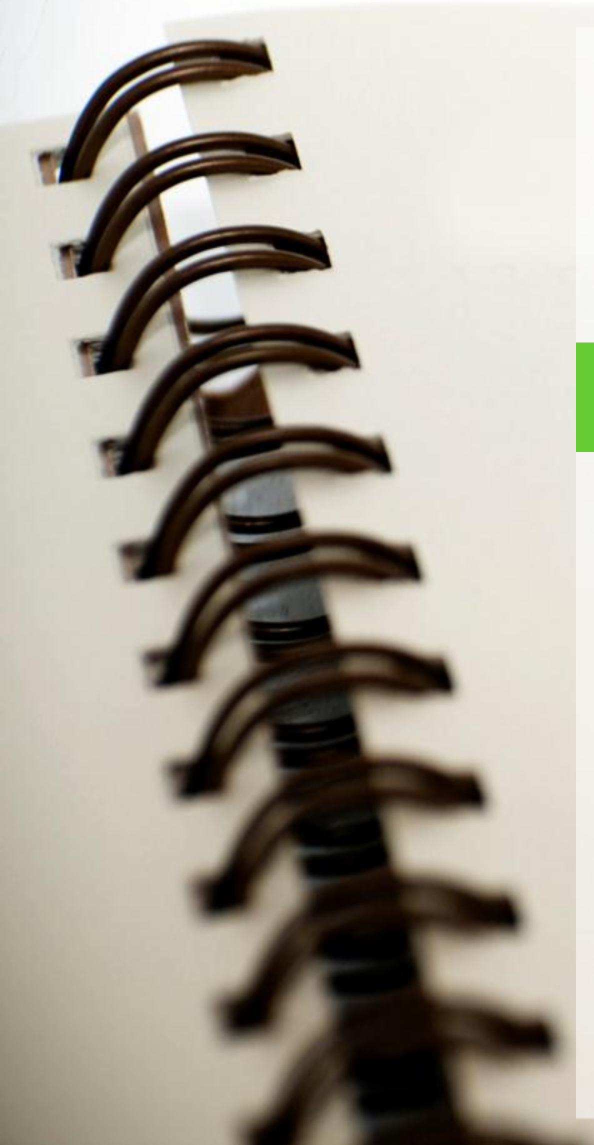
```
[root@upm1 ~]# mshell

login: secadmin
Password:
***************************************************************************************
*                                                                                     *
*                                                                                     *
*  Welcome to Unified Platform Version 3.0!                                           *
*                                                                                     *
*                                                                                     *
*                                                                                     *
***************************************************************************************


upm1:root:mshell>
```

mShell resides in the UPM and in all the UPAs.

Agenda



The Unified Platform

Security Overview

Using the Unified Platform Manager

Identity Management

Policy Management

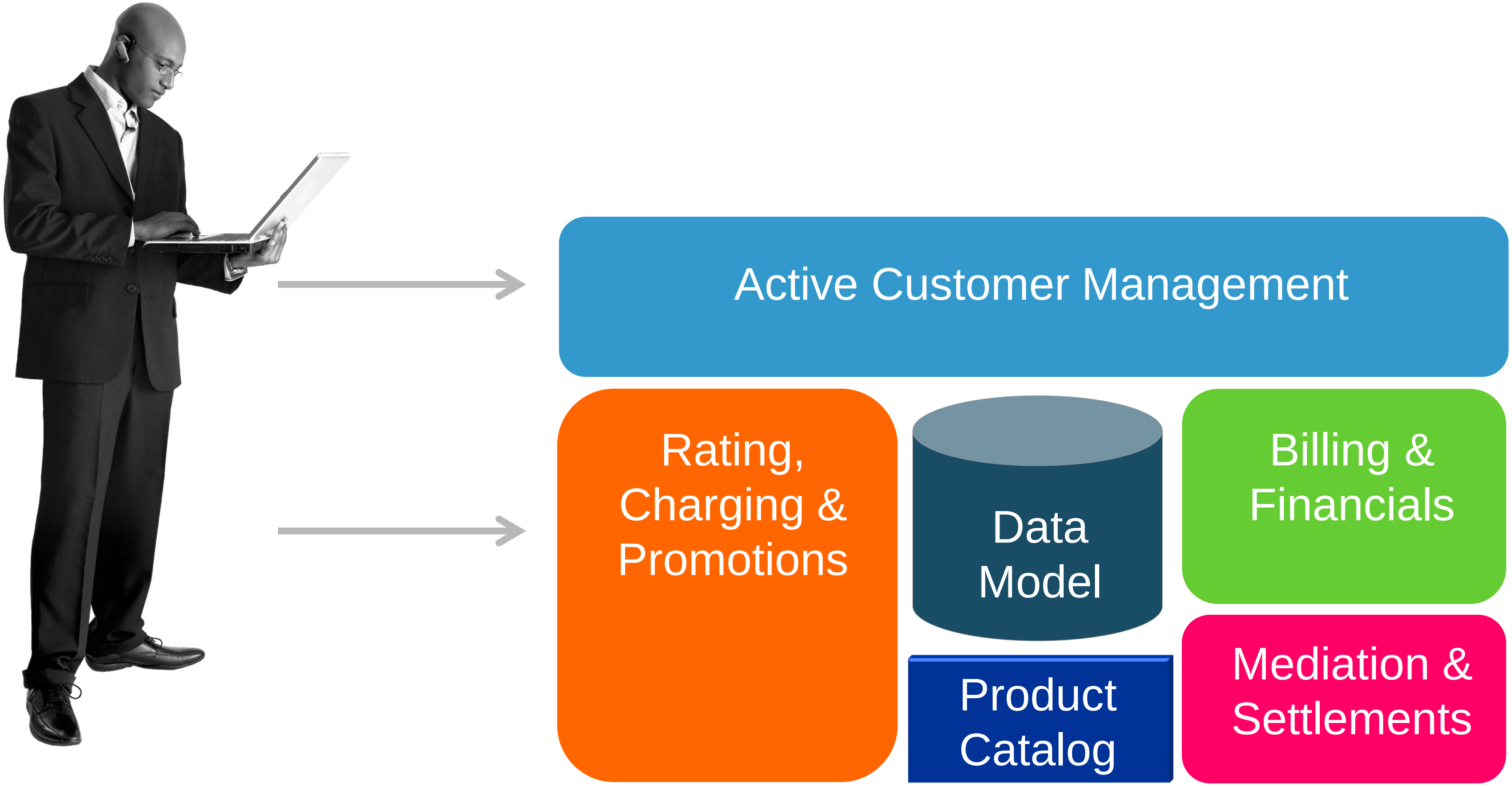
Key and Credential Management

Accounting and Audit

Identity Management

Authentication

- Who are the users?
- How do they relate to each part of the application?
- What is their role in the system?



Active Customer Management

Rating, Charging & Promotions

Data Model

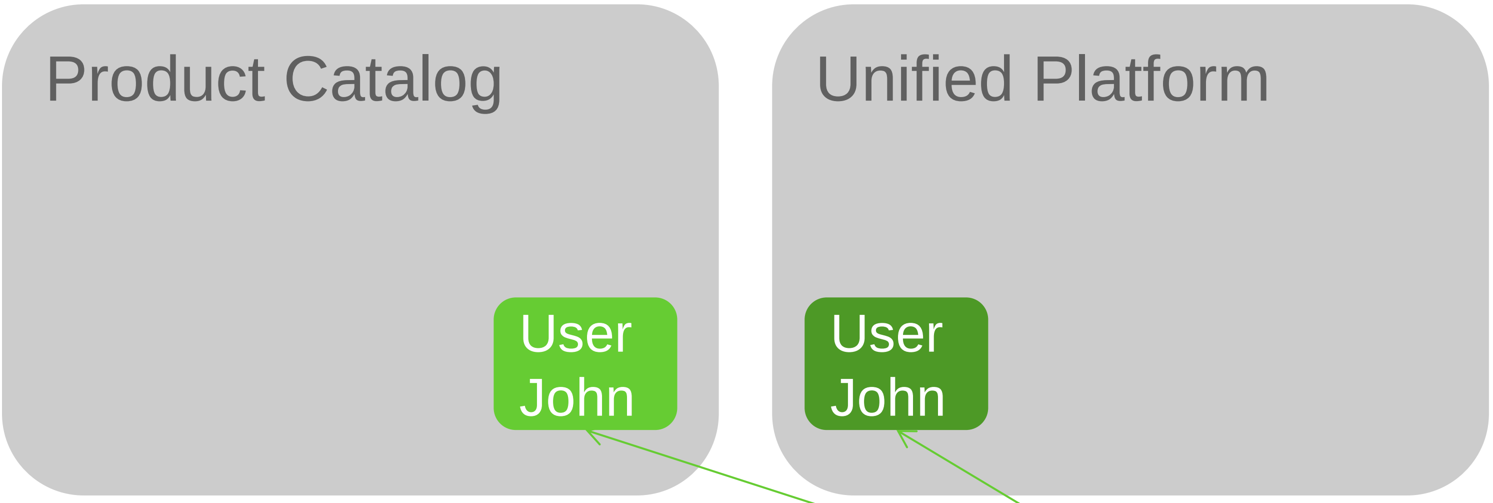
Billing & Financials

Product Catalog

Mediation & Settlements

Data Model – Security Realm

Security Realm


Product Catalog

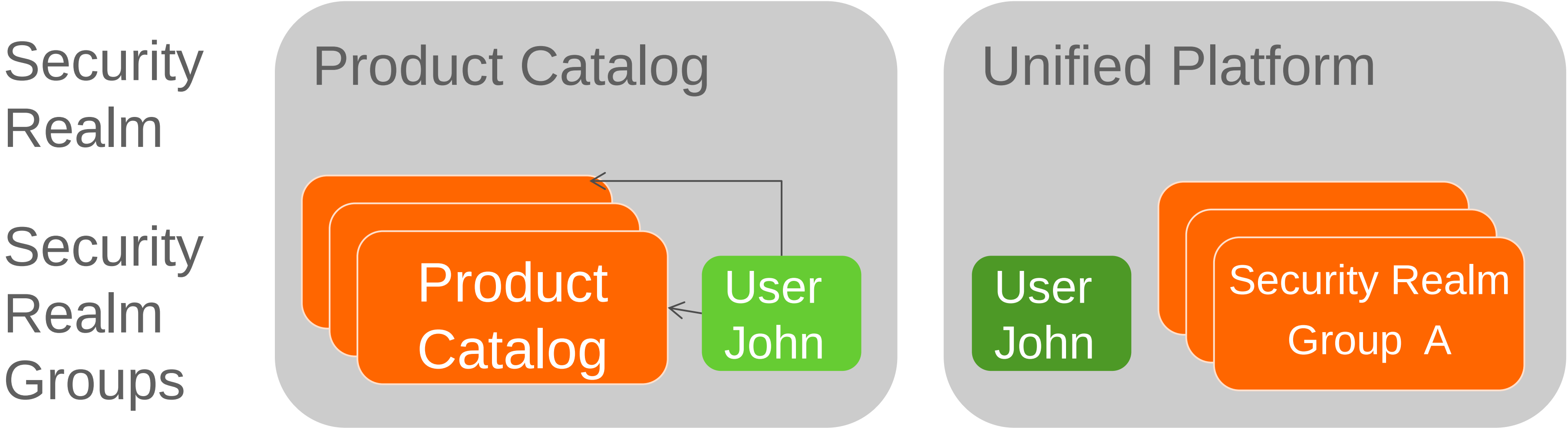
User John

Unified Platform

User John

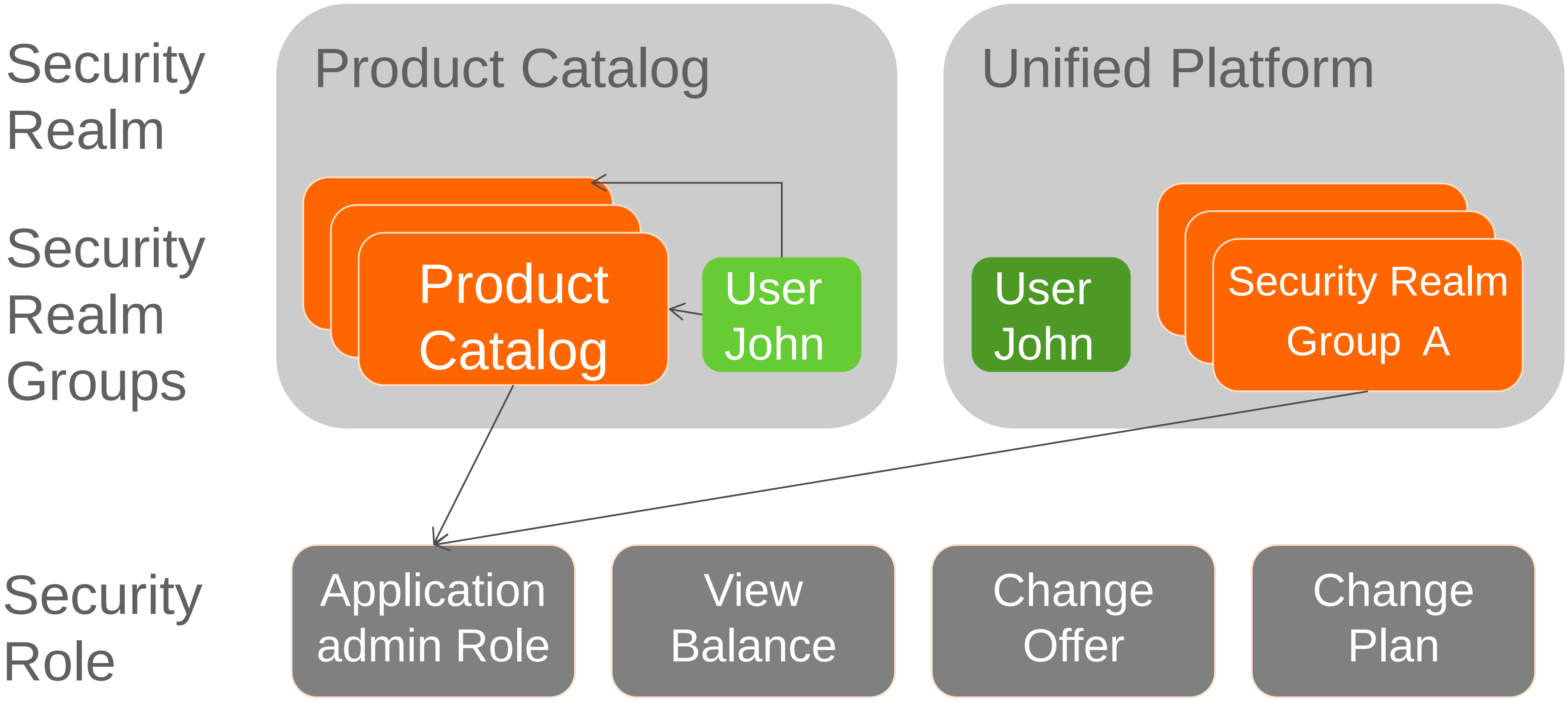
- Determines the scope of security data
- Usually scoped by application components
- Users are defined per realm

