Oracle® Fusion Middleware

Administrator's Guide for Oracle Privileged Account Manager

11*g* Release 2 (11.1.2)

E27152-02

August 2012

ORACLE

Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager, 11g Release 2 (11.1.2)

E27152-02

Primary Author: K. C. Francis

Contributor: Buddhika Kottahachchi, Arun Theebaprakasam, An Li, Olaf Stullich, Fannie Ho, Vishal Mishra, Himanshu Sharma, Trish Fuzesy, and Mark Wilcox

Contents

6 Managing Oracle Privileged Account Manager Auditing and Logging

B Working with Oracle Privileged Account Manager's RESTful Interface

C Troubleshooting Oracle Privileged Account Manager

Glossary

Index

Preface

Welcome to *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*. This document provides information about how to use and administer Oracle Privileged Account Manager in an enterprise infrastructure.

Audience

The *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager* is intended for Oracle Privileged Account Manager administrators who can configure connections to target systems and client applications, access passwords for target systems, and who can create roles and assign users to those roles.

Administrators must be familiar with either the UNIX operating system or the Microsoft Windows operating system to understand the command-line syntax and examples in this document. You also must be familiar with the Lightweight Directory Access Protocol (LDAP).

This book is also intended for Oracle Privileged Account Manager end-users who do not have administrative privileges, but who are authorized to check privileged accounts in and out.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Websites in Documentation

This documentation may contain links to websites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these websites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Identity Manager 11*g* Release 2 (11.1.2) documentation set:

- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Release Notes for Oracle Identity Management*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware Reference for Oracle Identity Management*
- *Oracle Fusion Middleware Application Security Developer's Guide*
- *Oracle Identity Manager Connector Concepts*
- *Oracle Identity Manager Connector Guide for Database User Management*
- *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Security Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Oracle WebLogic Scripting Tool*
- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*
- *Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server*
- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide?

This chapter introduces the new features of Oracle Privileged Account Manager and provides pointers to additional information.

New Features for 11*g* Release 2 (11.1.2)

Oracle Privileged Account Manager 11*g* Release 2 (11.1.2) includes the following features:

- Account lifecycle management, which enables you to manage the lifecycle of account and application credentials stored in the Credential Store Framework (CSF).

  See Section 1.2.4, "Oracle Privileged Account Manager-Managed CSF Credentials" for more information.

- An authentication and authorization framework that includes
  - Oracle Platform Security Services (OPSS) authorization for Oracle Privileged Account Manager resources, such as targets and accounts
  - Oracle WebLogic Server (WLS) authentication with identity propagation through OPSS Trust
  - Common Admin Roles for Oracle Privileged Account Manager administrators and user managers

  See Chapter 2, "Understanding Oracle Privileged Account Manager Security" for more information.

- A web-based user interface provided by the Oracle Identity Navigator product, a command line tool, and REST APIs that you can use to perform various tasks in Oracle Privileged Account Manager. The web-based interface provides access to
  - An administration user interface for configuring and managing targets, privileged accounts, password policies, and usage policies.
  - A self-service user interface that enables users with or without administrative privileges to check-in and check-out accounts.

  See Chapter 3, "Getting Started with Administering Oracle Privileged Account Manager," Chapter 5, "Configuring and Managing Oracle Privileged Account Manager," and the appendices for more information.

Note: The command line tool messages and help are only provided in English. Globalization support for the Oracle Privileged Account Manager command line tool is not available for this release.

- Integration with the Identity Connector Framework (ICF), which enables Oracle Privileged Account Manager to interact with identity repositories on third-party systems.

  See "Deploying ICF Connectors in Oracle Privileged Account Manager" in Chapter 3, "Getting Started with Administering Oracle Privileged Account Manager" for more information.

- Oracle Privileged Account Manager logs audit events or state changes and provides generic logging, which includes debugging statements and exception messages.

  Oracle Privileged Account Manager audits all security events that occur under its purview, which enables you to monitor how privileged accounts are being used in your organization, while leveraging proven technology to manage sensitive information.

  See Chapter 6, "Managing Oracle Privileged Account Manager Auditing and Logging" for more information.

- Certification with Oracle Identity Manager request and approval workflow.

  See Chapter 7, "Configuring Oracle Privileged Account Manager for Integrated Solutions" for more information.

Part I

Understanding Oracle Privileged Account Manager

This part contains introductory and conceptual information about Oracle Privileged Account Manager, and it includes the following chapters:

1

Understanding Oracle Privileged Account Manager

This chapter introduces you to Oracle Privileged Account Manager. The topics in this chapter include

- Section 1.1, "What is Oracle Privileged Account Manager?"
- Section 1.2, "Why Use Oracle Privileged Account Manager?"
- Section 1.3, "How Oracle Privileged Account Manager is Deployed in Oracle Fusion Middleware"

1.1 What is Oracle Privileged Account Manager?

Oracle Privileged Account Manager manages *privileged accounts* that are not being managed by any other Oracle Identity Management components.

Accounts are considered "privileged," if they can access sensitive data, can grant access to sensitive data, or can both access and grant access to that data. Privileged accounts are your company's most powerful accounts and they are frequently shared.

Accounts come under Oracle Privileged Account Manager's purview if they are associated with elevated privileges, are used by multiple end-users on a task-by-task basis, and must be controlled and audited.

For example, these accounts require security and may fall under compliance regulations:

- UNIX root, Windows administrator, and Oracle Database SYSDBA system accounts
- Application accounts, such as the database user accounts used by an application server when it connects to a Human Resources application
- Traditional shared and elevated privilege user accounts, such as system administrators and database administrators

Administrators determine which accounts are privileged within a particular deployment, and they must configure Oracle Privileged Account Manager to manage those accounts.

While Oracle Privileged Account Manager most commonly manages shared and elevated privileged accounts, administrators can also use it to manage passwords for any type of account. For example, if an employee is on extended leave and you have a business reason for allowing another employee to access the system using that person's email account, Oracle Privileged Account Manager can manage that privilege.

1.2 Why Use Oracle Privileged Account Manager?

Oracle Privileged Account Manager enables you to administer and provide better security for privileged accounts and passwords that are traditionally difficult to manage for several reasons.

First, privileged accounts generally have more access rights than a regular user's account. Because these accounts are not typically associated with one specific employee, they are often difficult to audit with existing tools and processes. Consequently, when employees leave the company, they might retain privileged account passwords that are still in use, which is a very serious compliance and security issue.

Also, changing privileged account passwords on a regular basis is difficult. If many people depend on the account, changing the password and notifying everyone requires a coordinated effort.

Finally, you typically do not want to store passwords in a central or well-known location, such as an external repository (like LDAP) or in application configuration files, because you cannot control access to those passwords.

Oracle Privileged Account Manager delivers a complete solution for securely managing privileged accounts and passwords because it provides

- Centralized password management for privileged and shared accounts, including UNIX and Linux root accounts, Oracle Database SYSDBA, application accounts, and LDAP admin accounts
- Interactive, policy-based account *check-out* and *check-in*

  Oracle Privileged Account Manager requires all authorized users to check out an account before using it, and then to check that account back in when they are finished with it. Oracle Privileged Account Manager audits account check outs and check ins by tracking the real identity (the person's name) of every shared administrator user at any given moment in time. By using this information, Oracle Privileged Account Manager can provide a complete audit trail that shows who accessed what, when, and where.
- Automatic password changes using the Identity Connector Framework (ICF)

  Oracle Privileged Account Manager modifies passwords when they are checked out and checked in (when configured to do so). Consequently, when a user checks out a password and then subsequently checks it back in, that user can no longer use the previously checked out password.

  In addition, Oracle Privileged Account Manager can change application privileged account passwords at specified intervals, such as every 90 days, with no changes to those applications and Oracle Privileged Account Manager synchronizes those passwords on the target systems. For example, Oracle Privileged Account Manager can update service and scheduled task credentials.
- User and group management and workflow integration using Oracle Identity Manager

1.2.1 Features

Oracle Privileged Account Manager's key features include:

- Multiple access points, including the Oracle Privileged Account Manager web-based user interface (called the Console), RESTful APIs, and Oracle Privileged Account Manager's command line tool (CLI)

Oracle Privileged Account Manager's simple RESTful APIs can access Oracle Privileged Account Manager functionality from applications and scripts.

- Administrator and Self-Service user interfaces that are accessed from Oracle Privileged Account Manager's web-based user interface
- Integration with Oracle technologies, including
  - Oracle Platform Security Services (OPSS) Policy Store for storing metadata and authorizing functionality
  - **Oracle Platform Security Services (OPSS) Trust Service** to authenticate and propagate identities from the Oracle Privileged Account Manager user interface to the Oracle Privileged Account Manager server
  - **Credential Store Framework (CSF)** to securely store passwords to target systems and privileged accounts, and to enable regular updates to application privileged account passwords for compliance, with no changes to applications running in Oracle WebLogic Server (WLS)
  - **Identity Connector Framework** (ICF) to connect to targets and to discover, update, or discover and update the passwords for privileged accounts on those systems
  - **Oracle Wallet** to manage public key security
- Support for multiple target types; including operating systems, databases, LDAP directories, and Oracle Fusion Middleware applications

  In addition, because ICF is an open standard, you can write your own connectors against other types of targets for which Oracle has not yet created an ICF connector.

  For more information about ICF and about developing your own connector, see "Understanding the Identity Connector Framework" and "Developing Identity Connectors Using Java" or "Developing Identity Connectors Using .Net" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
- Advanced reporting capabilities
  - Oracle Privileged Account Manager's out-of-the box audit reports are integrated with Oracle Business Intelligence Publisher 11g (BI Publisher) so you know who is using your privileged accounts. BI Publisher also enables you to create and manage formatted reports from different data sources.
  - The Oracle Fusion Middleware Audit Framework logs audit events in a centralized database. Oracle Privileged Account Manager uses these events to generate audit reports.
  - Events related to privileged account access roll up into Oracle Identity Manager and Oracle Identity Analytics for audit and attestation.
- Policy-driven access to privileged accounts
- Ability to manage *attended* (a person is present) and *unattended* (no person is present) accounts

  An unattended account, also called a *service account,* is an account that Oracle Privileged Account Manager uses when it connects to a target system. For example, this is the account and password you must provide when adding and registering a new target system.

  Oracle Privileged Account Manager uses service accounts to perform all Oracle Privileged Account Manager-related operations (such as discovering accounts,

resetting passwords, and so forth) on that system, which is why service accounts must have some special privileges and properties. End users are not expected to ever use service accounts.

1.2.2 Functionality

In addition to the functionality described in Section 1.2, "Why Use Oracle Privileged Account Manager?," Oracle Privileged Account Manager

- Associates privileged accounts with targets
- Grants users and roles access to privileged accounts, and removes that access
- Provides role-based access to passwords maintained in the Oracle Privileged Account Manager password request system
- Provides password check out and check in to control access to accounts
- Eliminates the potential of having unmanaged privileged accounts when your unattended applications use client-certificate authentication
- Resets passwords to a random value on check in and check out by default

  You can configure Oracle Privileged Account Manager to automatically check in privileged accounts after a specified time to protect against users who check out that privileged account and do not bother to explicitly check in the account.

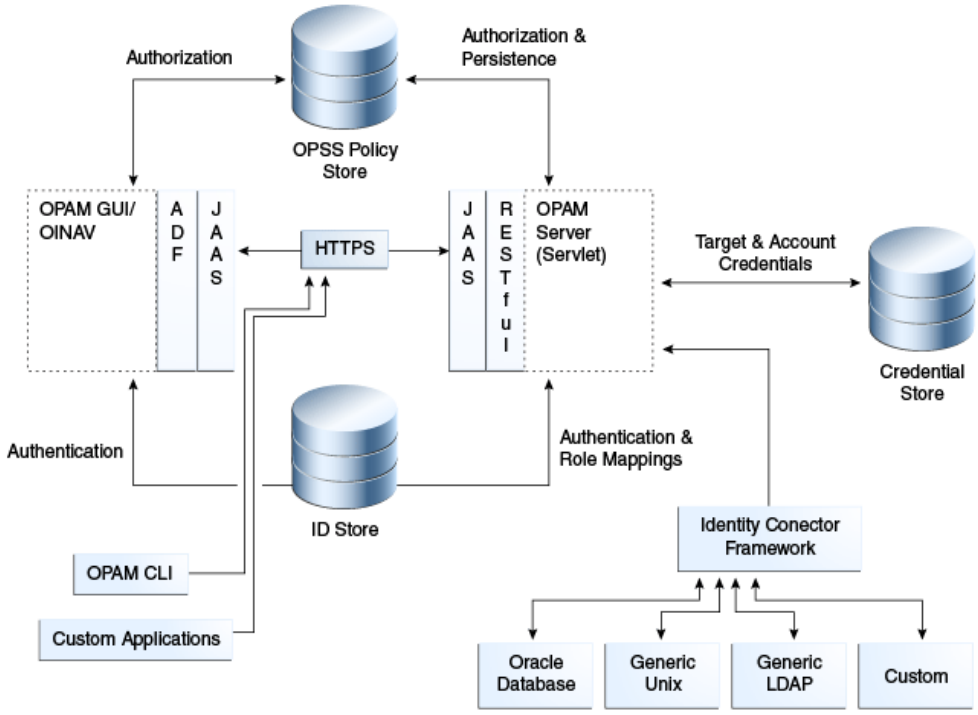
  You can also constrain how long users can check out a privileged account.
- Manages password resets on supported targets
- Makes authorization decisions to determine
  - Which targets, privileged accounts, and policies are exposed to an end user or administrator
  - Which operations (add, modify, check-in, and check-out) end users and administrators can perform
- Associates policies with privileged accounts
- Performs and supports Create, Read, Update, Delete, and Search (CRUDs) operations on targets, privileged accounts, and policies

  This core functionality is exposed through Oracle Privileged Account Manager's RESTful APIs. Check ins, check outs, and so forth are also supported through the RESTful interface.
- Uses Oracle's common auditing, logging, and reporting to monitor and report access
- Oracle Privileged Account Manager offers multiple high availability capabilities

1.2.3 Architecture and Topology

The following diagram illustrates Oracle Privileged Account Manager's architecture and topology:

Figure 1–1 Oracle Privileged Account Manager Architecture and Topology



As you examine this figure, it is important to note the following points:

- All of Oracle Privileged Account Manager's core logic resides on the Oracle Privileged Account Manager server. This functionality is exposed through a Representational State Transfer (REST or RESTful) service, where the data is encoded as JavaScript Object Notation (JSON).

  Note: Oracle Privileged Account Manager provides a web-based user interface (known as the *Console*) in Oracle Identity Navigator and an Oracle Privileged Account Manager command line tool (CLI). Both interfaces are essentially clients of the Oracle Privileged Account Manager server.

  However, third parties can write their own clients, such as custom applications, by leveraging the open RESTful service. For more information, refer to Appendix B, "Working with Oracle Privileged Account Manager's RESTful Interface."

- Oracle Privileged Account Manager authentication relies on Java Authentication & Authorization Service (JAAS) support in WebLogic.

  Refer to "WebLogic Security Service Architecture" in *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server* for more information about JAAS support in WebLogic.

  For more information about Oracle Privileged Account Manager authentication, see Section 2.2, "Understanding Oracle Privileged Account Manager Authentication."

- All communication with, and between, Oracle Privileged Account Manager-related components (including Oracle Privileged Account Manager's Console, command-line interface, and server) occurs over SSL
- Oracle Privileged Account Manager relies on and transparently uses the ID Store, Policy Store, and Credential Store configured for the WebLogic domain in which Oracle Privileged Account Manager is deployed.

  All of the passwords needed by Oracle Privileged Account Manager at run time (such as passwords to target systems, transient passwords for accounts, and so forth), are stored in the Credential Store through the Credential Store Framework.

  Refer to Section 1.3, "How Oracle Privileged Account Manager is Deployed in Oracle Fusion Middleware" for more information.
- The Oracle Privileged Account Manager Console leverages, and is rendered by, Oracle Application Development Framework (ADF).

  For more information about ADF, refer to the following website:

  http://www.oracle.com/technetwork/developer-tools/adf/overview/index.html
- Oracle Privileged Account Manager connects to targets by using ICF connectors.

  For additional information, see "Understanding the Identity Connector Framework" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1.2.4 Oracle Privileged Account Manager-Managed CSF Credentials

The Credential Store Framework (CSF) is an OPSS component that primarily provides secure storage for credentials. For example, many applications use CSF as a mechanism for storing application credentials.

Oracle Privileged Account Manager enables administrators to identify account credentials to be secured, shared, audited, and managed. In addition, Oracle Privileged Account Manager supports account lifecycle management activities such as periodic password modification.

Though many application developers use CSF to store application credentials for required targets (such as RDBMS and LDAP), there are certain aspects about how CSF is used that can potentially be improved, including:

- Applications storing their credentials in CSF do not expect these credentials to be shared. Therefore, a given instance of CSF can have multiple references to the same credential. For example, multiple applications could be relying on the same physical credential and yet have multiple logical references.
- Periodically modifying application credentials is necessary to satisfy compliance and internal IT policy requirements. However, modifying credentials (on the target and thereafter the CSF reference) remains a manual task, which is further complicated by the fact that there may be multiple references to the same credential in CSF. So, you must change the password or credential on the target and then manually update *all* references to that password in CSF.

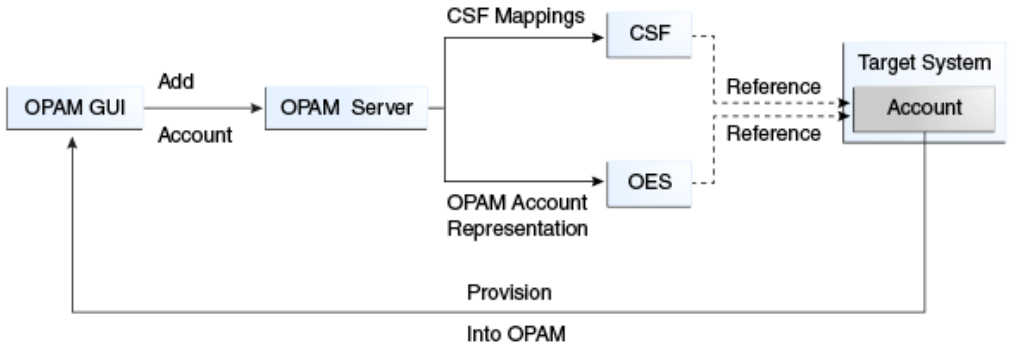
  Oracle Privileged Account Manager can automate this process, but automating the periodic modification of credentials is also complicated by the potential for multiple references that cannot be accurately traced.

Oracle Privileged Account Manager leverages its account lifecycle management feature to empower lifecycle management of application credentials stored in CSF.

1.2.4.1 Provisioning

If you decide that Oracle Privileged Account Manager will manage a particular account credential, then that credential must be provisioned through Oracle Privileged Account Manager. The following figure illustrates this provisioning process.

Figure 1–2 Oracle Privileged Account Manager Provisioning Process



The administrator

1. Adds an Oracle Privileged Account Manager target (if required).
2. Adds the Oracle Privileged Account Manager privileged account or credential to the target, which must include the necessary CSF mappings.

> **Note:** CSF mappings are the mechanism by which a specific credential instance is uniquely identified within CSF.

The Oracle Privileged Account Manager server stores the CSF mappings along with its representation of the Privileged Account. The Oracle Privileged Account Manager server creates instances of the credential in CSF that correspond to the provided mappings.

1.2.4.2 Lifecycle Management

An account provisioned as described in Section 1.2.4.1, "Provisioning" can have an associated Password Policy that governs password construction, periodic modification requirements, and so forth.

Oracle Privileged Account Manager normally honors and performs actions on the policy. However, whenever an administrator modifies an account credential that has associated CSF-mappings, Oracle Privileged Account Manager also updates the credential instances stored in CSF with those mappings. This update ensures that all relevant parties have access to the latest credential and allows the seamless management of password lifecycle events such as periodic modification.

1.2.4.3 Application Consumption

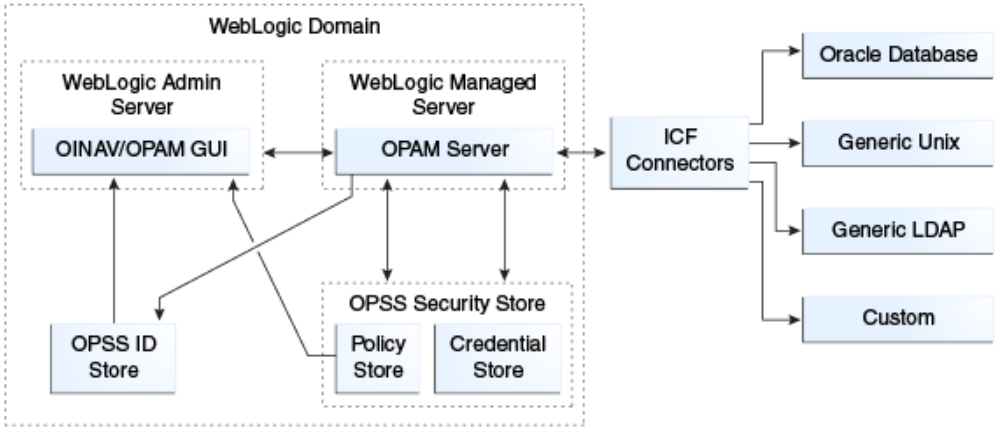
Using Oracle Privileged Account Manager to manage an application's credentials places no additional burden on that application. The only process change that occurs is that the credential must first be provisioned through Oracle Privileged Account Manager into Oracle Privileged Account Manager and CSF.