Data Model – Security Realm Groups



- Provide common attributes to a subset of users
- Provide one or more security roles for that group of users
- A user can belong to one or more groups
- Users must have a priority group assigned

Data Model – Security Role



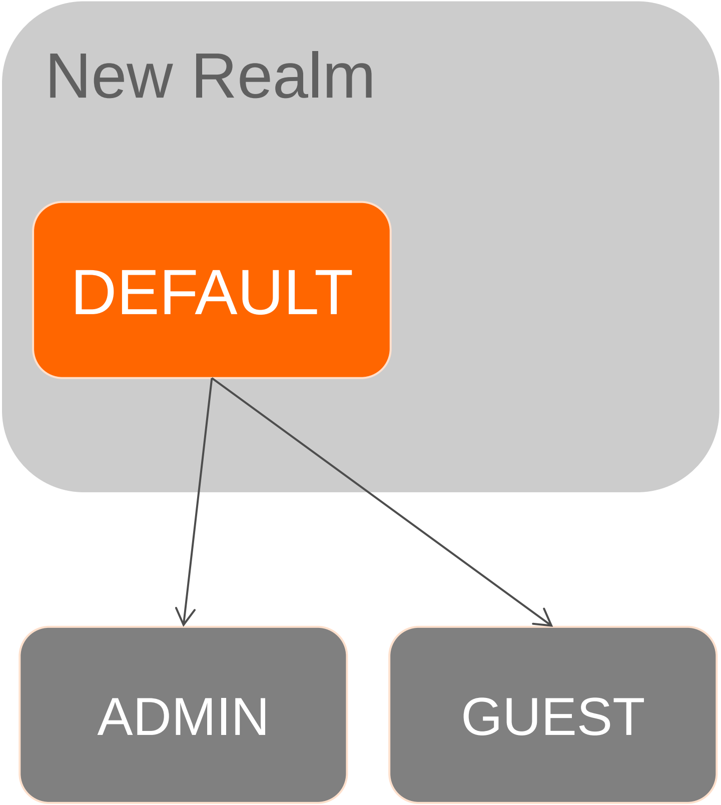
- Define privileges granted to a realm group of users
- Multiple groups can be granted a single security role.

Data Model – Default Objects

Security Realm

Security Realm Groups

Security Role



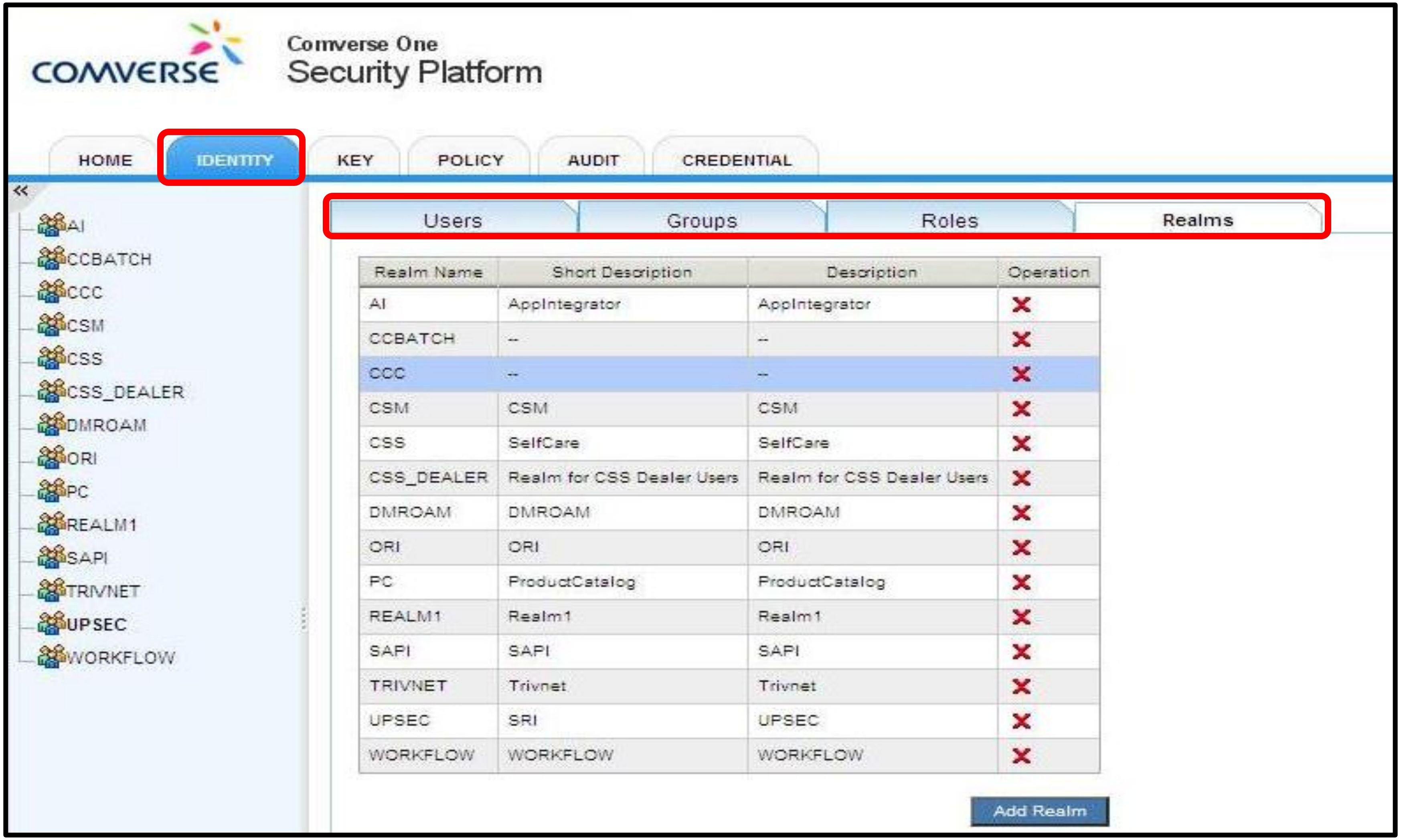
New Realm

DEFAULT

ADMIN

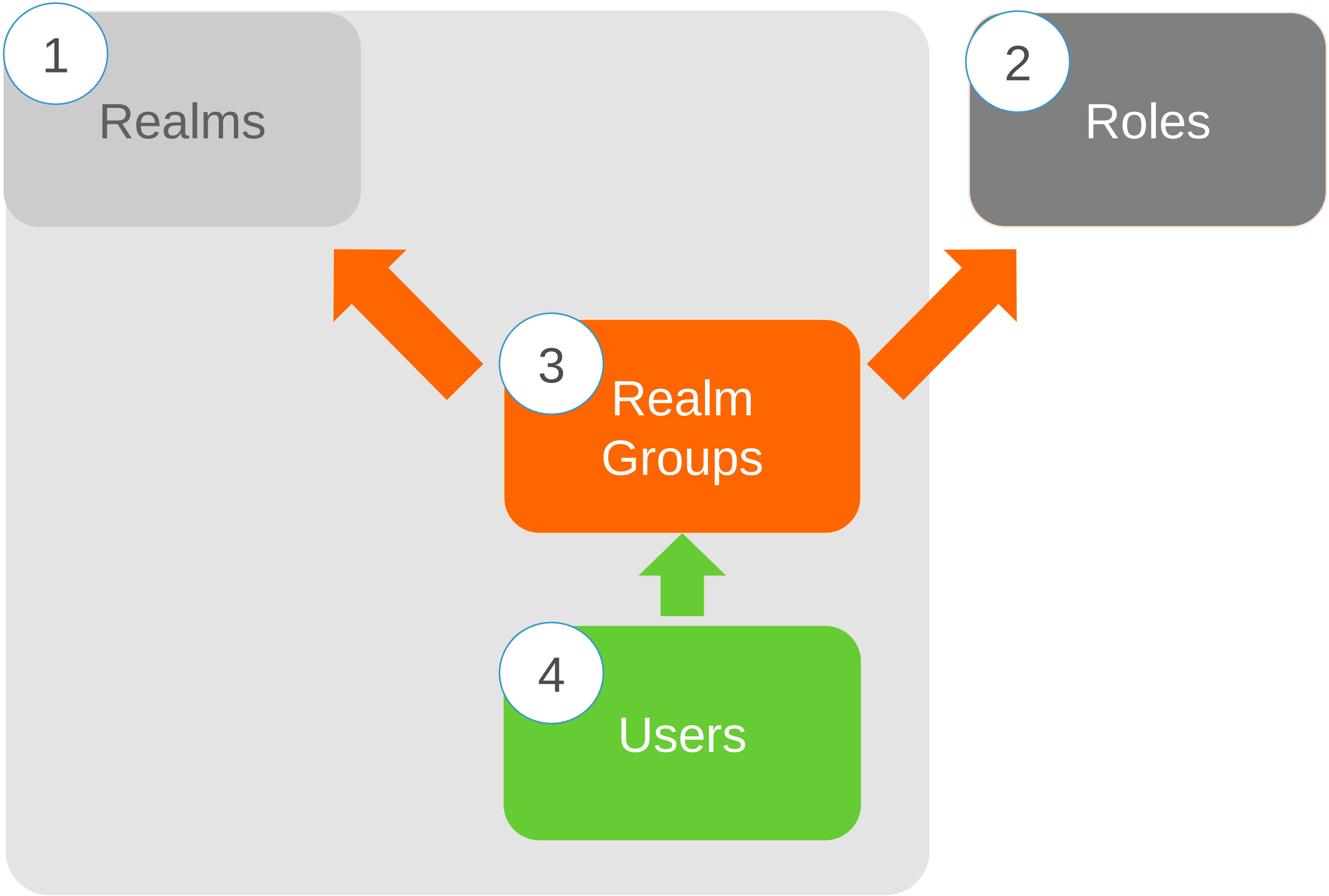
GUEST

Identity Management GUI



Realm Name	Short Description	Description	Operation
AI	AppIntegrator	AppIntegrator	✕
CCBATCH	--	--	✕
CCC	--	--	✕
CSM	CSM	CSM	✕
CSS	SelfCare	SelfCare	✕
CSS_DEALER	Realm for CSS Dealer Users	Realm for CSS Dealer Users	✕
DMROAM	DMROAM	DMROAM	✕
ORI	ORI	ORI	✕
PC	ProductCatalog	ProductCatalog	✕
REALM1	Realm1	Realm1	✕
SAPI	SAPI	SAPI	✕
TRIVNET	Trivnet	Trivnet	✕
UPSEC	SRI	UPSEC	✕
WORKFLOW	WORKFLOW	WORKFLOW	✕

Definition Process



1

Realms

2

Roles

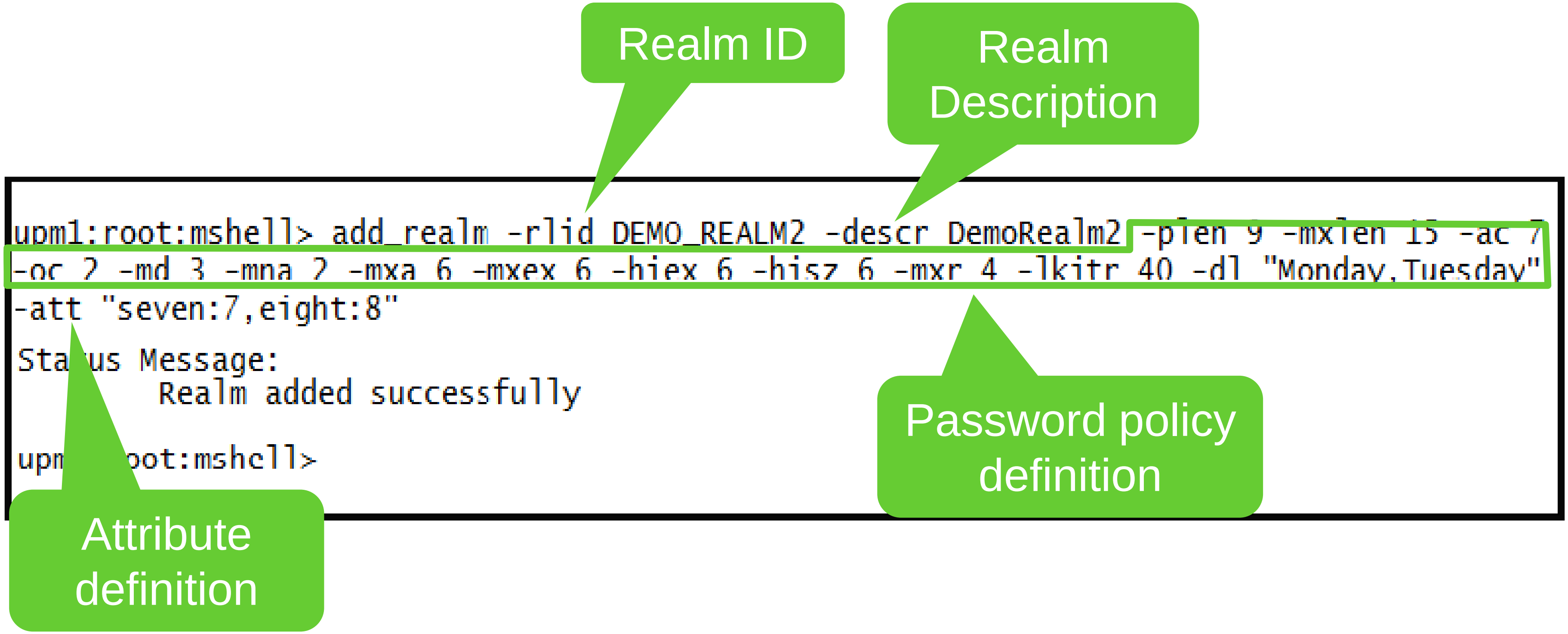
3

Realm Groups

4

Users

Adding Realms



```
upm1:root:mshell> add_realm -rlid DEMO_REALM2 -descr DemoRealm2 -plen 9 -mxlen 15 -ac 7
-oc 2 -md 3 -mna 2 -mxa 6 -mxex 6 -hiex 6 -hisz 6 -mxr 4 -lkitr 40 -dl "Monday,Tuesday"
-att "seven:7,eight:8"
 Status Message:
         Realm added successfully

 upm1:root:mshell>
```