Oracle Privileged Account Manager pushes the credential to CSF with the administrator-provided mappings. If those mappings remain constant, the application can continue to access the credentials directly through CSF.

1.3 How Oracle Privileged Account Manager is Deployed in Oracle Fusion Middleware

The following figure illustrates how Oracle Privileged Account Manager is deployed within Oracle Fusion Middleware.

Figure 1–3 Oracle Privileged Account Manager Deployed Within Oracle Fusion Middleware



As you examine this figure, note the following points:

- All components are deployed within a single WebLogic domain.
- Oracle Identity Navigator and the Oracle Privileged Account Manager web-based user interface are both deployed in the WebLogic Admin Server.
- The OPSS ID Store and the OPSS Security Store (which includes the Policy Store and Credential Store) are WebLogic domain-wide constructs, so there is one of each per domain.

  Oracle Privileged Account Manager simply works with what is configured for that domain. You are not required to use an Oracle Privileged Account Manager-specific configuration to use these constructs and services. In addition, Oracle Privileged Account Manager abstracts out the use of these constructs and services so that you do not have to understand what goes on "under the covers" in great detail.

  – The OPSS ID Store can point to the LDAP embedded in WebLogic (out of the box) or to an external LDAP server.

    Refer to "Configuring the Identity Store Service" in the *Oracle Fusion Middleware Application Security Guide* for configuration instructions.

  – The OPSS Security Store can point to an XML file based store (out of the box), to an external RDBMS, or to an external LDAP server.

    Refer to "Configuring the OPSS Security Store" in the *Oracle Fusion Middleware Application Security Guide* for configuration instructions.

– For information about managing the Policy Store and the Credential Store, see "Managing the Policy Store" and "Managing the Credential Store" in the *Oracle Fusion Middleware Application Security Guide*.

2

Understanding Oracle Privileged Account Manager Security

This chapter describes how Oracle Privileged Account Manager authenticates and authorizes different types of users by using the authentication and authorization framework provided in the Oracle Privileged Account Manager server.

In addition, this chapter explains various methods that you can use to further secure Oracle Privileged Account Manager in your deployment environment.

The topics include:

2.1 Overview

The authentication and authorization framework provided in the Oracle Privileged Account Manager server provides the following features and functionality:

- Supports OPSS-Trust tokens and HTTP-Basic Authentication

  You can also configure the Oracle Privileged Account Manager user interface to work alongside Oracle Single Sign-On (SSO).

- Leverages the Java Authentication & Authorization Service (JAAS) for authentication

  Note: Oracle Privileged Account Manager authentication relies on JAAS support in WebLogic. Refer to "WebLogic Security Service Architecture" in *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server* for more information.

- Defines different Oracle Privileged Account Manager-specific Admin Roles and their Oracle Privileged Account Manager-specific responsibilities
- Enforces authorization decisions that determine
  - Which targets and privileged accounts are exposed to an administrator or to an end-user

  - Which operations (such as add, modify, check-in, and check-out) an end-user or an administrator can perform on targets, privileged accounts, and policies

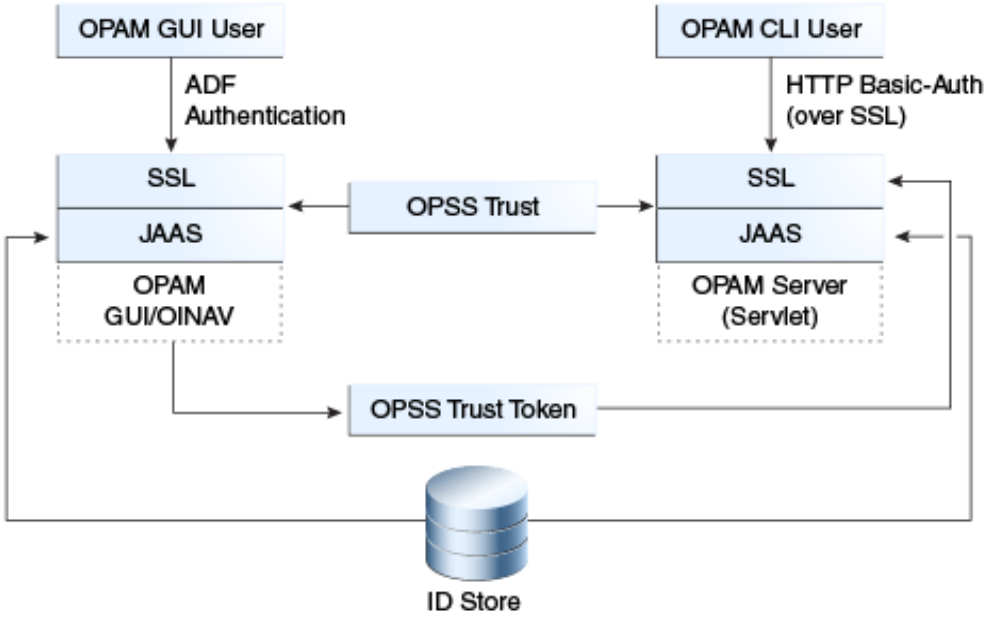
- Supports Usage Policies and Password Policies for privileged accounts

2.2 Understanding Oracle Privileged Account Manager Authentication

SAML-based token authentication is provided by using the OPSS trust service in WebLogic Server. The OPSS Policy Store stores all of the meta data required by the authorization decision engine.

The following figure illustrates Oracle Privileged Account Manager authentication.

Figure 2–1 Trust-Based Authentication in Oracle Privileged Account Manager



Trust Service instances are typically configured to securely propagate user identities from the client application to the Oracle Privileged Account Manager server as part of the Oracle Privileged Account Manager installation and configuration process.

Oracle Privileged Account Manager requires authentication when

- Users and clients interact with Oracle Privileged Account Manager's web-based user interface and Oracle Identity Navigator
- Users and clients interact directly with the Oracle Privileged Account Manager server

In both cases, Oracle Privileged Account Manager supports the following authentication modes, over SSL, out of the box:

- HTTP Basic-Authentication
- OPSS-Trust Service Assertions

In addition, Oracle Privileged Account Manager and Oracle Identity Navigator can support ADF-based authentication for UI-based interactions, which is done transparently against the domain-specific ID Store.

2.2.1 Authentication for the Oracle Privileged Account Manager Graphical User Interface

The Oracle Privileged Account Manager web-based user interface, or *Console*, supports the same authentication mechanisms as Oracle Identity Navigator and you can configure the interface with Oracle Single Sign-On (SSO).

When a user interacts with the Oracle Privileged Account Manager Console and Oracle Identity Navigator, the following occurs:

> **Note:** Oracle Privileged Account Manager administrators and users will probably never have to use the Oracle Identity Navigator interface except during the initial set-up of Oracle Privileged Account Manager.

1. The user authenticates against the Oracle Privileged Account Manager Console and Oracle Identity Navigator by using ADF authentication.
2. The Oracle Privileged Account Manager Console and Oracle Identity Navigator call the OPSS-Trust Service to request a token that asserts the identity of the user logged into the Oracle Privileged Account Manager Console.
3. Now, whenever the Oracle Privileged Account Manager Console and Oracle Identity Navigator make RESTful calls to the Oracle Privileged Account Manager server to execute Oracle Privileged Account Manager functionality, the Oracle Privileged Account Manager Console and Oracle Identity Navigator present the generated token to the Oracle Privileged Account Manager server.
4. Because the OPSS Trust Service Asserter is configured by default, the Asserter examines the token presented in the previous step, validates the token, and then asserts that the identity performing the RESTful call against the Oracle Privileged Account Manager server is the one contained in the token.

   This process is called *identity propagation*. An end-user only authenticates against the Oracle Privileged Account Manager Console and Oracle Identity Navigator, but the Oracle Privileged Account Manager Console and Oracle Identity Navigator can securely convey to the Oracle Privileged Account Manager server the identity for which they are making a request.

   The important point to note about identity propagation is that it removes the need for end users to authenticate themselves against the Oracle Privileged Account Manager Console, Oracle Identity Navigator, and the Oracle Privileged Account Manager server.

> **Note:** If you deploy your own client applications against the Oracle Privileged Account Manager server, then you must have identity propagation. In such a context, it is recommended that you use OPSS-Trust Service based Identity Assertions. For more information, see the *Oracle Fusion Middleware Security Guide*.

2.2.2 Authentication for the Oracle Privileged Account Manager Server

The Oracle Privileged Account Manager server only exposes RESTful interfaces and supports HTTP-Basic Authorization or OPSS-Trust. In addition, the Oracle Privileged Account Manager server requires that all communication with that server occurs over an SSL-secured channel.

The Oracle Privileged Account Manager command line tool client uses HTTP Basic-Authentication over SSL to connect to, and authenticate against, the Oracle Privileged Account Manager server.

2.3 Understanding Oracle Privileged Account Manager Authorization

This section describes Oracle Privileged Account Manager authorization.

The topics include:

- Administration Role Types
- End Users

2.3.1 Administration Role Types

Common Admin Roles are a set of predefined, standardized application roles for securing administrative access to Oracle Identity Management applications. These roles encapsulate the common administrative tasks across the Oracle Identity Management suite.

> **Note:** For more information about Common Admin Roles, including the responsibilities of each role and the skills and expertise required to perform that role, see "Common Admin Roles" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

Oracle Privileged Account Manager uses Admin Roles to manage access to targets and privileged accounts and to control which operations administrators can perform. Specifically, the Oracle Privileged Account Manager server renders different user interface components based on the Admin Role assigned to the user logging in.

Only administrators who are assigned the Oracle Privileged Account Manager-specific Common Admin Roles can administer Oracle Privileged Account Manager.

> **Note:** Authorized administrators must configure and assign roles from the Administration tab in the Oracle Identity Navigator Console. Refer to "Configuring Enterprise Roles" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator* for detailed information.

The following table describes the Common Admin Roles that are specific to Oracle Privileged Account Manager.

Table 2–1 Supported Admin Roles

Admin Role	Access Rights
Application Configurator (OPAM_APPLICATION_CONFIGURATOR)	Configure Oracle Privileged Account Manager servers.
Security Administrator (OPAM_SECURITY_ADMIN)	▪ Manage targets (add, edit, and remove targets). ▪ Manage accounts (add, edit, and remove accounts). **Note**: This role cannot assign grantees to privileged accounts. ▪ Manage Password and Usage Policies (create, edit, and delete policies). ▪ Assign Password and Usage Policies to accounts. **Note**: This role can only apply a Usage Policy at the account level.
Security Auditor (OPAM_SECURITY_AUDITOR)	▪ Open and review Oracle Privileged Account Manager reports. ▪ View Oracle Privileged Account Manager Audit reports in the Oracle Identity Navigator Reports portlet.
User Manager (OPAM_USER_MANAGER)	▪ Assign end users with grants to privileged accounts. ▪ Manage Usage Policies (create, edit, and delete Usage Policies). ▪ Assign Usage Policies to grants. **Note**: The relationship between an account and a grantee (end user) of that account is called a *grant*. The User Manager can assign different Usage Policies to different grantees of the same account. This role cannot assign Password Policies to accounts.

After installation, the default administrator is the `weblogic` user (also known as the *bootstrap* user) who is a member of the Administrators group. You must use the `weblogic` user to create and assign users to the Oracle Privileged Account Manager Admin Roles described in Table 2–1. Those users can then perform the administration tasks described in this table.

Note: Although it is possible for the default administrator to assign all those roles to himself or herself, this is not typical.

After installation, you can use the `weblogic` user, as the bootstrap user, to map the users from the domain identity store to the Oracle Privileged Account Manager Common Admin Roles detailed in Table 2–1. Users mapped to the Security Administrator role can assign the Common Admin Roles to other users, and can later replace the `weblogic` user in your environment. After you complete the initial user mapping, replace the default administrator user by mapping the Security Administrator role to at least one administrator user defined in your domain identity store.

2.3.2 End Users

Oracle Privileged Account Manager End Users or Enterprise Users are not assigned any roles, so they have limited access to Oracle Privileged Account Manager user interface components. These users are only entitled to perform certain tasks; which includes viewing, searching, checking out, and checking in privileged accounts for which they have been granted access.

Note: Refer to Section 5.2, "Working with Self-Service" for more information.

2.4 Securing Oracle Privileged Account Manager

You can implement the recommendations described in this section to further secure Oracle Privileged Account Manager in your deployment environment.

The topics include:

- Securing the Network Channel
- Securing Shared Accounts
- Enabling Password Resets
- Avoiding Assignments through Multiple Paths
- Defining Richer Password Policies

2.4.1 Securing the Network Channel

As part of its normal functionality, Oracle Privileged Account Manager performs remote password resets on target systems. Because these passwords allow access to those systems as privileged identities (Oracle Privileged Account Manager manages privileged accounts and identities) you must ensure that these remote password resets occur over a secured network channel.

After being reset, Oracle Privileged Account Manager propagates these passwords to end users who are requesting access to the target system as a privileged account. Again, you must ensure that these newly reset passwords are propagated to the end users over a secured channel.

Considering these points, there are two aspects of an Oracle Privileged Account Manager deployment that must be closely examined and secured:

- Connecting to Target Systems
- Securing the End User Interface

2.4.1.1 Connecting to Target Systems

Oracle Privileged Account Manager leverages ICF connectors to communicate with target systems. These connectors are highly flexible and they can be configured in several ways. To allow flexibility in testing (and even production), Oracle Privileged Account Manager does not mandate that this connectivity always occurs over a secure channel.

Except for the Generic UNIX targets, which mandates SSH, the Generic LDAP and Generic DB targets allow connections through both secured (encrypted) and clear channels. Therefore, it is important for an Oracle Privileged Account Manager administrator to consider all relevant factors when deciding what type of channel to use when connecting to target systems.

Oracle recommends always using secured channels to mitigate the risk of password compromise due to packet sniffing. If the target system (either LDAP or DB) supports SSL and is listening on an SSL port, then Oracle Privileged Account Manager can communicate with that target over SSL.

Consult your target systems' product documentation for information about configuring your targets so that they are listening on an SSL port. To configure Oracle

Privileged Account Manager to communicate through SSL, refer to Section 3.3.2, "Configuring SSL Communication in Oracle Privileged Account Manager." Securing these connections through SSL ensures that the password reset operations performed by Oracle Privileged Account Manager occur in a secure manner.

2.4.1.2 Securing the End User Interface

There are two primary interfaces open to an Oracle Privileged Account Manager end user:

- Console (see Section 3.4, "Navigating Oracle Privileged Account Manager's Console" for more information)
- Command line tool (see Appendix A, "Working with the Command Line Tool" for more information)

Oracle Privileged Account Manager's Console is hosted in Oracle Identity Navigator. However, Oracle Identity Navigator is also used for other purposes, so it can be deployed with SSL enabled or disabled.

If you deploy Oracle Identity Navigator with SSL disabled, even if Oracle Identity Navigator communicates with the Oracle Privileged Account Manager server over an SSL secured channel, then the connectivity between Oracle Identity Navigator (for example, the Oracle Privileged Account Manager Console) and the end user browser is not secured, which can cause security concerns.

Oracle recommends that if you use Oracle Identity Navigator to serve the Oracle Privileged Account Manager Console, you must deploy Oracle Identity Navigator in an SSL (*and only SSL*) -enabled mode.

Note: For more information about configuring SSL for Oracle Identity Navigator, see "Configuring Secure Socket Layer" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

Because the Oracle Privileged Account Manager server mandates SSL connectivity, the Oracle Privileged Account Manager command line tool always uses SSL and communicates over a secure channel. Consequently, when the Oracle Privileged Account Manager server propagates a password to an end user through the command line tool, it always uses a secured channel and prevents compromises from packet sniffing.

2.4.2 Securing Shared Accounts

Oracle Privileged Account Manager enables you to specify whether a privileged account is *shared* or *not shared*. This section defines shared accounts, explains some security considerations, and describes how to improve security for a shared account.

2.4.2.1 What is a Shared Account?

By default, Oracle Privileged Account Manager allows only one user to check out an account at a time. If a second user tries to check out an already checked-out account, an error message displays stating the account is already checked out.

Oracle Privileged Account Manager also enables you to configure a *shared* account, which enables multiple users to check out the account at the same time.

When multiple users check out a shared account, Oracle Privileged Account Manager shares the password generated by the first user instead of generating a new password for each user. (Setting a new password would affect the existing check out.) Oracle Privileged Account Manager does not reset that password until all users have checked in the account and the last person has checked in the password.

Oracle recommends that you designate an account as shared only if there are compelling business reasons to do so. For example, sharing a database account might be advantageous if that account that is being administered by multiple people.

2.4.2.2 Security Limitations

When you configure a shared account, keep in mind the following security limitations:

- Users can still use the password after checking in an account because Oracle Privileged Account Manager does not reset the password until the last user checks it in.
- Sharing accounts presents a problem with achieving a fine-grained audit. Oracle Privileged Account Manager can provide an audit trail that shows when the account was checked out and which users had access to that account at any given time. However, if multiple end users have the same privileged account checked out at the same time, then Oracle Privileged Account Manager cannot isolate the actions taken by an individual end user.

2.4.2.3 How to Secure the Account

If you do have a compelling reason for sharing an account, its useful to take the following steps to secure that account:

1. Configure the Usage Policy to automatically check-in the privileged account after a specified period of time. Automatic check-ins ensure that shared privileged accounts get checked-in and that passwords get cycled in a timely manner.
2. Limit the number of users to whom you assign the privileged account and try to further segregate these users by specifying when they can access the account. You can configure the Usage Policy to specify which days of the week and what times of the day a user can access an account. These limitations can minimize overlapping checkouts, which improves Oracle Privileged Account Manager's ability to audit.

> **Note:** For more information about configuring a Usage Policy, refer to Section 5.1.1.4, "Modifying the Default Usage Policy" or Section 5.1.1.6, "Creating a Usage Policy."

2.4.3 Enabling Password Resets

Oracle Privileged Account Manager allows you to configure the Password Policy for a privileged account so that Oracle Privileged Account Manager automatically resets the privileged account's password when the account is checked-out, checked-in, in both cases, or in neither case.

At a minimum, Oracle recommends that you configure and apply a Password Policy to reset the privileged account's password on check-in. Resetting the password on check-in prevents end users from using that account after checking it in because the password they used is no longer associated with that privileged account. This feature is one of the fundamental innovations in Oracle Privileged Account Manager and should be used.

Note: For more information about configuring and working with Password Policies, refer to Section 5.1.1, "Working with Policies."

2.4.4 Avoiding Assignments through Multiple Paths

In addition to directly assigning privileged accounts to end users, Oracle Privileged Account Manager allows you to assign privileged accounts to groups. For example, you might want to create a "Data Center Product UNIX Administrators" group and give that group access to certain privileged accounts.

When designing your deployment, it is important to ensure that a given end user is granted access to a privileged account through only one path (either directly or through a single group). When Oracle Privileged Account Manager discovers multiple grant paths, it picks the first path retrieved from its back-end, which leads to non-deterministic behavior. This behavior can cause the *effective* Usage Policy to be different from the *intended* Usage Policy.

Note: For more information about granting privileged accounts, see Section 5.1.4, "Working with Grantees."

2.4.5 Defining Richer Password Policies

The primary purpose of an Oracle Privileged Account Manager's Password Policy is to ensure the success of an Oracle Privileged Account Manager-initiated password reset that occurs against a target system.

At a minimum, Oracle Privileged Account Manager requires the effective Password Policy on a privileged account to describe the Password Policy being enforced on the target system. However, Oracle Privileged Account Manager administrators are not restricted to this requirement. You can define a much richer Password Policy in Oracle Privileged Account Manager that generates more complex and secure passwords during Oracle Privileged Account Manager reset operations.

Note: For more information about configuring and working with Password Policies, refer to Section 5.1.1, "Working with Policies."

Part II

Basic Administration

This part provides information about performing basic administration tasks for Oracle Privileged Account Manager, and it contains the following chapters:

- Getting Started with Administering Oracle Privileged Account Manager
- Adding and Managing an Oracle Privileged Account Manager Server
- Configuring and Managing Oracle Privileged Account Manager
- Managing Oracle Privileged Account Manager Auditing and Logging

3

Getting Started with Administering Oracle Privileged Account Manager

You can administer Oracle Privileged Account Manager from the Console and from the command line. This chapter describes how to perform basic administration tasks.