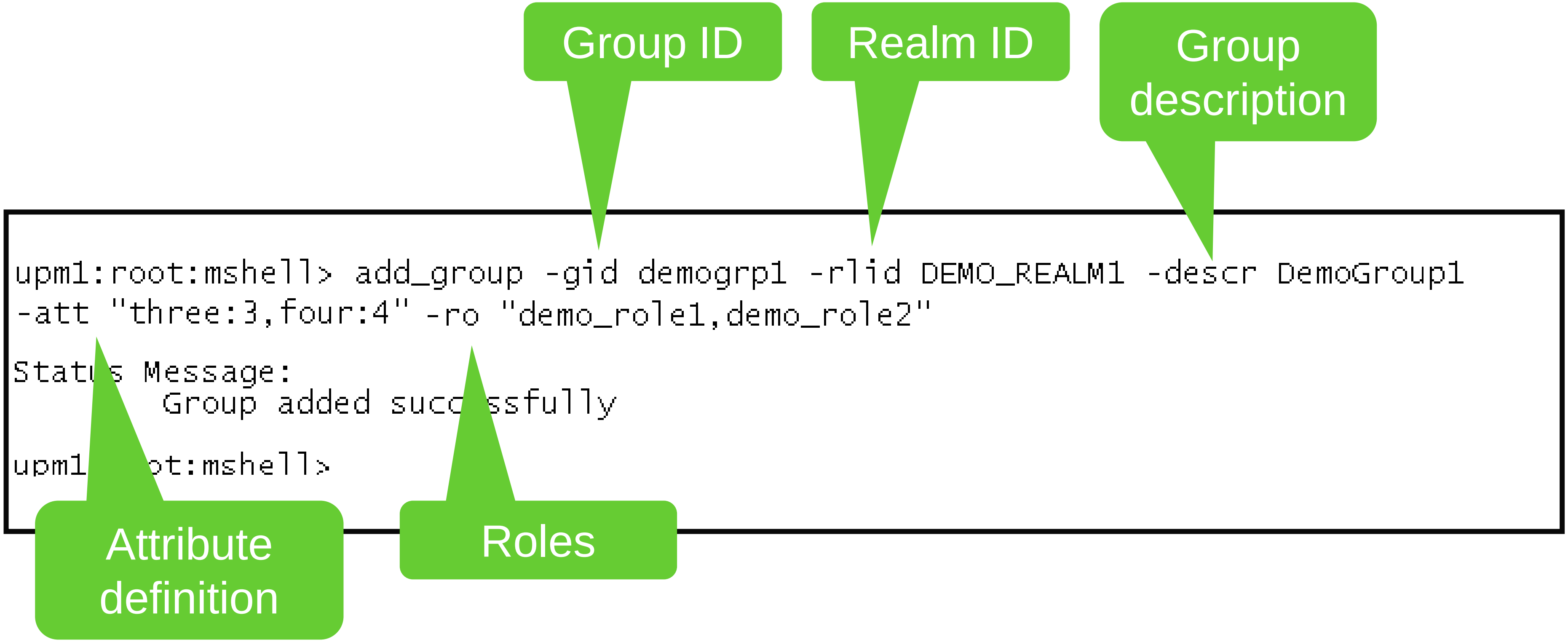
Realm ID

Realm Description

Password policy definition

Attribute definition

Adding Realm Groups



```
upm1:root:mshell> add_group -gid demogrp1 -rlid DEMO_REALM1 -descr DemoGroup1
-att "three:3,four:4" -ro "demo_role1,demo_role2"

Status Message:
        Group added successfully

upm1:root:mshell>
```

Group ID

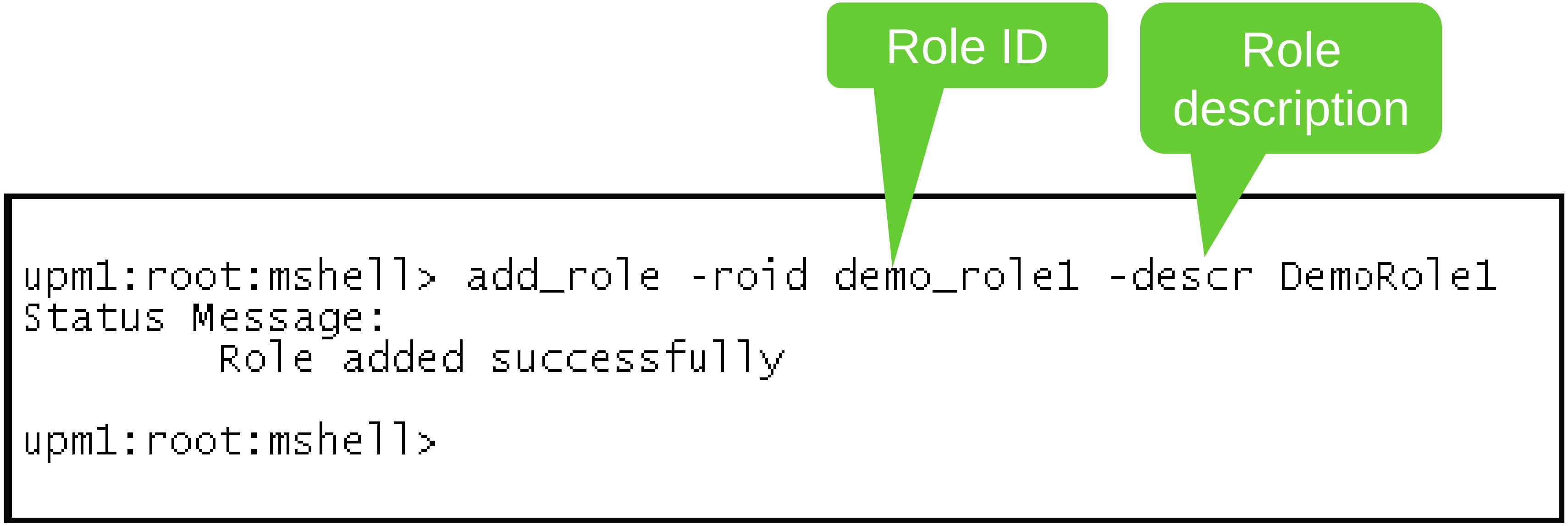
Realm ID

Group description

Attribute definition

Roles

Adding Roles



Role ID

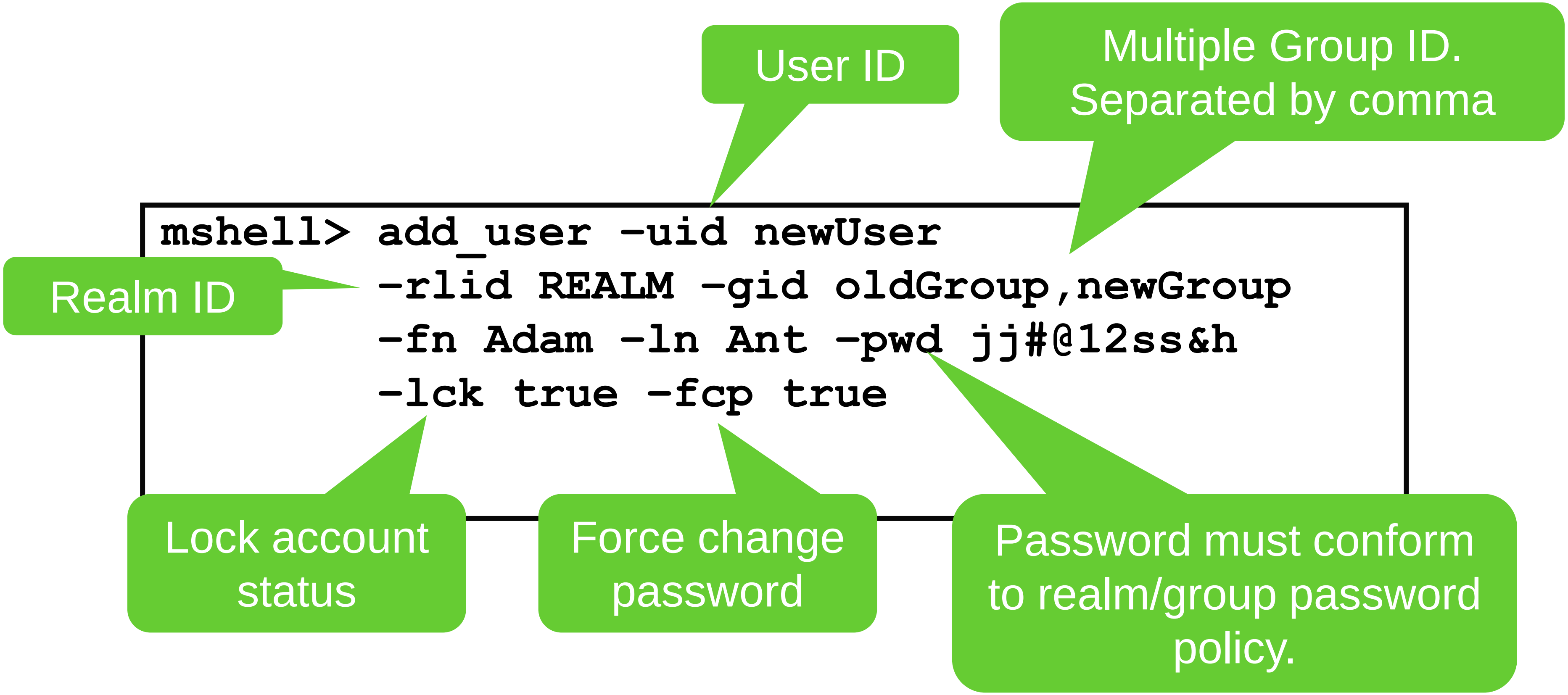
Role description

```
upm1:root:mshell> add_role -roid demo_role1 -descr DemoRole1
Status Message:
        Role added successfully

upm1:root:mshell>
```

Roles are used to define authorization policies (described later)

Adding Users – mShell



```
mshell> add_user -uid newUser
        -rlid REALM -gid oldGroup,newGroup
        -fn Adam -ln Ant -pwd jj#@12ss&h
        -lck true -fcp true
```

User ID

Multiple Group ID. Separated by comma

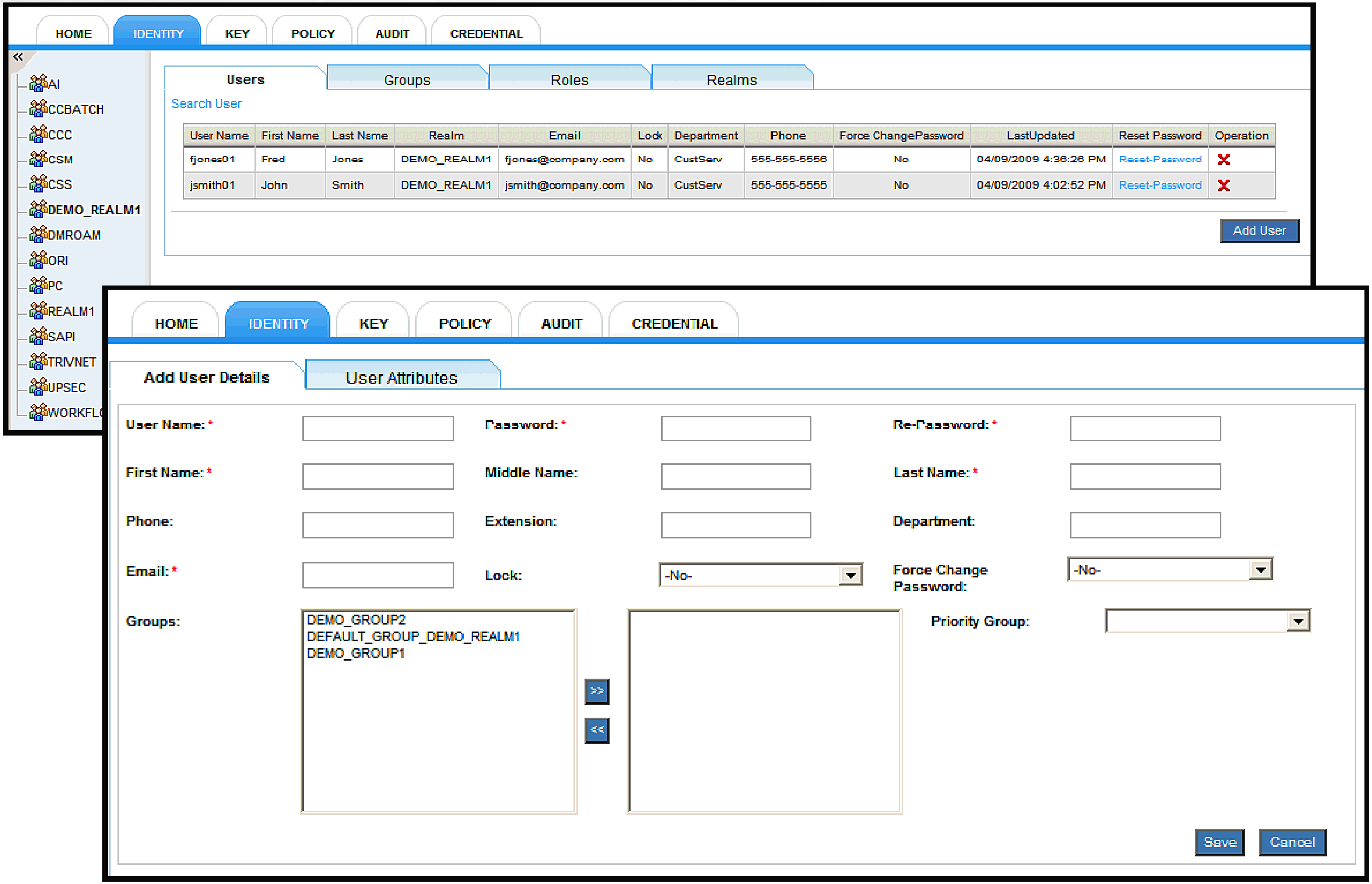
Realm ID

Lock account status

Force change password

Password must conform to realm/group password policy.