> **Note:** This chapter assumes you have installed and configured Oracle Privileged Account Manager as described in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
>
> Reading the "Configuring Oracle Privileged Account Manager" chapter in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* might be particularly helpful.
>
> In this guide, when you are instructed to start the Oracle WebLogic Administration Server (Admin Server) or various Managed Servers, refer to "Starting or Stopping the Oracle Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for instructions.

This chapter includes the following topics:

3.1 Getting Started after Installing 11*g* Release 2 (11.1.2)

After installing 11g Release 2, Oracle recommends:

- Reviewing Table 3–1 to understand the default application URLs for various interfaces that you use to manage Oracle Privileged Account Manager in this release:

Table 3–1 Default Application URLs

Interface	Default URL
Oracle Identity Navigator	http://*adminserver_host*:*adminserver_port*/oinav/
Oracle WebLogic Server Administrative Console	http://*adminserver_host*:*adminserver_port*/console/

Table 3–1 (Cont.) Default Application URLs

Interface	Default URL
Oracle Privileged Account Manager Console	http://*adminserver_host*:*adminserver_port*/oinav/opam
Oracle Privileged Account Manager Server	http://*managedserver_host*:*managedserver_port*/opam

- Reviewing Table 3–2 to understand various default ports for Oracle Privileged Account Manager in this release:

Table 3–2 Default Ports

Port Type	Default Port	Description
Oracle Privileged Account Manager	18102	Default SSL-enabled port for the WebLogic Managed Server where the Oracle Privileged Account Manager server is deployed. In a shiphome (such as an out-of-the-box environment) there are two WebLogic servers relevant to Oracle Privileged Account Manager: ■ The WebLogic Admin Server in the Oracle Privileged Account Manager domain runs Oracle Identity Navigator and the Oracle Privileged Account Manager Console. ■ An additional WebLogic Managed Server runs the Oracle Privileged Account Manager server.
WebLogic responds to SSL	7002	Default SSL-enabled port for the WebLogic Admin Server (where Oracle Identity Navigator and the Oracle Privileged Account Manager Console are deployed).

3.2 Deploying ICF Connectors in Oracle Privileged Account Manager

Oracle Privileged Account Manager enables you to secure, share, audit, and manage administrator-identified account credentials. To provide these capabilities, Oracle Privileged Account Manager must be able to access and manage privileged accounts on a target system.

Connectors enable Oracle Privileged Account Manager to interact with target systems, such as LDAP or Oracle Database, and to perform Oracle Privileged Account Manager-relevant administrative operations on those systems.

Oracle Privileged Account Manager leverages connectors that are compliant with the ICF standard.

This section describes how Oracle Privileged Account Manager consumes these ICF connectors. The topics include:

- About ICF Connectors
- Locating the Oracle Privileged Account Manager Connector Bundles
- Consuming ICF Connectors
- Adding New Connectors to an Existing Oracle Privileged Account Manager Installation

For more information about the Identity Connector Framework, refer to "Understanding the Identity Connector Framework" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3.2.1 About ICF Connectors

Oracle Privileged Account Manager ships with the following ICF-compliant connectors that were developed by Oracle:

- Database User Management (DBUM) Connector
- Generic LDAP Connector
- Oracle Identity Manager Connector for UNIX

These connectors enable Oracle Privileged Account Manager to manage privileged accounts on a range of target systems belonging to the preceding types.

Oracle Privileged Account Manager can also use customer-created, ICF-compliant connectors, which empowers you to manage your proprietary systems by using Oracle Privileged Account Manager.

For more information about the Identity Connector Framework, refer to "Developing Identity Connectors" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3.2.2 Locating the Oracle Privileged Account Manager Connector Bundles

Because ICF connectors are generic, and useful in numerous contexts, a given Oracle installation puts all connector bundles into a single location on the file system. All components (such as Oracle Privileged Account Manager) that rely on these connector bundles can access them from this location:

ORACLE_HOME/connectors

The connectors that are pushed into ORACLE_HOME/connectors are actually shipped with Oracle Identity Manager. Of all the connectors in this directory, only the following three connectors are certified with Oracle Privileged Account Manager for this release:

- org.identityconnectors.dbum-1.0.1116.jar
- org.identityconnectors.genericunix-1.0.0.jar
- org.identityconnectors.ldap-1.0.6380.jar

Note: If you obtain any new ICF connectors from Oracle, you must place them in the location specified in the instructions provided.

Storing custom third-party connectors is at your discretion; however, you must ensure they can be read by Oracle Privileged Account Manager at run time.

3.2.3 Consuming ICF Connectors

Oracle Privileged Account Manager consumes ICF connectors by using the opam-config.xml file. The contents of this file provide the following information to Oracle Privileged Account Manager:

1. Where to pick up the ICF connector bundle (on the file system)

2. Which configuration attributes are relevant for the Oracle Privileged Account Manager use-cases
3. How to render the Oracle Privileged Account Manager Console when configuring connectivity to a target system using a particular connector

You will find the `opam-config.xml` file in the *`ORACLE_HOME`*`/opam/config` directory. During domain creation, the `opam-config.xml` file is copied to the *`DOMAIN_HOME`*`/config/fmwconfig/opam` directory, and this file is applicable for that domain. The out-of-the-box image is configured to pick up and use the connector bundles that ship with the Oracle Identity Management Suite.

The `opam-config.xsd` file (also located in the `ORACLE_HOME/opam/config` directory) describes the schema for `opam-config.xml`. If you make any changes to *`DOMAIN_HOME`*`/config/fmwconfig/opam/opam-config.xml` file, verify them with the `opam-config.xsd` file.

3.2.4 Adding New Connectors to an Existing Oracle Privileged Account Manager Installation

This section describes the processes for adding new connectors to your existing Oracle Privileged Account Manager installation. The topics include:

- Adding Connectors Supplied by Oracle
- Adding Custom Connectors

3.2.4.1 Adding Connectors Supplied by Oracle

If you are adding new ICF connectors that are supplied by Oracle, then they will be accompanied by installation instructions. These instructions describe where to store the connector bundle and how to modify the installation specific `opam-config.xml` file.

3.2.4.2 Adding Custom Connectors

Oracle Privileged Account Manager can use custom connectors that you created or that were created by a third party. However, these connectors must strictly adhere to the ICF standard. After verifying that the connector is ICF-compliant, perform the following steps to deploy the connector for Oracle Privileged Account Manager consumption:

1. Put the connector bundle in a location on the file system where the bundle can be read by the Oracle Privileged Account Manager at run time.
2. Perform the following steps to create a configuration block for the connector and include that block in the installation specific `opam-config.xml` file:
   a. Design and create a relevant configuration block.

      Both the `opam-config.xml` and `opam-config.xsd` files contain documentation and an example at the beginning of the file describing how to create a configuration block.

   b. Ensure that this connector configuration block includes the file system location you specified for the connector bundle in step 1.
   c. Add the new connector configuration block to the `opam-config.xml` file by containing it in a `<connectorConfig>` block.
   d. Validate the modified `opam-config.xml` file against the `opam-config.xsd` file to ensure that the Oracle Privileged Account Manager server can read the

modified file. You can use your favorite XML schema validation tool for this purpose.

3. Restart the Oracle Privileged Account Manager server.
4. Connect to Oracle Privileged Account Manager, and then add and configure a new target system using the newly added connector type.

3.3 Starting Oracle Privileged Account Manager

This section provides some high-level information about starting and working with Oracle Privileged Account Manager's Console. The topics include:

- Starting WebLogic
- Configuring SSL Communication in Oracle Privileged Account Manager
- Assigning the Application Configurator Role to a User
- Invoking Oracle Privileged Account Manager's Web-Based Console

Note: Refer to *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator* for more detailed information.

3.3.1 Starting WebLogic

Before you start Oracle Privileged Account Manager, you must start the WebLogic servers and console.

Note:

- For detailed information about starting WebLogic and managed servers, see "Starting or Stopping the Oracle Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
- You must have the appropriate Administration Role and credentials to start the server. Refer to Section 2.3.1, "Administration Role Types" for more information.

1. Connect the Node Manager to WLST by running the `nmConnect` command.

   See "Node Manager Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference* for instructions.

2. Start the WebLogic Admin Server. For example,

   On UNIX, type

   ```
   MIDDLEWARE_HOME/user_projects/domains/DOMAIN_NAME/bin/startWebLogic.sh
   ```

   On Windows, type

   ```
   MIDDLEWARE_HOME\user_projects\domains\DOMAIN_NAME\bin\startWebLogic.bat
   ```

3. Start the Oracle Privileged Account Manager managed server.
4. Open a browser and start the WebLogic Console from the following location:

   http://*adminserver_host*:*adminserver_port*/console

3.3.2 Configuring SSL Communication in Oracle Privileged Account Manager

Oracle Privileged Account Manager can connect to target systems through Secure Socket Layer (SSL) or non-SSL options. The SSL option is more secure, but requires some additional configuration.

To communicate securely over SSL with a target system, the WebLogic instance running Oracle Privileged Account Manager must trust the SSL certificate used by the target system because Oracle Privileged Account Manager inherits its SSL configuration from the WebLogic container in which it runs. To have the WebLogic instance running Oracle Privileged Account Manager (and therefore Oracle Privileged Account Manager) trust the target system's SSL certificate, you must import the certificate into the truststore used by that WebLogic instance.

Use the following steps to enable SSL communication between the target system and Oracle Privileged Account Manager:

1. Export the SSL certificate from the target system host computer.

   Note: The steps for exporting an SSL certificate are different for each target system type. Refer to the product documentation provided for your target system for detailed instructions.

2. Copy the certificate to the machine where you have the WebLogic instance running Oracle Privileged Account Manager.

   If you have the Oracle Privileged Account Manager/Oracle Identity Navigator Console and the Oracle Privileged Account Manager server running on different machines, you must copy the SSL certificate to the Oracle Privileged Account Manager server machine.

3. Run the following command to import the certificate into the JVM truststore of the WebLogic Server on which Oracle Privileged Account Manager is running:

   ```
   JAVA_HOME\bin\keytool -import -file FILE_LOCATION -keystore TRUSTSTORE_LOCATION
   -storepass TRUSTSTORE_PASSWORD -trustcacerts -alias ALIAS
   ```

   Where

   - *JAVA_HOME* is the location used by your WebLogic server. For example.
     - *MIDDLEWARE_HOME*/jrockit..
     - *MIDDLEWARE_HOME*/jdk..
     - The location where you installed the Java software
   - *FILE_LOCATION* is the full path and name of the certificate file.
   - *TRUSTSTORE_LOCATION* is one of the following truststore paths:

Table 3–3 Truststore Locations

If you are using:	Import the Certificate into the Keystore in This Directory:
Oracle jrockit_R27.3.1-jdk	*JROCKIT_HOME*/jre/lib/security
The default Oracle WebLogic Server JDK	*WEBLOGIC_HOME*/java/jre/lib/security/cacerts
A JDK other than Oracle jrockit_R27.3.1-jdk or Oracle WebLogic Server JDK	*JAVA_HOME*/jre/lib/security/cacerts

- *TRUSTSTORE_PASSWORD* is the password for the truststore.
- *ALIAS* is an alias for the certificate.