Adding Users – Security GUI



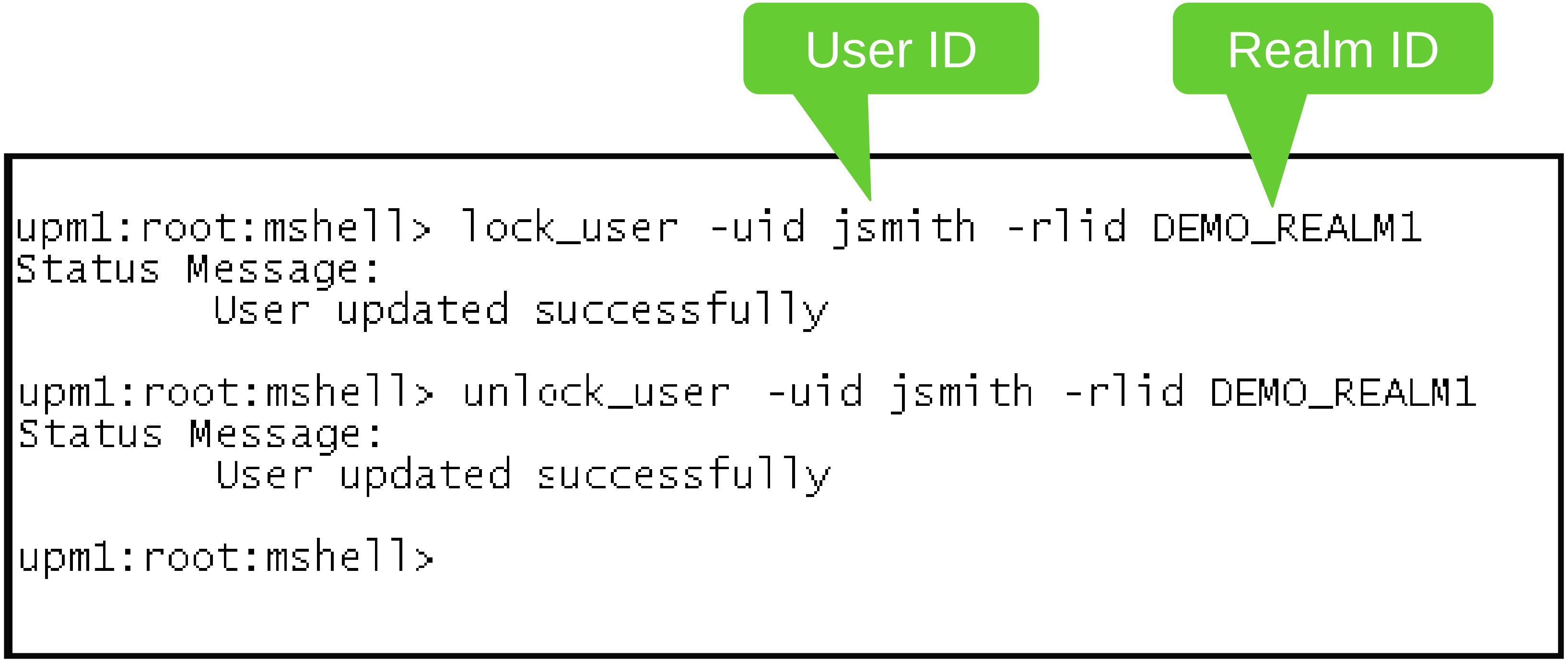
User Name	First Name	Last Name	Realm	Email	Lock	Department	Phone	Force ChangePassword	LastUpdated	Reset Password	Operation
fjones01	Fred	Jones	DEMO_REALM1	fjones@company.com	No	CustServ	555-555-5556	No	04/09/2009 4:36:26 PM	Reset-Password	✗
jsmith01	John	Smith	DEMO_REALM1	jsmith@company.com	No	CustServ	555-555-5555	No	04/09/2009 4:02:52 PM	Reset-Password	✗

User Name: *		Password: *		Re-Password: *	
First Name: *		Middle Name:		Last Name: *	
Phone:		Extension:		Department:	
Email: *		Lock:	-No-	Force Change Password:	-No-
Groups:	DEMO_GROUP2 DEFAULT_GROUP_DEMO_REALM1 DEMO_GROUP1			Priority Group:	

Locking / Unlocking User Accounts

User Account is locked when:

- Created with locked status
- Failed login attempts
- User didn’t change password



User ID

Realm ID

```
upm1:root:mshell> lock_user -uid jsmith -rlid DEMO_REALM1
Status Message:
        User updated successfully

upm1:root:mshell> unlock_user  -uid jsmith -rlid DEMO_REALM1
Status Message:
        User updated successfully

upm1:root:mshell>
```

Bulk Account Management Operations

- A sample spreadsheet is located in: $JBOSS_HOME/templates/security

- After editing the file, execute command

```
mshell> add_user –b
```

Provisioning Style	Users are associated to group	User attributes	Group attributes
Basic	DEFAULT	No	No
Normal	DEFAULT	Yes	No
Advanced	Multiple groups within a given realm	Yes	Yes

Review Questions

1. Realms normally represent
   a. A scope of a Comverse ONE application
   b. A grope of users that belong to the same department in the organization
   c. A group of users with the same security attributes
2. When you define a user, what do you associate it with?
   a. Realms
   b. Realm groups
   c. Roles
3. What is a role associated with?
   a. Realms
   b. Realm groups
   c. Users
4. Which of the following is NOT true?
   a. A user can belong to more than one Realm
   b. A user can belong to more than one Realm Group
   c. A user can belong to more than one Role

Agenda

The Unified Platform

Security Overview

Using the Unified Platform Manager

Identity Management

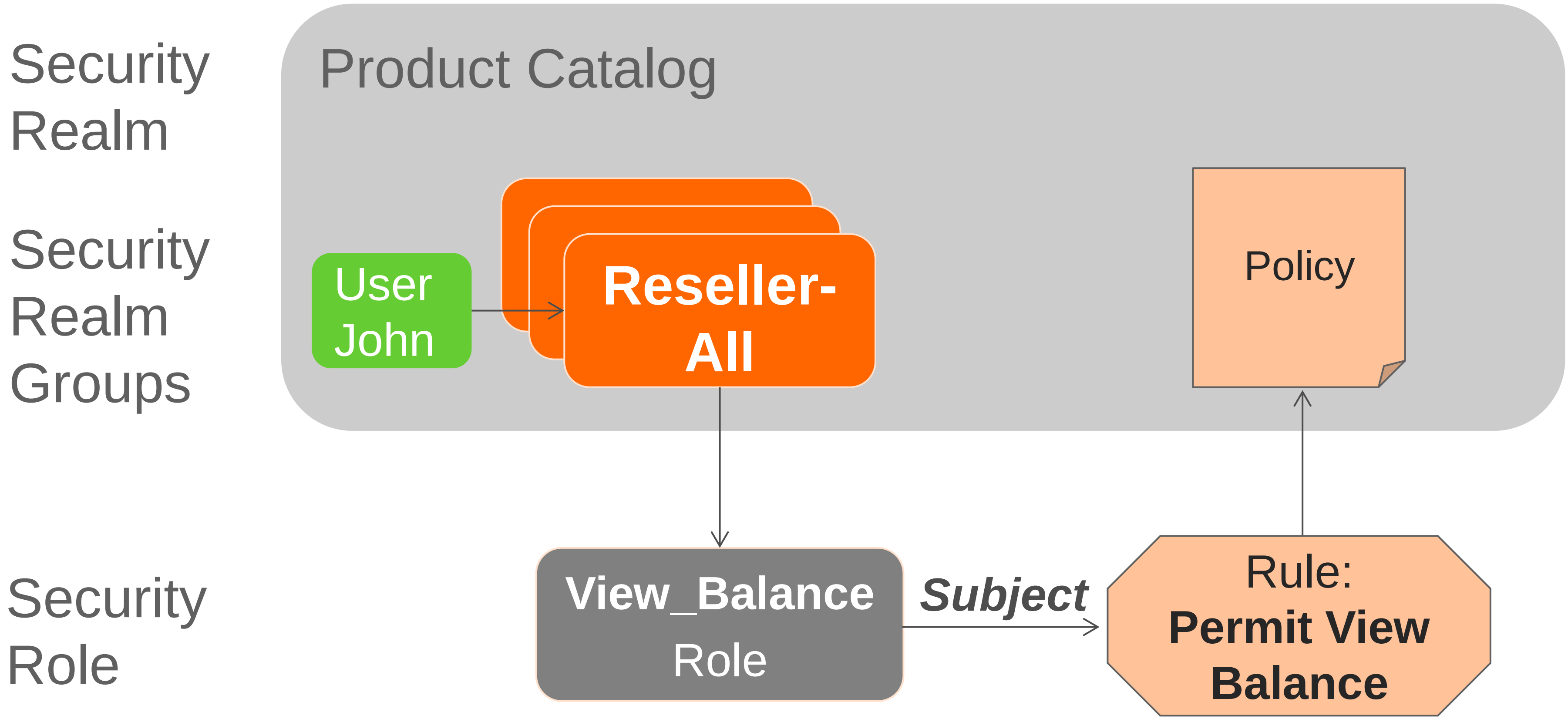
Policy Management

Key and Credential Management

Accounting and Audit

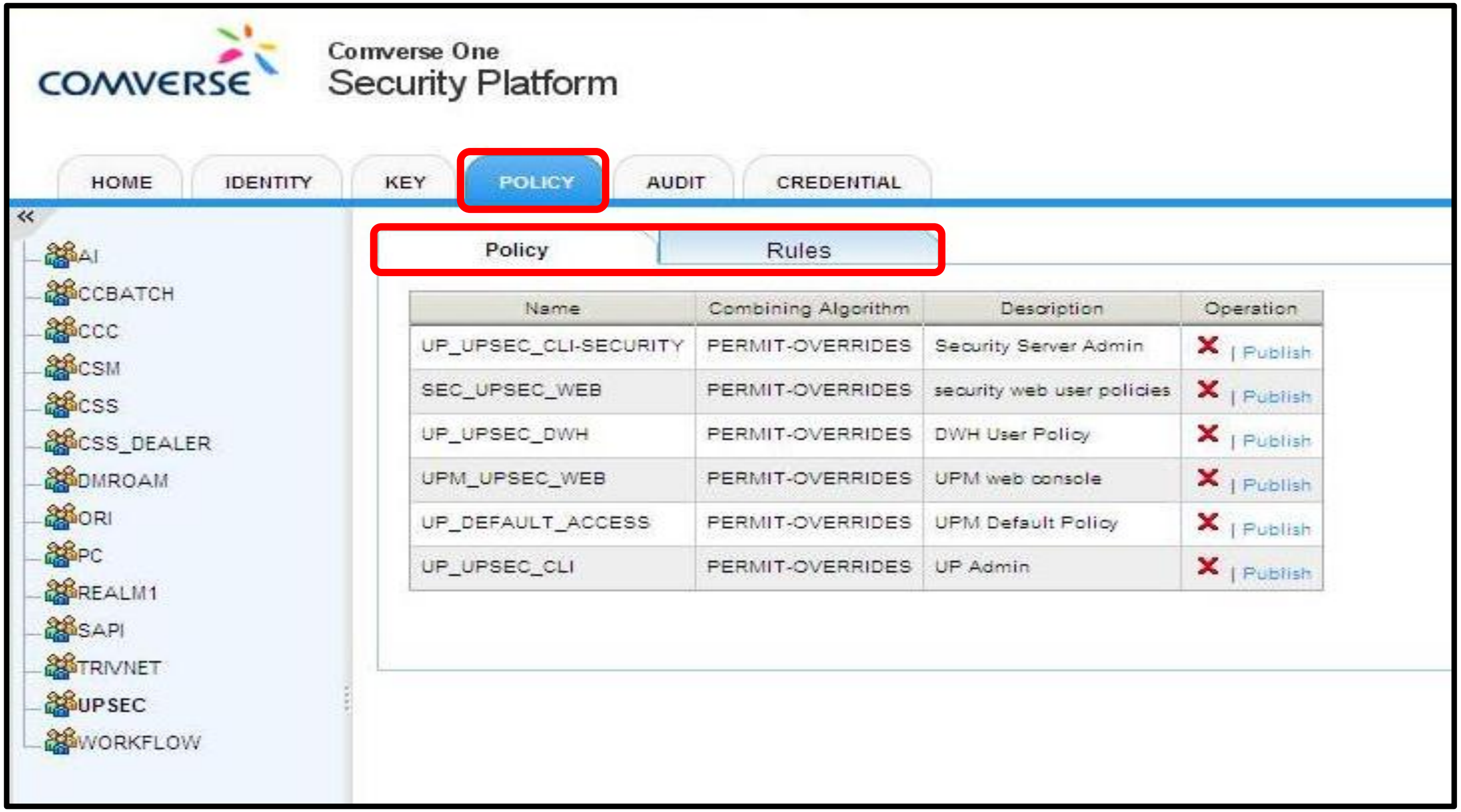
Policy Management

Authorization



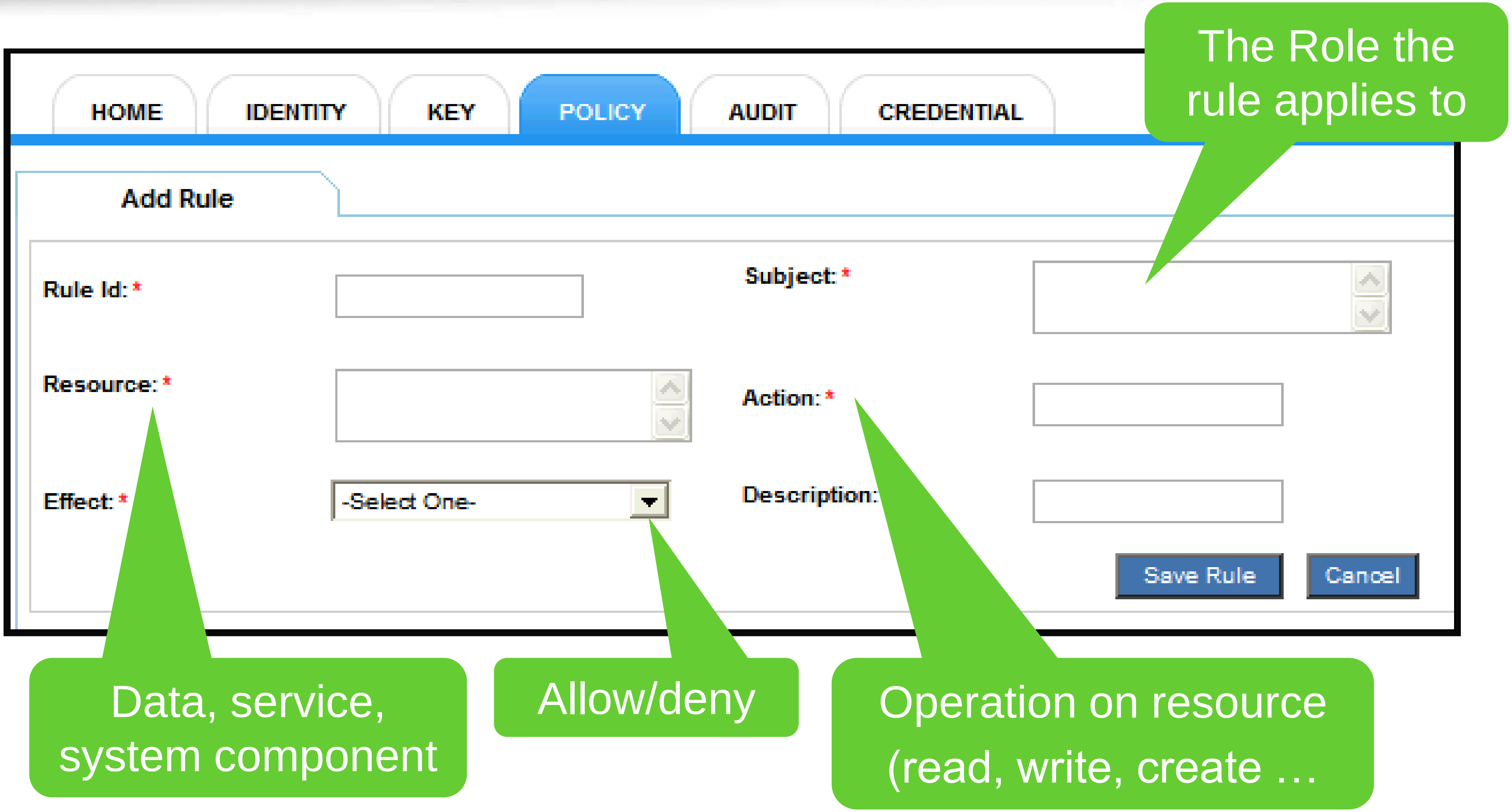
- Policy – a collection of Rules
- Rules – a function that is permitted or denied

Policy Management GUI



Name	Combining Algorithm	Description	Operation
UP_UPSEC_CLI-SECURITY	PERMIT-OVERRIDES	Security Server Admin	✗ | Publish
SEC_UPSEC_WEB	PERMIT-OVERRIDES	security web user policies	✗ | Publish
UP_UPSEC_DWH	PERMIT-OVERRIDES	DWH User Policy	✗ | Publish
UPM_UPSEC_WEB	PERMIT-OVERRIDES	UPM web console	✗ | Publish
UP_DEFAULT_ACCESS	PERMIT-OVERRIDES	UPM Default Policy	✗ | Publish
UP_UPSEC_CLI	PERMIT-OVERRIDES	UP Admin	✗ | Publish

Rule Definition

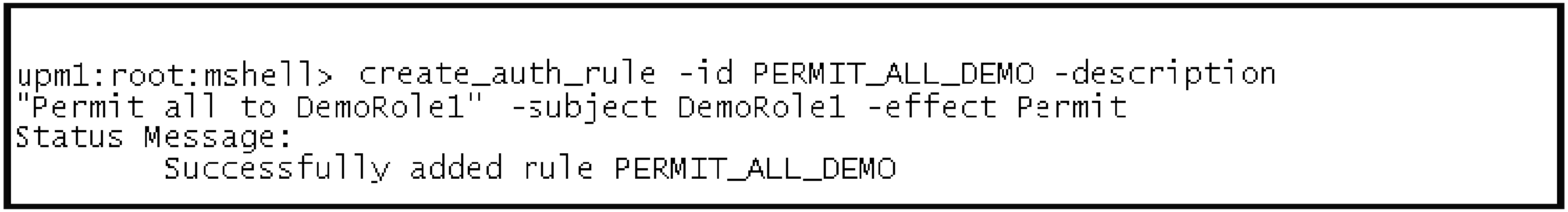


The Role the rule applies to

Data, service, system component

Allow/deny

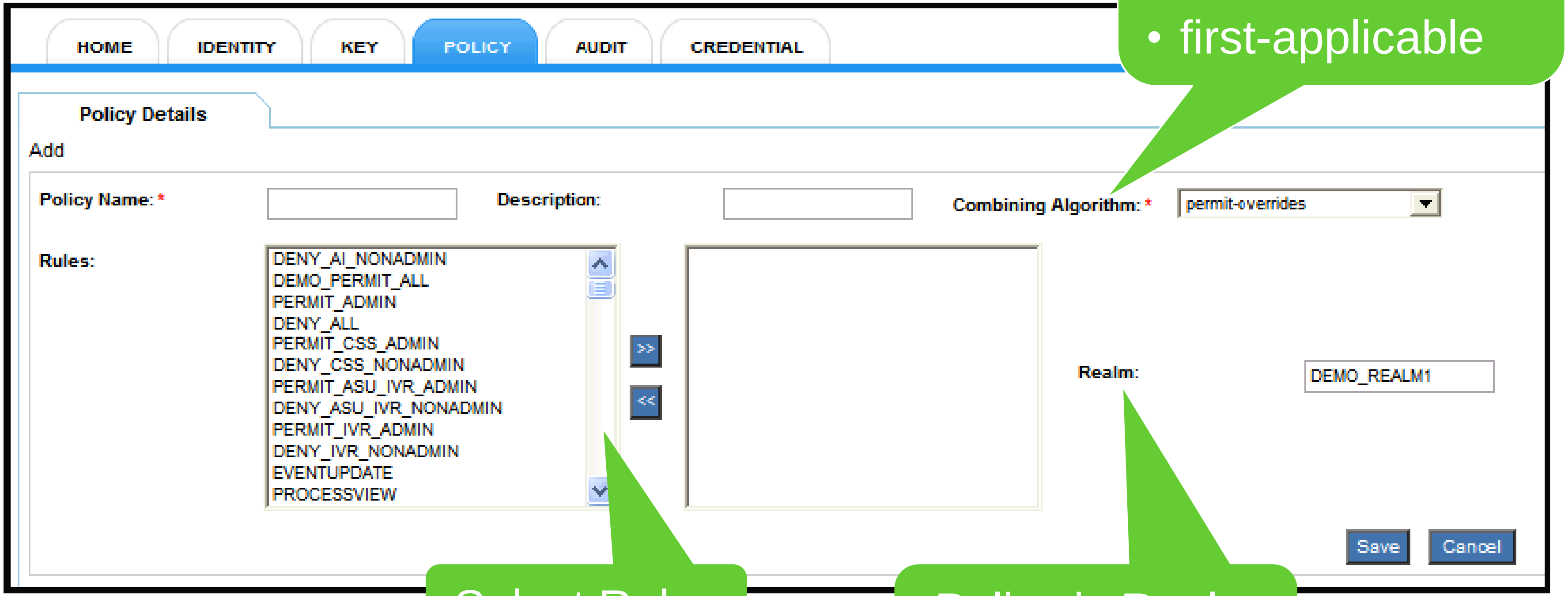
Operation on resource (read, write, create …



```
upm1:root:mshell> create_auth_rule -id PERMIT_ALL_DEMO -description
"Permit all to DemoRole1" -subject DemoRole1 -effect Permit
Status Message:
        Successfully added rule PERMIT_ALL_DEMO
```

Policy Definition

- permit-overrides
- deny-overrides
- first-applicable



Add

Policy Name:*

Description:

Combining Algorithm:* permit-overrides

Rules:
DENY_AI_NONADMIN
DEMO_PERMIT_ALL
PERMIT_ADMIN
DENY_ALL
PERMIT_CSS_ADMIN
DENY_CSS_NONADMIN
PERMIT_ASU_IVR_ADMIN
DENY_ASU_IVR_NONADMIN
PERMIT_IVR_ADMIN
DENY_IVR_NONADMIN
EVENTUPDATE
PROCESSVIEW

Realm: DEMO_REALM1

Select Rules

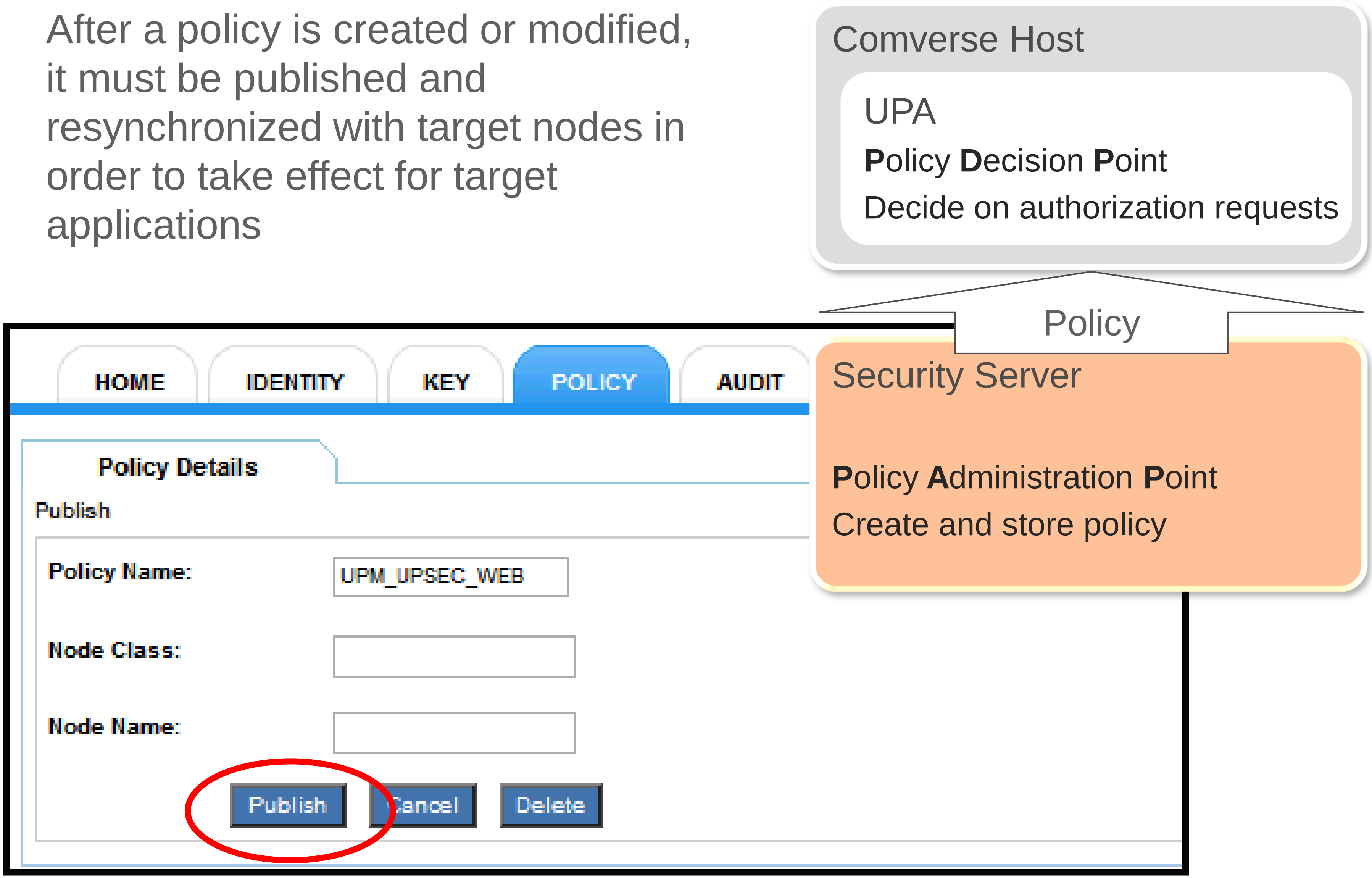
Policy is Realm specific

```
uom1:root:mshell> create_auth_policy -id DEMO_DEFAULT_ACCESS -description
 "Demo Default Access" -realm DEMO_REALM1 -rules "PERMIT_ALL_DEMO,DENY_ALL"
Status Message:
       Successfully added policy DEMO_DEFAULT_ACCESS

uom1:root:mshell>
```

Publishing a Policy – GUI

After a policy is created or modified, it must be published and resynchronized with target nodes in order to take effect for target applications



Comverse Host

UPA

Policy **D**ecision **P**oint

Decide on authorization requests

Policy

Security Server

Policy **A**dministration **P**oint

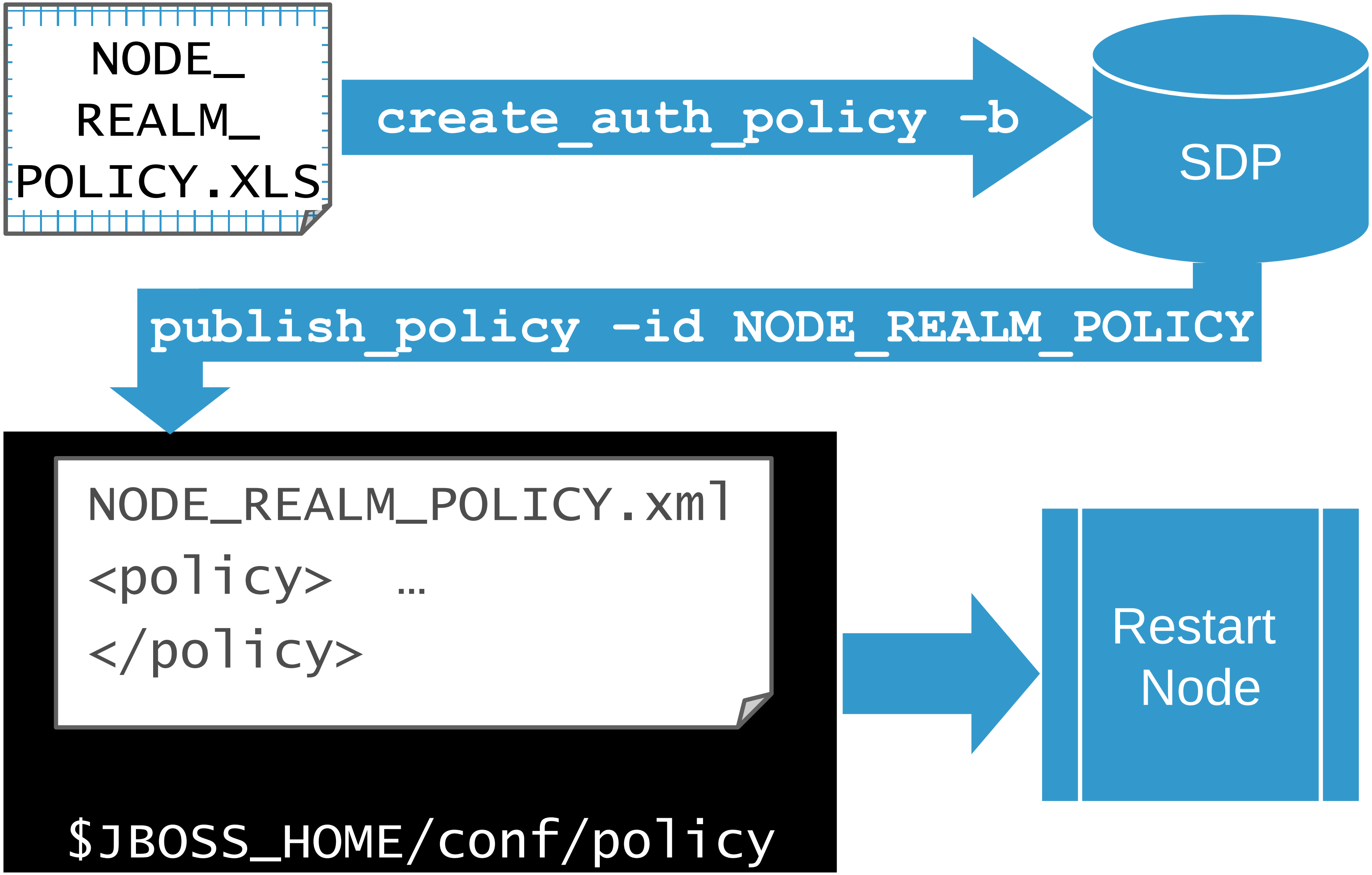
Create and store policy

Policy Details

Publish

Policy Name:	UPM_UPSEC_WEB
Node Class:	
Node Name:	