Note: The default password for the `cacerts` keystore is *changeit*.

4. Restart all WebLogic servers.

Note: For more information about WebLogic security concepts and how to create custom keystores, refer to "Configuring Identity and Trust" in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

3.3.3 Assigning the Application Configurator Role to a User

After installation, you do not have any users present with administrator roles. You must select a user and grant that person the *Application Configurator* role by using Oracle Identity Navigator.

Note: Refer to "Assigning a Common Admin Role" in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator* for instructions.

The Application Configurator user can have other roles in addition to this role. For more information about other Admin Roles, see Section 2.3.1, "Administration Role Types."

When the Application Configurator user logs in by using the following URL, that user will see a empty screen with a **Configure OPAM** link.

http://*adminserver_host*:*adminserver_port*/oinav/opam

The Application Configurator user can use this link to let the Oracle Privileged Account Manager Console know where Oracle Privileged Account Manager server is running by providing the Oracle Privileged Account Manager server's host and port.

When the Oracle Privileged Account Manager Console can successfully communicate with the Oracle Privileged Account Manager server, the Oracle Privileged Account Manager Console will be populated with content.

Note: Oracle Privileged Account Manager administrators and users will probably never have to use the Oracle Identity Navigator interface except during the initial set-up of Oracle Privileged Account Manager.

3.3.4 Invoking Oracle Privileged Account Manager's Web-Based Console

You can access Oracle Privileged Account Manager's Console by opening a browser window and entering the following URL:

http://*adminserver_host*:*adminserver_port*/oinav/opam

When the Oracle Privileged Account Manager page displays with the Sign In screen, log in with the appropriate administrator or end user credentials.

Note: If you prefer using Oracle Privileged Account Manager's command line tool or Oracle Privileged Account Manager's RESTful interface, refer to Appendix A, "Working with the Command Line Tool" or Appendix B, "Working with Oracle Privileged Account Manager's RESTful Interface" (respectively) for detailed information about using those interfaces.

3.4 Navigating Oracle Privileged Account Manager's Console

This section provides a high-level overview of the Oracle Privileged Account Manager Console.

Note: Access to certain features in the Console is based on your administration role (Admin Role) and credentials. For example, the Reports and Administration accordions described in this section are not available to users with the Security Administrator role.

Refer to Section 2.3, "Understanding Oracle Privileged Account Manager Authorization" for more information about Admin Roles.

The topics in this section include:

- Working with the Home Accordion
- Working with the Reports Accordion
- Working with the Administration Accordion
- Working with the Search Portlet
- Working with a Search Results Table

Tip: Hover your mouse over elements in the Oracle Privileged Account Manager interface (such as nodes in the Home accordion or parameter fields) to see helpful prompts.

3.4.1 Working with the Home Accordion

When you log in to Oracle Privileged Account Manager, the Home accordion is displayed and expanded by default. Based on your Admin Role and credentials, this area gives you access to a tree containing some or all of the following nodes:

- **Accounts**: Search, open, add, and remove accounts
- **Targets**: Search, open, add, and remove targets
- **Policies**: Search, open, create, and delete Password Policies and Usage Policies
- **Grantees**: Search, open, add, and remove grantees (users and groups)
- **My Checked-out Accounts**: View, check out, and check in accounts

Note: For detailed information about Admin Roles, see Section 2.3.1, "Administration Role Types."

You can expand these nodes to view the target types, domains, Password and Usage Policies, and Users and Groups Grantees.

For example, in this figure, the **ldap** node is the Target Type, and **us** is the Domain. So, if you are looking for an account and know that it is managed by an LDAP target in the us Domain, simply click the **us** node to view a list of the accounts in that domain. The results display in the Search Results table.

Selecting the nodes or subnodes on this accordion causes a new page to display. You use parameters on these pages to configure and manage Oracle Privileged Account Manager.

Above the Home accordion are two menus that you can use to control how the Home accordion is displayed:

- **View**: Use the options on this drop-down menu to expand or collapse all nodes at once, expand or collapse all subnodes below a selected node, or scroll to the first or last node.
- **Perspective**: Use this drop-down menu to control whether information is displayed from a **Target Type** or from a **Domain** perspective.

3.4.2 Working with the Reports Accordion

Expand the Reports accordion and click a **Report** link to access different reports about the targets and privileged accounts in your deployment. The information is displayed in the Reports page on the right side of the Console.

Note: For detailed information about these Reports, see Section 5.1.5, "Working with Reports."

3.4.3 Working with the Administration Accordion

Expand the Administration accordion and click **Server Configuration** to open a Server Configuration tab. You use the Server Configuration tab to set up and test a connection to your Oracle Privileged Account Manager server.

Note: For detailed information about managing an Oracle Privileged Account Manager server, see Section 4.4, "Managing an Oracle Privileged Account Manager Server."

3.4.4 Working with the Search Portlet

You use Oracle Privileged Account Manager's Search portlet to search for targets, accounts, policies, users, and groups.

Figure 3–1 Example Search Portlet

You can configure searches by using one or more of the parameters displayed in a Search portlet. The available parameters depend on the type of search. The following table describes the different search parameters:

Table 3–4 Search Portlet Parameters

Parameter Name	Description	Search Type
Account Name	Enter one or more letters of the account name for which you are searching.	Accounts, Users, Groups
Target Name	Specify one or more letters of the target name on which to search.	Accounts, Targets, Users, Groups
Target Type	Specify **All** (to search all target types), **ldap**, **unix**, or **database**.	Accounts, Targets
Domain	Specify the domain on which to search.	Accounts, Targets
Host Name	Specify the name of the host on which to search.	Targets
Policy Name	Specify one or more letters of the policy name for which you are searching.	Policies
Policy Status	Specify whether to search for **All** policies or limit the search to only **Active** or only **Disabled** policies.	Policies
Policy Type	Specify whether to search for **All** policy types or limit the search to only **Password Policies** or only **Usage Policies**.	Policies
User Name	Specify one or more letters of the user's name for which you are searching.	Users
First Name	Specify one or more letters of the user's first name.	Users
Last Name	Specify one or more letters of the user's last name.	Users
Group Name	Specify one or more letters of the group name for which you are searching.	Groups
Description	Provide the group description.	Groups

The general steps for performing a search are as follows:

1. Select the appropriate node in the Home tree.

   For example, to search for an account, select the **Accounts** node.

2. Enter one or more of the search parameters available in the Search portlet and then click **Search**.

   For example, to search for a list of all the accounts on a particular LDAP target, enter one or more letters of the target's name, select LDAP from **Target Type** menu, and then click **Search**.

   The results are displayed in the Search Results table.

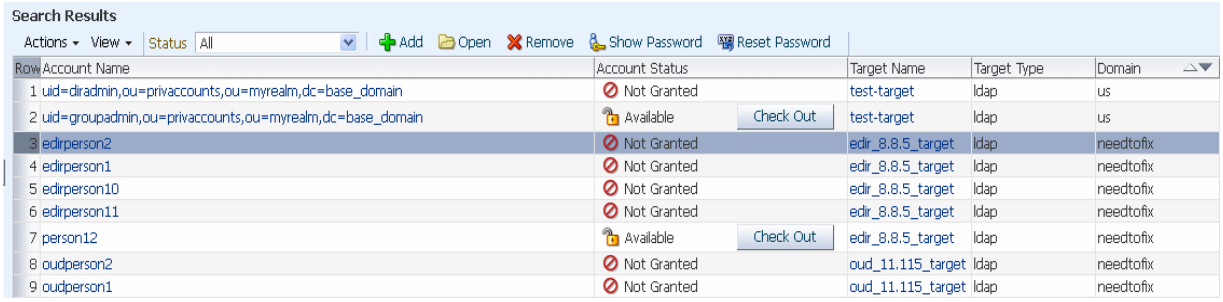
   Note: You can use the **Status** menu, located above the Search Results table, to control the search results based on the account status. See the table in Section 3.4.5, "Working with a Search Results Table" for more information.

3. To perform another search, click **Reset**.

3.4.5 Working with a Search Results Table

You can use the drop-down menus and icons located along the top of the different Search Results tables to perform various tasks.

Figure 3–2 Example Search Results Table



The following table describes these features:

> **Note:** The availability of these features change, based on your role (privileges) and what type of search was performed. See Section 2.3.1, "Administration Role Types" for more information.

Table 3–5 Search Results Table Features

Feature Name	Search Type	Description
Actions	Accounts, Targets, Policies, Users, Groups, and My Checked-out Accounts	Click to select an action from a drop-down menu. **Note**: The Actions menu options duplicate the task icons displayed above the table.
View	Accounts, Targets, Policies, Users, Groups, and My Checked-out Accounts	Use this drop-down menu to control how the columns are displayed in the Search Results table. ▪ **Columns** > **Show All**: Displays all columns in the table. ▪ **Columns** > **Manage Columns**: Provides a dialog that enables you to display or hide columns. ▪ **Reorder Columns**: Select this option and a dialog displays that enables you to select the visible columns and shift their order.
Status	Accounts only	Choose an option from the menu to control how the search results are displayed: ▪ **All**: Lists all accounts on the target. ▪ **Available Accounts**: Lists only those accounts that are available to be checked-out. **Note**: If you are viewing the account as an administrator, Available Accounts are accounts that can be checked out by any user who has been granted access to that account. If you are viewing the account as a grantee, Available Accounts means you can check out the account. ▪ **Checked-out Accounts**: Lists only those accounts that are currently checked-out. ▪ **Unavailable Accounts**: Lists only those accounts that you have not been granted permission to checkout.

Table 3–5 (Cont.) Search Results Table Features

Feature Name	Search Type	Description
Add	Accounts, Targets, Users, and Groups	Click to add a new target, account, user, or group to the Oracle Privileged Account Manager repository.
Open	Accounts, Targets, Policies, Users, and Groups	Click to open the selected account, target, policy, user, or group.
Remove	Accounts, Targets, Policies, Users, and Groups	Click to remove the selected account, target, policy, user, or group from the Oracle Privileged Account Manager repository.
Show Password	Accounts only	Click to open a message listing the account name and the password for that account.
Reset Password	Accounts only	Click to open the Reset Password dialog where you can enter a new password for the selected account.
Create Password Policy	Policies only	Click to create a Password Policy. See Section 5.1.2.2, "Adding Targets to Oracle Privileged Account Manager" for more information.
Create Usage Policy	Policies only	Click to create a Usage Policy. See Section 5.1.2.2, "Adding Targets to Oracle Privileged Account Manager" for more information.
Delete	Policies only	Click to delete a selected policy from the Oracle Privileged Account Manager repository.
Check-In	My Checked-out Accounts only	Click to check in the selected checked-out account. See Section 5.1.3.7, "Checking In Accounts" for more information.