Publishing a Policy – mShell



NODE_
REALM_
POLICY.XLS

```
create_auth_policy -b
```

SDP

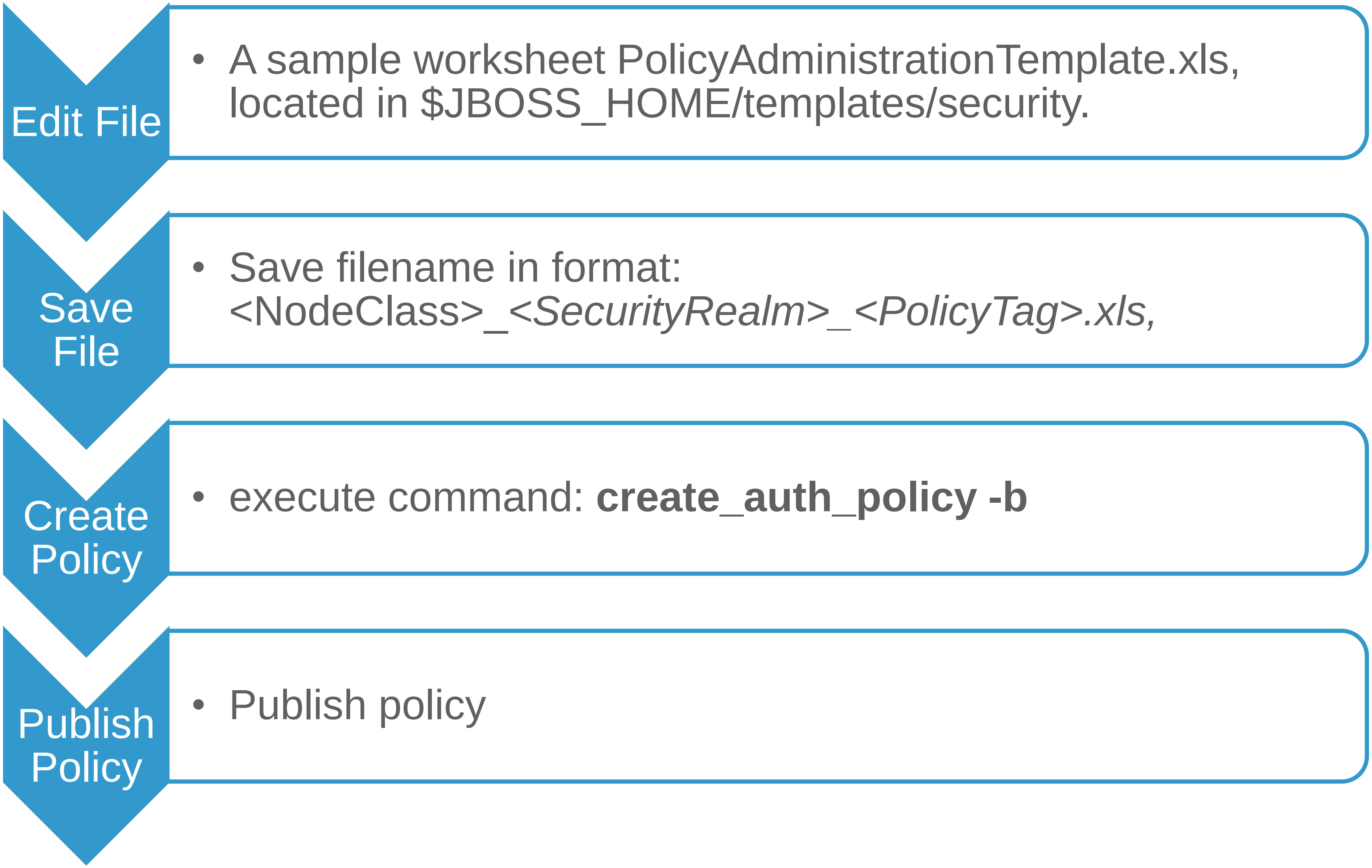
```
publish_policy -id NODE_REALM_POLICY
```

```
NODE_REALM_POLICY.xml
<policy>  …
</policy>
```

$JBOSS_HOME/conf/policy

Restart
Node

Bulk Policy Operations



Edit File

- A sample worksheet PolicyAdministrationTemplate.xls, located in $JBOSS_HOME/templates/security.

Save File

- Save filename in format: <NodeClass>_*<SecurityRealm>_<PolicyTag>.xls,*

Create Policy

- execute command: **create_auth_policy -b**

Publish Policy

- Publish policy

Policy Implementation – XACML

Extensible Access Control Markup Language (XACML)

- Standard governed by Organization for the Advancement of Structured Information Standards (OASIS).
- XML based
- Defines:
  - Policy Control Language
  - Request/Response Language
  - Runtime Architectural Components

Review Questions

1. In a rule definition, what are possible values of the Subject field?
   a. Data , service, system component
   b. Allow/deny
   c. Read, write, create
   d. Role names
2. A policy is defined in a scope of:
   a. Realm
   b. Realm Group
   c. Role
   d. Rule
3. Which of the following is true regarding a rule
   a. A rule can include one or more policies
   b. A policy can include one or more rules
   c. Rules can be associated to only one Realm
   d. Rules can be associated to only one role
4. Once you have finished editing a Policy, what must you do in order for the new policy to take effect?
   a. All application must re-authenticate.
   b. Publish the new policy to all currently connected applications
   c. Publish the new policy to all Comverse ONE nodes.
   d. Publish the new policy to all relevant Comverse ONE nodes.

Agenda

The Unified Platform

Security Overview

Using the Unified Platform Manager

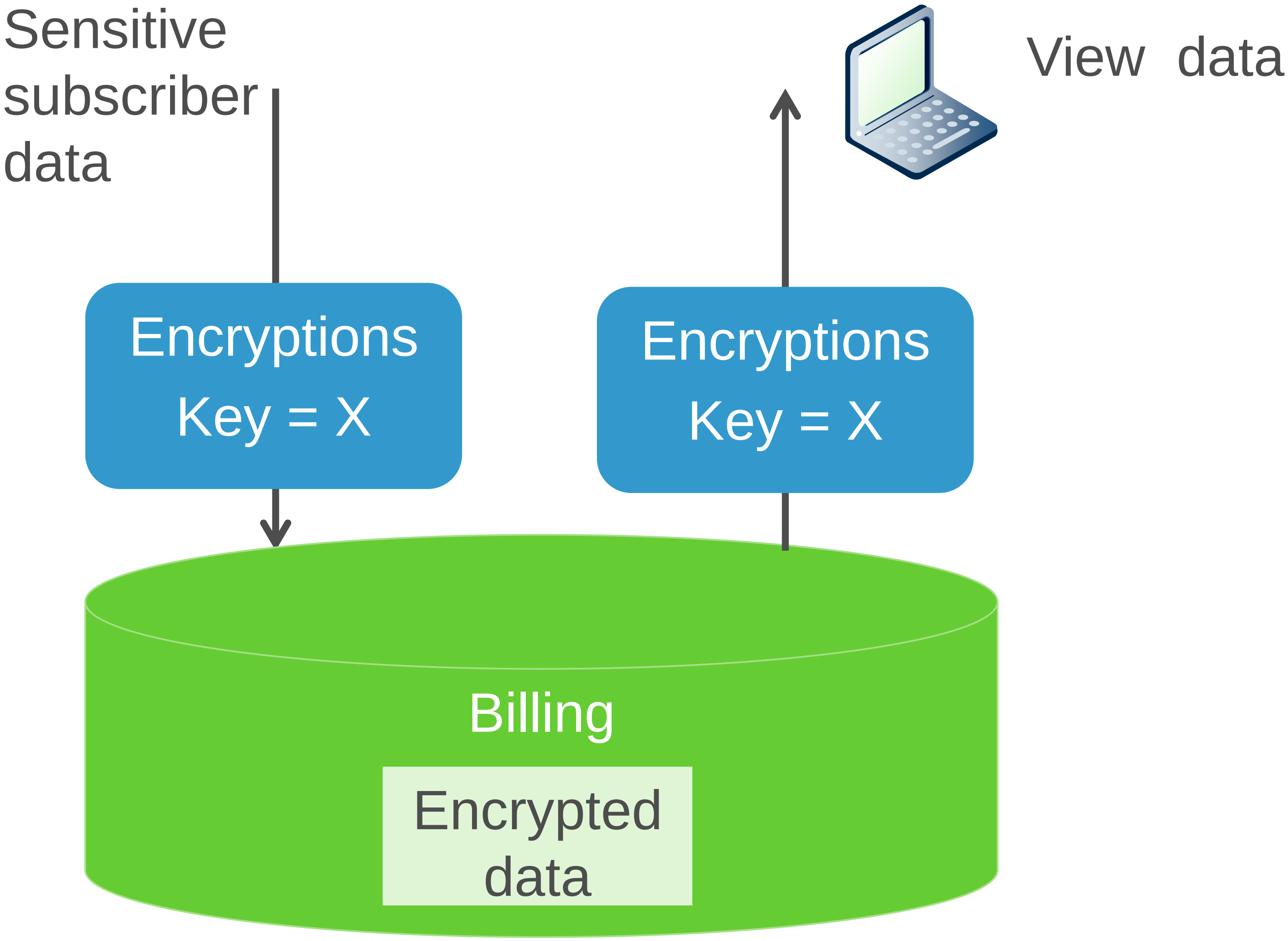
Identity Management

Policy Management

Key and Credential Management

Accounting and Audit

Keys



Sensitive subscriber data

View data

Encryptions

Key = X

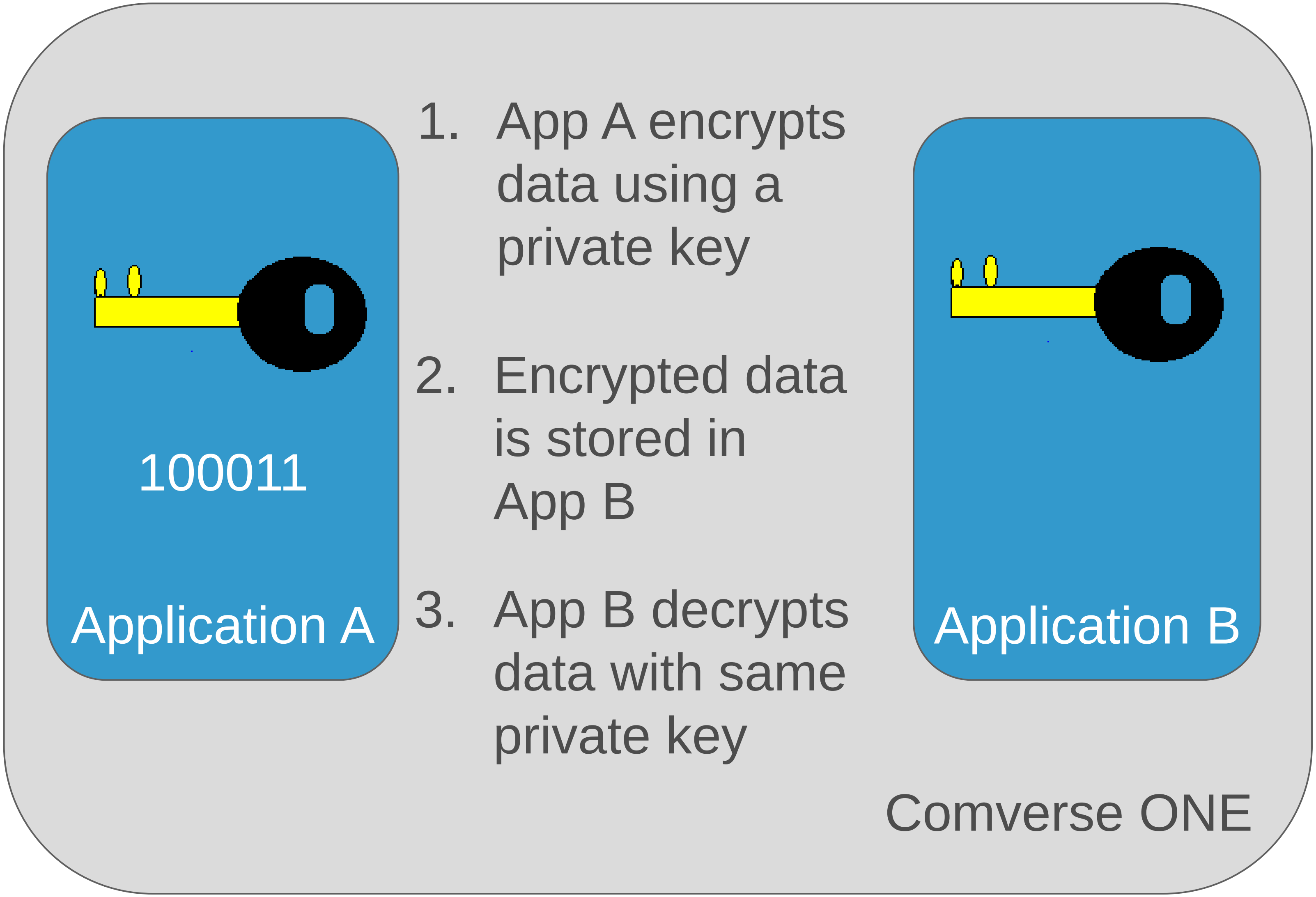
Encryptions

Key = X

Billing

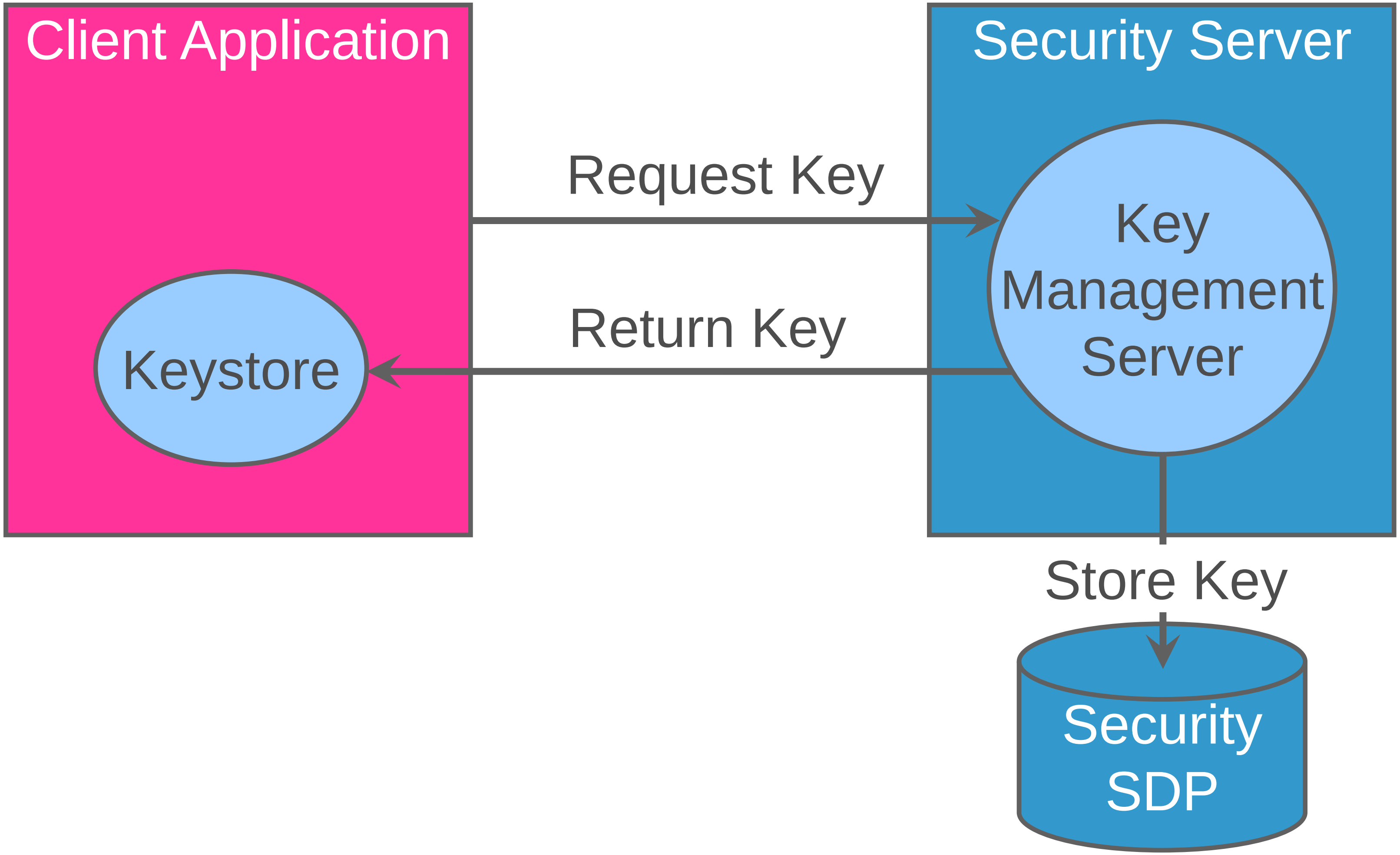
Encrypted data

Symmetric Key Process

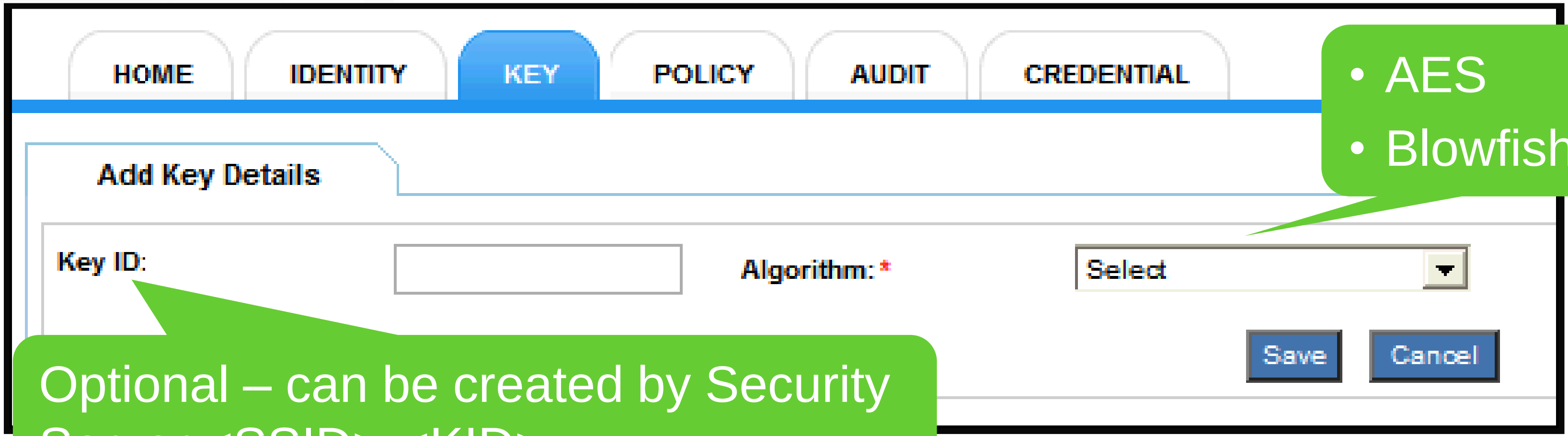


1. App A encrypts data using a private key
2. Encrypted data is stored in App B
3. App B decrypts data with same private key

Central Symmetric Key Management



Adding a Key



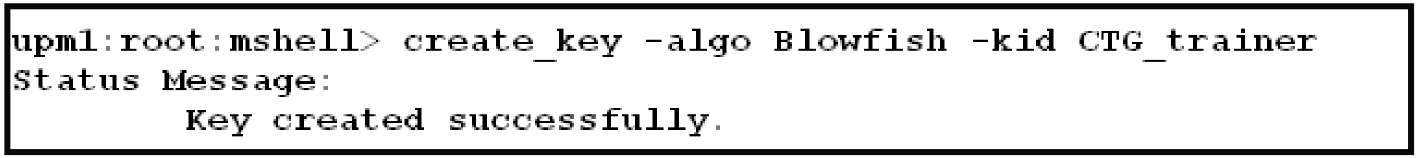
Add Key Details

Key ID:

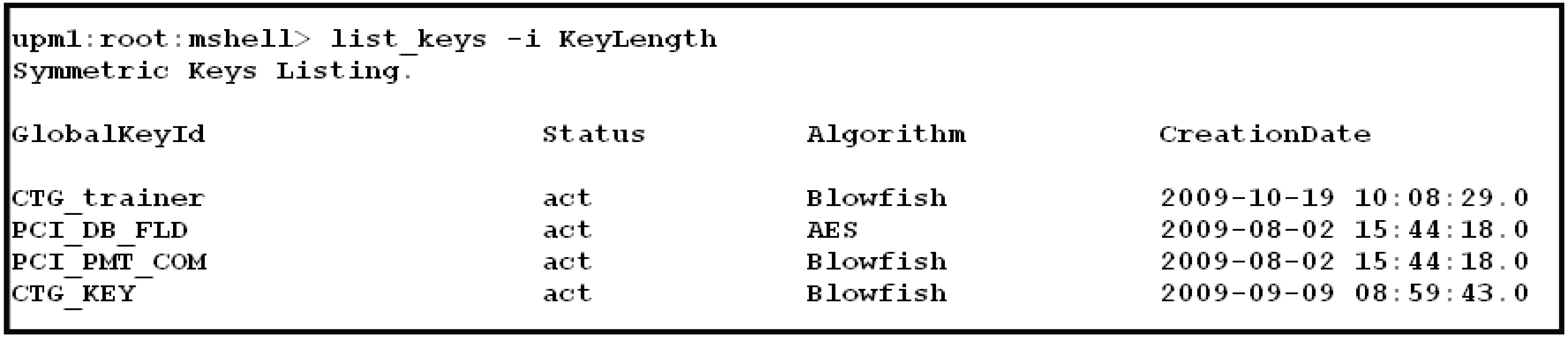
Algorithm:* Select

- AES
- Blowfish

Optional – can be created by Security Server <SSID>-<KID>



```
upml:root:mshell> create_key -algo Blowfish -kid CTG_trainer
Status Message:
        Key created successfully.
```

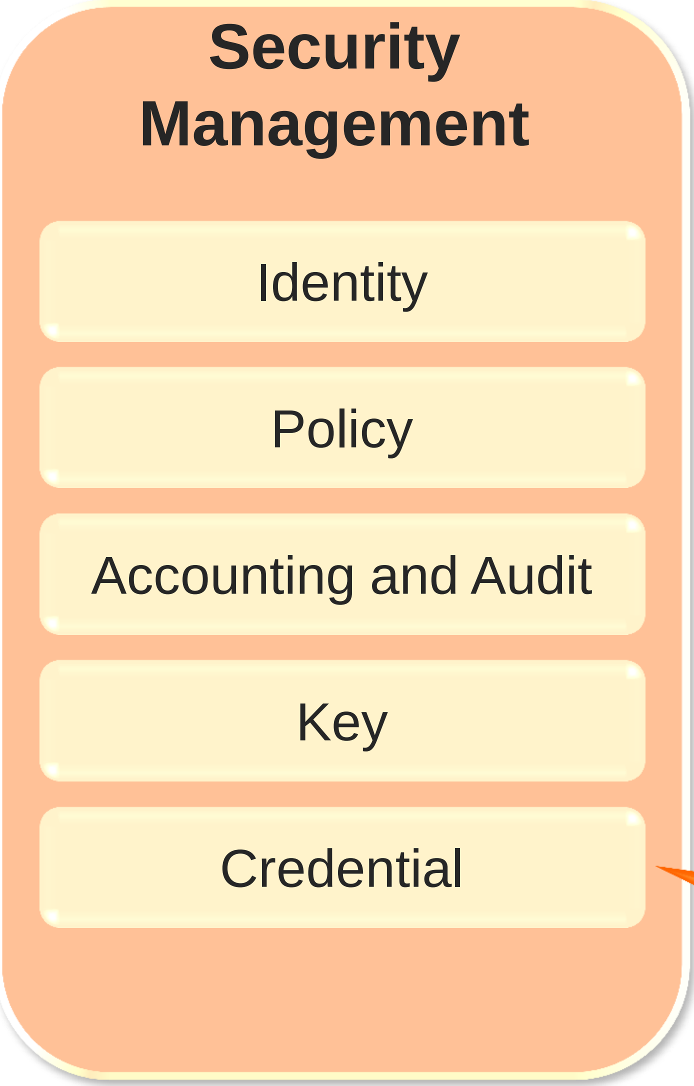


```
upml:root:mshell> list_keys -i KeyLength
Symmetric Keys Listing.

GlobalKeyId                  Status        Algorithm          CreationDate

CTG_trainer                  act           Blowfish           2009-10-19 10:08:29.0
PCI_DB_FLD                   act           AES                2009-08-02 15:44:18.0
PCI_PMT_COM                  act           Blowfish           2009-08-02 15:44:18.0
CTG_KEY                      act           Blowfish           2009-09-09 08:59:43.0
```

Credentials Management



Security Management

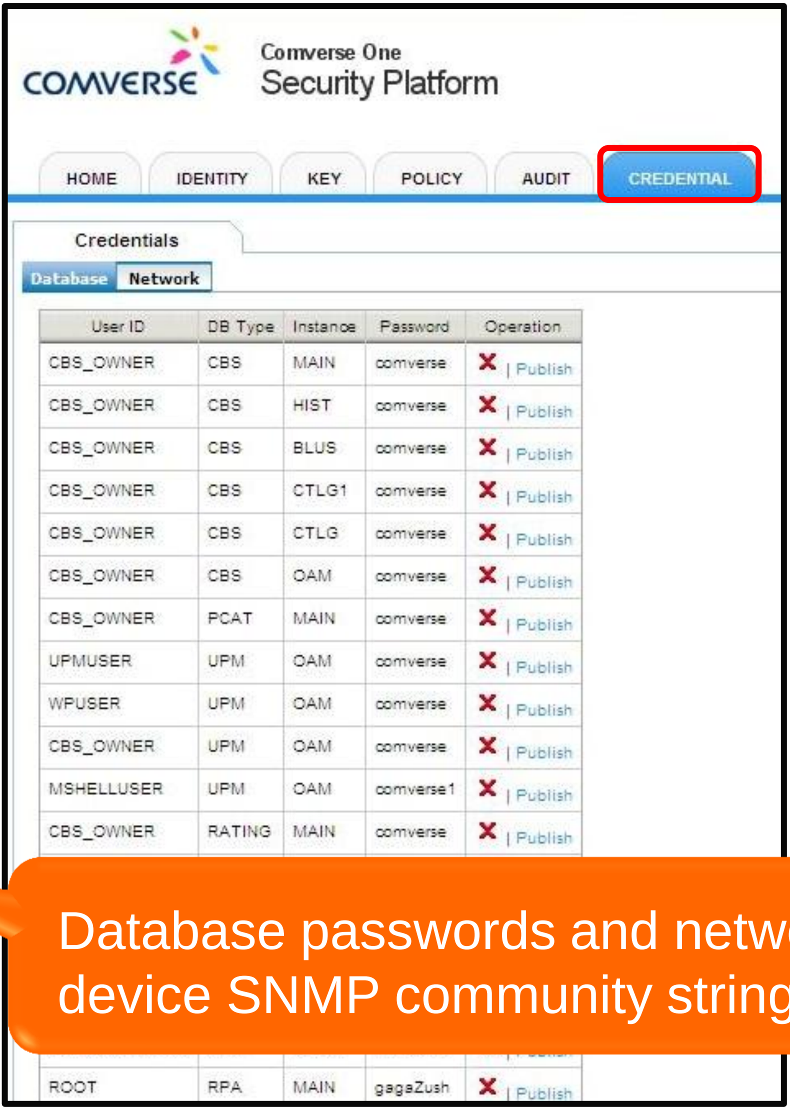
Identity

Policy

Accounting and Audit

Key

Credential



User ID	DB Type	Instance	Password	Operation
CBS_OWNER	CBS	MAIN	comverse	✗ | Publish
CBS_OWNER	CBS	HIST	comverse	✗ | Publish
CBS_OWNER	CBS	BLUS	comverse	✗ | Publish
CBS_OWNER	CBS	CTLG1	comverse	✗ | Publish
CBS_OWNER	CBS	CTLG	comverse	✗ | Publish
CBS_OWNER	CBS	OAM	comverse	✗ | Publish
CBS_OWNER	PCAT	MAIN	comverse	✗ | Publish
UPMUSER	UPM	OAM	comverse	✗ | Publish
WPUSER	UPM	OAM	comverse	✗ | Publish
CBS_OWNER	UPM	OAM	comverse	✗ | Publish
MSHELLUSER	UPM	OAM	comverse1	✗ | Publish
CBS_OWNER	RATING	MAIN	comverse	✗ | Publish
ROOT	RPA	MAIN	gagaZush	✗ | Publish