4

Adding and Managing an Oracle Privileged Account Manager Server

This chapter provides information that administrators must know to add, configure, and manage an Oracle Privileged Account Manager server.

The topics in this chapter include

Note:

- Refer to "Oracle Fusion Middleware Directory Structure" in the *Oracle Fusion Middleware Installation Planning Guide* for information about directory structure.
- For detailed information about starting WebLogic and Managed Servers, see "Starting or Stopping the Oracle Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
- You must have the *Application Configurator* Admin Role and credentials to start the Oracle Privileged Account Manager server.

4.1 Overview

The Oracle Privileged Account Manager server is a component that handles password requests, generates passwords, and protects the password keystore.

The Oracle Privileged Account Manager server implements the core functionality of Oracle Privileged Account Manager and makes authorization decisions that determine:

- Which targets and privileged accounts are exposed to administrators and end-users
- Which operations administrators and end-users can perform on targets, privileged accounts, and policies

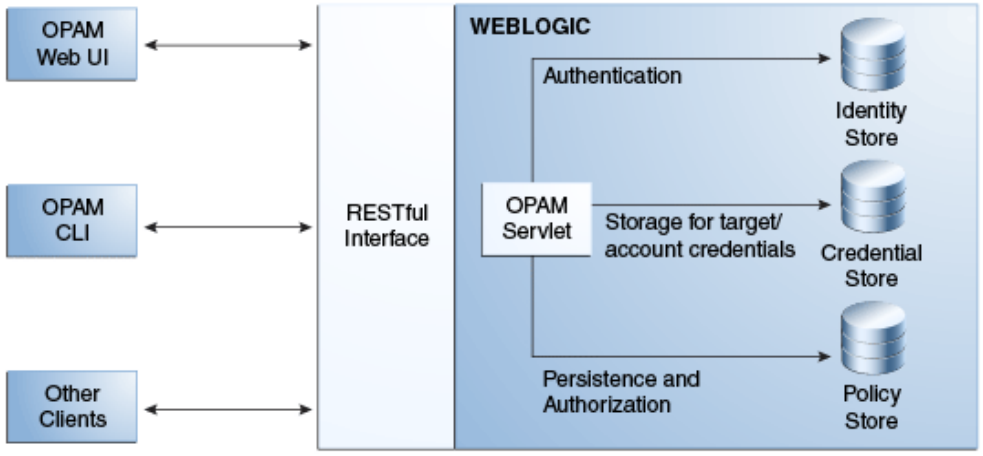
In addition, the Oracle Privileged Account Manager server

- Supports usage and password policies for accounts
- Enforces the authorization decisions mentioned
- Supports authentication by using the SAML-based Oracle Security Token from OPSS Trust Services and HTTP-Basic Authentication
- Supports different Admin Roles for Oracle Privileged Account Manager server

> **Note:** For security purposes, the Oracle Privileged Account Manager server only responds to SSL traffic.
>
> When you add the Oracle Privileged Account Manager server target to the Oracle Privileged Account Manager user interface or to the Oracle Privileged Account Manager command line tool (CLI), you must provide the SSL endpoint as https://*hostname*:*sslport*/opam.
>
> By default, WebLogic responds to SSL using port 7002 on the Admin Server and port 18102 on the Managed Server. You can use the WebLogic console to check the port for your particular instance.

The following figure illustrates the Oracle Privileged Account Manager server architecture.

Figure 4–1 Server Architecture



4.2 Before You Begin

You must be an Oracle Privileged Account Manager administrator with the *Application Configurator* Admin Role to add and manage an Oracle Privileged Account Manager server.

The procedures described in this chapter reference information and instructions contained in the following Oracle publications. If necessary, review the referenced

concepts, terminology, and procedures before you begin configuring the Oracle Privileged Account Manager server:

Table 4–1 Reference Publications

For Information About	Refer to
Admin Roles	Section 2.3.1, "Administration Role Types"
Supported identity and policy store configurations for Oracle Privileged Account Manager and Oracle Identity Navigator	Section 1.7, "System Requirements and Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
Oracle WebLogic Server concepts and terminology	*Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* and *Oracle Fusion Middleware Securing Oracle WebLogic Server*
Creating a default authenticator in Oracle WebLogic Server	*Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* and *Oracle Fusion Middleware Securing Oracle WebLogic Server*
Configuring an identity store in your environment	Your vendor product documentation
Configuring Oracle Virtual Directory with the LDAP-based server	"Creating LDAP Adapters" in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
Configuring the OVD authenticator in Oracle WebLogic Server	*Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*
Associating a policy store using WLST	"Setting a Node in an Oracle Internet Directory Server" and "reassociateSecurityStore" sections in the *Oracle Fusion Middleware Application Security Guide*
Associating a policy store using Enterprise Manager	"Reassociating with Fusion Middleware Control" in the *Oracle Fusion Middleware Application Security Guide*
Managing the Oracle Privileged Account Manager server	Section 4.4, "Managing an Oracle Privileged Account Manager Server"

Note: Oracle Privileged Account Manager administrators and users will probably never have to use the Oracle Identity Navigator interface except during the initial set-up of Oracle Privileged Account Manager.

4.3 Configuring an External Identity Store for Oracle Privileged Account Manager

This section describes how to configure a new, external identity store for Oracle Privileged Account Manager.

The topics in this section include:

- Configuring the External Identity Store
- Configuring Enterprise Roles

4.3.1 Configuring the External Identity Store

You must configure a domain identity store before you can view users when searching from the Oracle Identity Navigator Access Privileges pane. To configure the identity store as the main authentication source, you must configure the Oracle WebLogic Server domain where Oracle Identity Navigator is installed.

This section describes how to configure the domain identity store using Oracle Internet Directory or Oracle Virtual Directory with a supported LDAP-based directory server. You configure the identity store in the WebLogic Server Administration Console.

Note:

- Theoretically, you can configure any LDAP server as an external identity store to WebLogic.

  For more information about configuring an identity store, see "Configuring the Identity Store Service" in the *Oracle Fusion Middleware Application Security Guide*.

- For information about other supported identity stores, see "System Requirements and Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

To configure the Oracle Internet Directory authenticator in Oracle WebLogic Server:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.
2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, the default realm is `myrealm`.
3. Select the Providers tab, then select the Authentication subtab.
4. Click **New** to launch the Create a New Authentication Provider page and complete the fields as follows:

   - **Name**: Enter a name for the authentication provider. For example, **`MyOIDDirectory`**.
   - **Type**: Select **OracleInternetDirectoryAuthenticator** from the list.

   Click **OK** to update the authentication providers table.
5. In the authentication providers table, click the newly added authenticator.
6. In Settings, select the Configuration tab, then select the Common tab.
7. On the Common tab, set the **Control Flag** to **SUFFICIENT**.

   Setting the Control Flag attribute for the *authenticator provider* determines the ordered execution of the Authentication providers. The possible values for the Control Flag attribute are:

   - **REQUIRED** - This LoginModule must succeed. Even if it fails, authentication proceeds down the list of LoginModules for the configured Authentication providers. This setting is the default.
   - **REQUISITE** - This LoginModule must succeed. If other Authentication providers are configured and this LoginModule succeeds, authentication proceeds down the list of LoginModules. Otherwise, control is returned to the application.
   - **SUFFICIENT** - This LoginModule need not succeed. If it does succeed, return control to the application. If it fails and other Authentication providers are configured, authentication proceeds down the LoginModule list.

- **OPTIONAL** - This LoginModule can succeed or fail. However, if all Authentication providers configured in a security realm have the JAAS Control Flag set to `OPTIONAL`, the user must pass the authentication test of one of the configured providers.

8. Click **Save**.
9. Select the Provider Specific tab and enter the following required settings using values for your environment:
   - **Host**: The host name of the Oracle Internet Directory server.
   - **Port**: The port number on which the Oracle Internet Directory server is listening.
   - **Principal**: The distinguished name (DN) of the Oracle Internet Directory user to be used to connect to the Oracle Internet Directory server. For example: cn=OIDUser,cn=users,dc=us,dc=mycompany,dc=com.
   - **Credential**: Password for the Oracle Internet Directory user entered as the Principal.
   - **Group Base DN**: The base distinguished name (DN) of the Oracle Internet Directory server tree that contains groups.
   - **User Base DN**: The base distinguished name (DN) of the Oracle Internet Directory server tree that contains users.
   - **All Users Filter**: LDAP search filter. Click **More Info** for details.
   - **User From Name Filter**: LDAP search filter. Click **More Info** for details.
   - **User Name Attribute**: The attribute that you want to use to authenticate (for example, cn, uid, or mail). For example, to authenticate using a user's email address you set this value to mail.
   - Enable **Use Retrieved User Name As Principal**.
10. Click **Save**.
11. From the Settings for myrealm page, select the Providers tab, then select the Authentication tab.
12. Click **Reorder**.
13. Select the new authenticator and use the arrow buttons to move it into the first position in the list.
14. Click **OK**.
15. Click **DefaultAuthenticator** in the Authentication Providers table to display the Settings for DefaultAuthenticator page.
16. Select the Configuration tab, then the Common tab, and select **SUFFICIENT** from the **Control Flag** list.
17. In the Change Center, click **Activate Changes**.
18. Restart Oracle WebLogic Server.
19. Verify your configuration and set-up by confirming that the users present in the LDAP directory (Oracle Internet Directory or Oracle Virtual Directory) can log in to Oracle Privileged Account Manager with no issues.

To use Oracle Virtual Directory as the domain identity store, you must do the following:

- Configure Oracle Virtual Directory with an LDAP-based server as described in "Creating LDAP Adapters" in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.
- Configure the OVD authenticator in Oracle WebLogic Server as described in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.
- You must enable the **Use Retrieved User Name As Principal** option when configuring authenticators in Oracle WebLogic Server, as described in the preceding step 9.

4.3.2 Configuring Enterprise Roles

You must create enterprise roles in the domain identity store to support the Common Admin Roles. Templates are provided for both Oracle Internet Directory and Oracle Virtual Directory configured with an LDAP-based directory server. You use these templates with the Oracle Internet Directory Migration Tool (`ldifmigrator`), which enables you to convert LDIF files output from other directories or application-specific repositories into a format recognized by Oracle Internet Directory.