Database passwords and network-device SNMP community strings

Review Questions

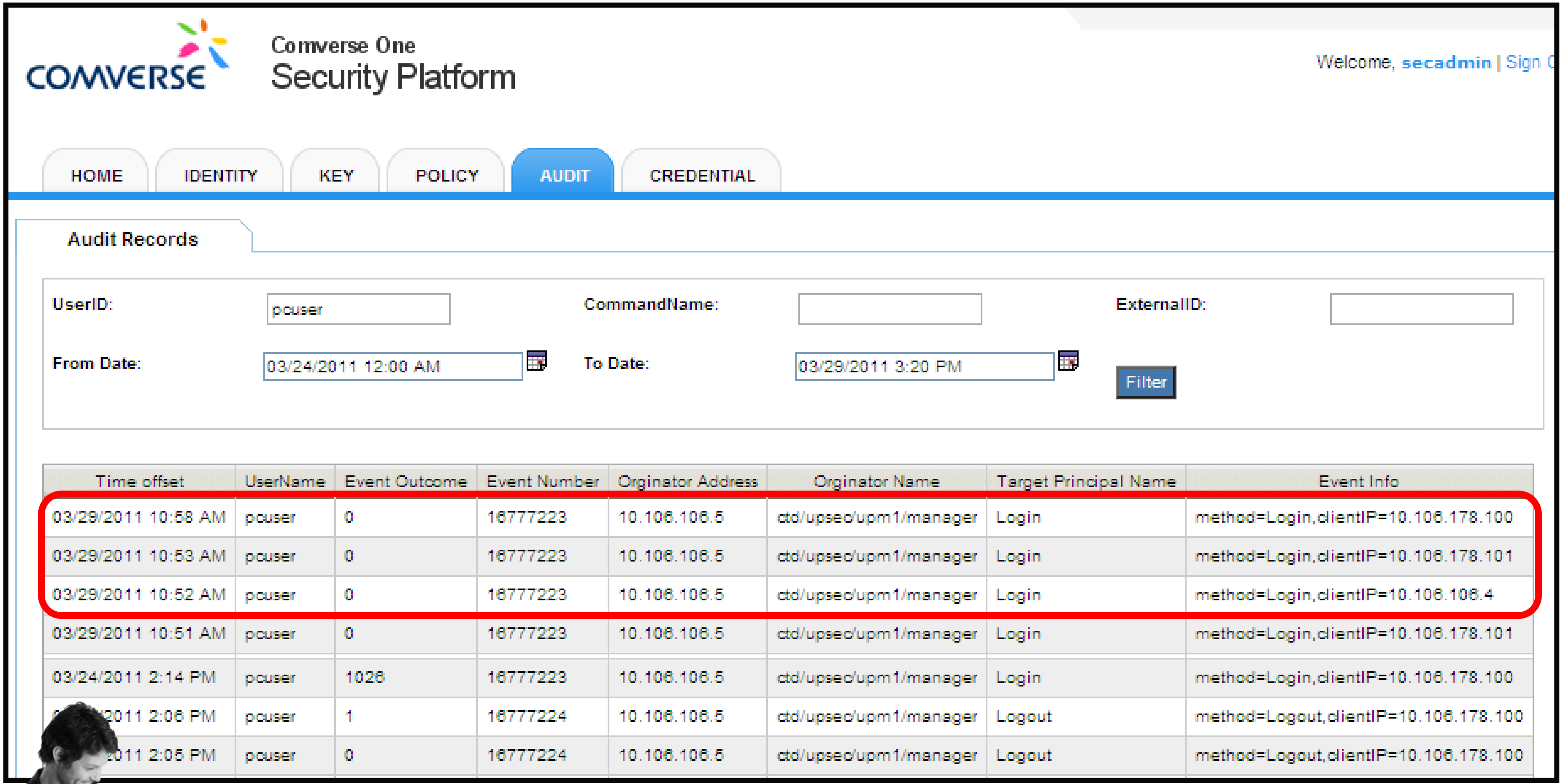
1. What are Keys used for?
   a. Allowing customer applications to perform sensitive actions
   b. Allowing customer applications to access sensitive data
   c. Encrypting sensitive data
2. How are Keys created? Which of the following is **NOT** true?
   a. By customer applications
   b. By the security server upon a customer application request
   c. Manually using the GUI
   d. Manually using the CLI

Agenda

- The Unified Platform
- Security Overview
- Using the Unified Platform Manager
- Identity Management
- Policy Management
- Key and Credential Management
- **Accounting and Audit**

Audit Management (1)

Account and Audit



Comverse One
Security Platform

Welcome, secadmin | Sign

UserID:	pcuser	CommandName:		ExternalID:	
From Date:	03/24/2011 12:00 AM	To Date:	03/29/2011 3:20 PM	Filter	

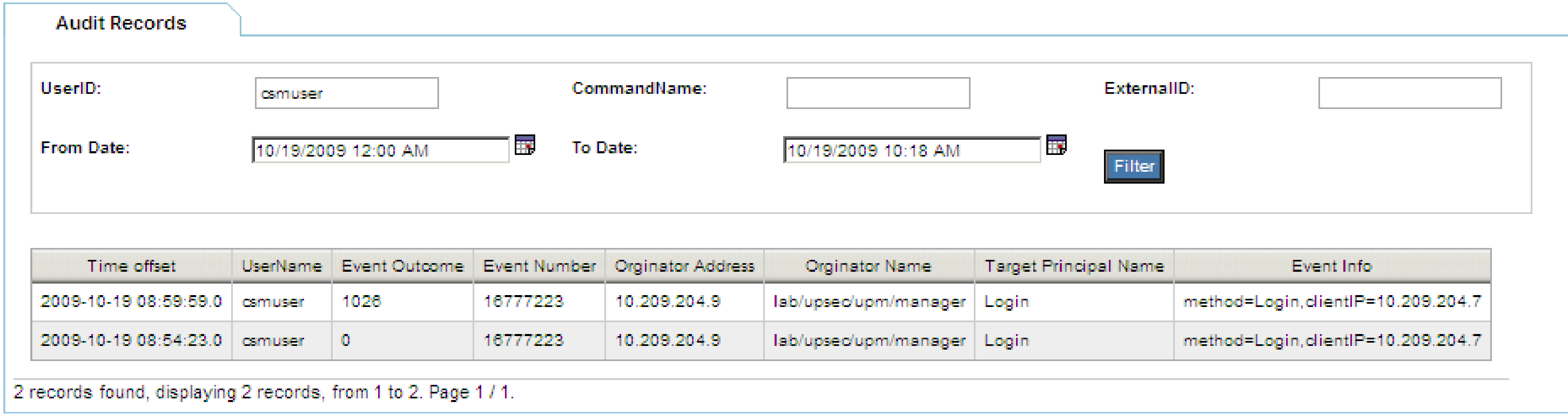
Time offset	UserName	Event Outcome	Event Number	Orginator Address	Orginator Name	Target Principal Name	Event Info
03/29/2011 10:58 AM	pcuser	0	16777223	10.106.106.5	ctd/upsec/upm1/manager	Login	method=Login,clientIP=10.106.178.100
03/29/2011 10:53 AM	pcuser	0	16777223	10.106.106.5	ctd/upsec/upm1/manager	Login	method=Login,clientIP=10.106.178.101
03/29/2011 10:52 AM	pcuser	0	16777223	10.106.106.5	ctd/upsec/upm1/manager	Login	method=Login,clientIP=10.106.106.4
03/29/2011 10:51 AM	pcuser	0	16777223	10.106.106.5	ctd/upsec/upm1/manager	Login	method=Login,clientIP=10.106.178.101
03/24/2011 2:14 PM	pcuser	1026	16777223	10.106.106.5	ctd/upsec/upm1/manager	Login	method=Login,clientIP=10.106.178.100
0[illegible]2011 2:06 PM	pcuser	1	16777224	10.106.106.5	ctd/upsec/upm1/manager	Logout	method=Logout,clientIP=10.106.178.100
[illegible]011 2:05 PM	pcuser	0	16777224	10.106.106.5	ctd/upsec/upm1/manager	Logout	method=Logout,clientIP=10.106.178.100

Management of the user activities that directly or indirectly affect financial data or controls

Audit Management (2)

- Distributed Audit Service (XDAS) specification
  - Record format
  - Event/event outcome codes
  - Client API
- Audit is enabled on each node at installation.
- Predefined audit record format
- Use **`build_report`** to view audit records.

Retrieving an Audit Report – GUI



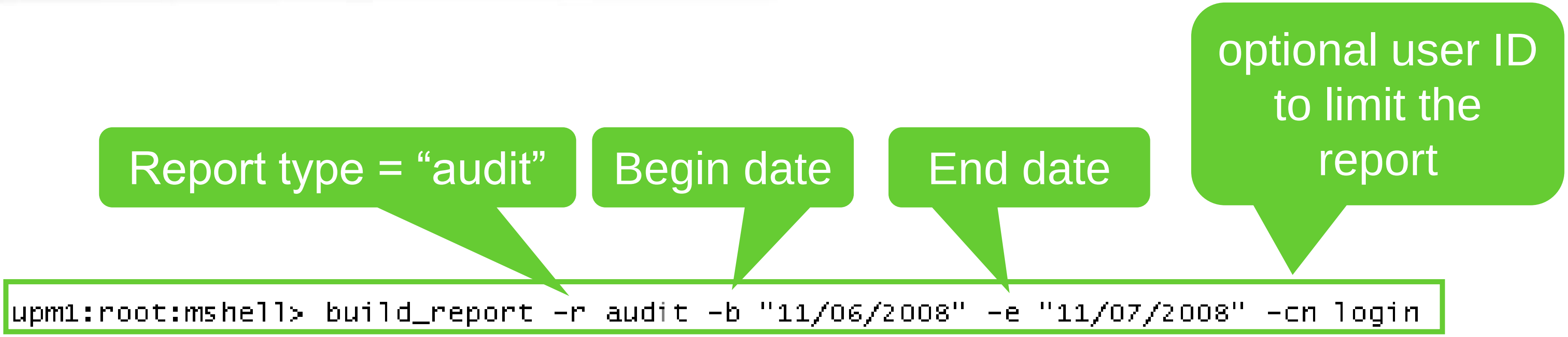
Audit Records

UserID:	csmuser	CommandName:		ExternalID:	
From Date:	10/19/2009 12:00 AM	To Date:	10/19/2009 10:18 AM	Filter	

Time offset	UserName	Event Outcome	Event Number	Orginator Address	Orginator Name	Target Principal Name	Event Info
2009-10-19 08:59:59.0	csmuser	1026	16777223	10.209.204.9	lab/upsec/upm/manager	Login	method=Login,clientIP=10.209.204.7
2009-10-19 08:54:23.0	csmuser	0	16777223	10.209.204.9	lab/upsec/upm/manager	Login	method=Login,clientIP=10.209.204.7

2 records found, displaying 2 records, from 1 to 2. Page 1 / 1.

Retrieving an Audit Report – mShell



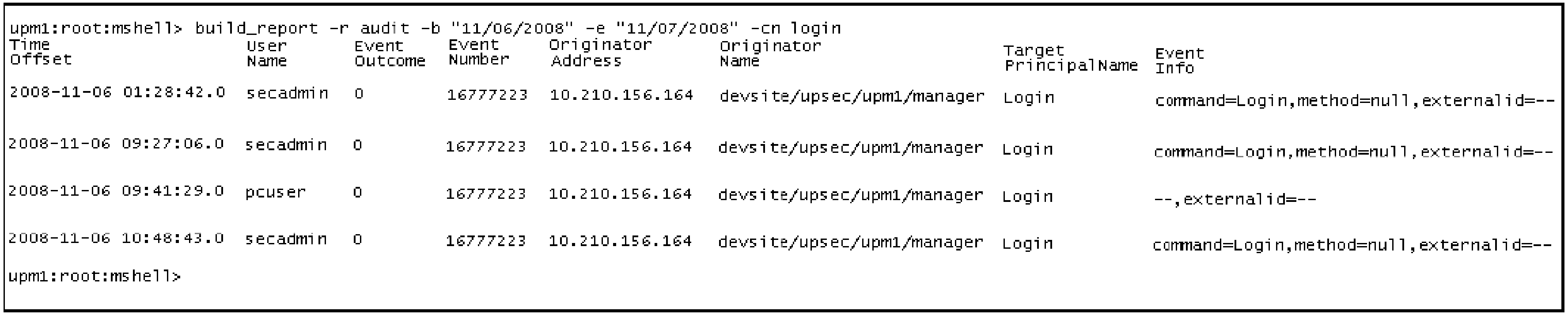
Report type = “audit”

Begin date

End date

optional user ID to limit the report

```
upm1:root:mshell> build_report -r audit -b "11/06/2008" -e "11/07/2008" -cn login
```



```
upm1:root:mshell> build_report -r audit -b "11/06/2008" -e "11/07/2008" -cn login
Time                   User       Event     Event     Originator       Originator                  Target         Event
Offset                 Name       Outcome   Number    Address          Name                        PrincipalName  Info

2008-11-06 01:28:42.0  secadmin   0         16777223  10.210.156.164   devsite/upsec/upm1/manager  Login          command=Login,method=null,externalid=--

2008-11-06 09:27:06.0  secadmin   0         16777223  10.210.156.164   devsite/upsec/upm1/manager  Login          command=Login,method=null,externalid=--

2008-11-06 09:41:29.0  pcuser     0         16777223  10.210.156.164   devsite/upsec/upm1/manager  Login          --,externalid=--

2008-11-06 10:48:43.0  secadmin   0         16777223  10.210.156.164   devsite/upsec/upm1/manager  Login          command=Login,method=null,externalid=--

upm1:root:mshell>
```

Purging Audit Records

- The amount of audit record depends on:
  - Database sizing and capacity
  - Organization’s requirements

- Audit record purging is handled by an automated job called purge_audit.

Summary

This lesson has covered the security capabilities of the UPM:

- Identity management
- Policy management
- Auditing
- Credentials
- Encryption keys