Before you configure enterprise roles for the Common Admin Roles, you must configure the domain identity store as described in Section 4.3.1, "Configuring the External Identity Store."

> **Note:** For more information about supported identity store configurations for Oracle Privileged Account Manager and Oracle Identity Navigator, see Section 1.7, "System Requirements and Certification" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

To configure enterprise roles in the domain identity store:

1. Select the template for your environment from `ORACLE_HOME/common/templates`.
   - For Oracle Internet Directory, use `oinav_template_oid.ldif`
   - For Oracle Virtual Directory, use `oinav_template_ovd.ldif`
2. To use the `ldifmigrator` tool, set *`JAVA_HOME`* and include *`JAVA_HOME`*`/bin` in `PATH`.
3. Use the `ldifmigrator` tool to create the enterprise roles in the identity store under `<GroupBase>` as follows:

```
Run
java -cp MIDDLEWARE_HOME/oracle_common/modules/oracle.ldap_11.1.1
  /ldapjclnt11.jar
-DORACLE_HOME=ORACLE_HOME/oracle_common oracle.ldap.util.LDIFMigration
   input_file=<ldif template>  output_file=<outputfile>  namespace=<GroupBase>
-load dn=<bindDn> password=<>  host=<hostName>  port=<portNumber>
```

   Where *ldif template* is the template name.

Note:

- When using Oracle Virtual Directory with an LDAP-based directory server, the host, port, dn, and groupbase refer to Oracle Virtual Directory and not the LDAP server.
- For more information about using the `ldifmigrator` tool, refer to the *Oracle Fusion Middleware Reference for Oracle Identity Management*.

Note: To configure Single Sign On, see Section 7.2.2, "Enabling Single Sign-On."

4.4 Managing an Oracle Privileged Account Manager Server

This section provides information administrators need to manage an Oracle Privileged Account Manager server, which includes the following topics:

- Configuring a Connection to the Oracle Privileged Account Manager Server
- Managing Oracle Privileged Account Manager Server Properties

4.4.1 Configuring a Connection to the Oracle Privileged Account Manager Server

Use the following steps to configure a connection to the Oracle Privileged Account Manager server from the Oracle Privileged Account Manager Console:

1. Open Oracle Privileged Account Manager by logging in to:

   http://*adminserver_host*:*adminserver_port*/oinav/opam

   Note: You must log in as a user with the *Application Configurator* Admin Role, or the Server Configuration page will not be accessible.

   For more information about this, and other, Admin Roles see Section 2.3.1, "Administration Role Types" and Section 3.3.3, "Assigning the Application Configurator Role to a User."

2. Expand the Administration accordion and select **Server Configuration**.
3. When the Server Configuration page displays, enter the **Host** name and **SSL Port** number.

   Notice the URL displayed below the SSL Port field.
4. Click the **Test** button to test the connection settings.

   You should see a message display, stating the configuration tested successfully.
5. Click the **Apply** button to save this connection information.

4.4.2 Managing Oracle Privileged Account Manager Server Properties

You can use properties in the OPAM Global Config configuration entry to control how often the Oracle Privileged Account Manager server

- Checks accounts and then automatically checks-in the accounts that have exceeded the expiration time defined in the Usage Policy.
- Checks accounts and then resets the password for any accounts that have exceeded the maximum password age defined in the password policy.

To access the OPAM Global Config configuration entry and modify these server properties, use the `getglobalconfig` and the `modifyglobalconfig` commands from the command line.

Note: Refer to Section A.2.13, "`getglobalconfig` Command" and Section A.2.16, "`modifyglobalconfig` Command" for detailed information about using these commands.

5

Configuring and Managing Oracle Privileged Account Manager

This chapter explains how to configure and manage Oracle Privileged Account Manager. This information is organized into the following topics:

- Section 5.1, "Administering Oracle Privileged Account Manager"
- Section 5.2, "Working with Self-Service"
- Section 5.3, "Moving from a Test Environment to a Production Environment"

> **Note:** You can also use Oracle Privileged Account Manager's command line tool or Oracle Privileged Account Manager's RESTful interface to perform many of the tasks described in this chapter.
>
> If you prefer using these interfaces instead of the Oracle Privileged Account Manager Console, see Appendix A, "Working with the Command Line Tool" or Appendix B, "Working with Oracle Privileged Account Manager's RESTful Interface" for instructions.

5.1 Administering Oracle Privileged Account Manager

This section provides instructions for administrators who must configure and maintain Oracle Privileged Account Manager.

The topics include:

- Working with Policies
- Working with Targets
- Working with Privileged Accounts
- Working with Grantees
- Working with Reports

You must be an Oracle Privileged Account Manager administrator with a particular Admin Role to perform the different configuration tasks described in this section.

The following list describes the basic workflow that is performed by Oracle Privileged Account Manager administrator users based on their different Admin Roles:

Note: An administrator with the *Application Configurator* Admin Role should have already configured a connection to the Oracle Privileged Account Manager server. See Section 4.4.1, "Configuring a Connection to the Oracle Privileged Account Manager Server" for more information.

Table 5–1 Administrator Workflows Based on Admin Roles

Administrator	Responsibility
Security Administrator	1. Evaluates Oracle Privileged Account Manager's Default Usage Policy and Default Password Policy and, if necessary, modifies these policies or creates new ones. 2. Adds targets to Oracle Privileged Account Manager. 3. Adds privileged accounts on that target. **Note**: This role cannot assign grantees to privileged accounts. 4. Assigns Usage Policy and Password Policy to the accounts. 5. Manages existing targets, accounts, and policies.
User Manager	1. Assigns grants to accounts. 2. Creates and manages Usage Policies as needed. 3. Assigns Usage Policy to grants. 4. Manages existing grants and Usage Policy assignments.
Security Auditor	Reviews Oracle Privileged Account Manager reports.

Note: For more information about these Admin Roles, see Section 2.3.1, "Administration Role Types."

5.1.1 Working with Policies

This section provides information about working with Oracle Privileged Account Manager Usage Policies and Password Policies.

The topics include

- Policies Overview
- "Viewing Policies" on page 3
- Modifying the Default Password Policy
- Modifying the Default Usage Policy
- Creating a Password Policy
- Creating a Usage Policy
- Searching for Policies
- Assigning Policies
- Deleting Policies

5.1.1.1 Policies Overview

In Oracle Privileged Account Manager, there are two types of policies:

- **Password Policy**. This policy type captures the password construction rules enforced by a specific target on an associated privileged account. For example, minimum and maximum number of numeric characters. You use a Password Policy to create a password value that Oracle Privileged Account Manager uses to reset a password for a privileged account.
- **Usage Policy**. This policy type defines when and how a grantee can use a privileged account. (Default access is 24x7.)

Every privileged account that is managed by Oracle Privileged Account Manager must have an associated Password Policy. A Usage Policy only applies at the level of a grant. You can associate a single Password Policy with multiple privileged accounts and a single Usage Policy with multiple grants.

Oracle Privileged Account Manager provides a Default Password Policy and a Default Usage Policy. You can choose to use the default policies, to modify these policies, or to create your own, specialized policies.

To review the parameter settings for these policies, see Section 5.1.1.2, "Viewing Policies."

Note: Only administrators with the *Security Administrator* Admin Role or the *User Manager* Admin Role can work with policies.

- An administrator with the *Security Administrator* Admin Role can modify the Default Password Policy and Default Usage Policy, create new policies, or delete policies.

  Administrators with the *Security Administrator* Admin Role can assign Password Policies, but they cannot assign Usage Policies.
- An administrator with the *User Manager* Admin Role can only assign a Usage Policy to accounts at the *grantee-account* pair level. In other words, the *User Manager* can assign different Usage Policies to different grantees of the same account.

  Administrators with the *User Manager* Admin Role cannot assign Password Policies.

5.1.1.2 Viewing Policies

To review the parameter settings for a Password Policy or a Usage Policy:

1. Select **Password Policies** or **Usage Policies** from the Home tree.
2. When the Policies page displays, use one of the following methods to open a policy:
   - Click the **Row** number next to the policy name and then click the **Open** icon located above the Search Results table.
   - Click the policy name (an active link) in the Search Results table.

     For example, clicking the **Default Password Policy** link opens the Password Policy: Default Password Policy page.

   A Password Policy page contains three tabs:
   - **General**. Contains parameters used to specify general information about the policy and Password Lifecycle Rules for the policy.
   - **Password Complexity Rules**. Contains parameters that govern the complexity requirements for account passwords.

- **Privileged Accounts**. Provides information about the privileged accounts currently using the Default Password Policy.

A Usage Policy page also contains three tabs:

- **General Fields**. Contains parameters used to specify general information about the policy.
- **Usage Rules**. Contains parameters that govern when the account can be checked out and when the check out expires.
- **Grantees**. Provides information about the grantees who are authorized to use that account.

5.1.1.3 Modifying the Default Password Policy

After evaluating the Default Password Policy, you may decide you want to modify the settings to better suit your environment.

To modify the Default Password Policy, use the following steps:

1. Select **Password Policies** from the Home tree.
2. When the Policies page displays, select the **Default Password Policy** link in the Search Results table to open the Password Policy: Default Password Policy page.
3. Select the General tab to edit the **Policy Description** field in the General Fields area or to modify any of the following Password Lifecycle Rules:

   - **Password maximum age**: Use the two menus to specify a duration period (number of days, hours, or minutes) after which Oracle Privileged Account Manager must automatically reset the account password.

     For example, if your enterprise wants a security policy where account passwords must be changed every month, you would set this value to 30 days.

     Every time the account is checked out and its password gets changed (if the policy is configured so that passwords must be changed on checkout/check-in) Oracle Privileged Account Manager tracks the password change time.

     Note: An administrator with the *Security Administrator* Admin Role can also manually reset a password by using the **Reset Password** option (described in Section 5.1.3.5.2, "Resetting an Account Password") and Oracle Privileged Account Manager tracks this password change time as well.

     If Oracle Privileged Account Manager detects the account is idle and no password changes have occurred over the specified number of days, then Oracle Privileged Account Manager automatically resets the password to a new, randomized value, which helps the enterprise to automatically enforce the security policy without human intervention.

     To disable this automatic reset option, set the numeric value to 0.

   - **Reset password on check-in**: Use this option to specify whether Oracle Privileged Account Manager must auto-generate and set a randomized password during a check-in operation.

     Uncheck this box if you do not want the password to be reset during the check-in operation.

- **Reset password on check-out**: Use this option to specify whether Oracle Privileged Account Manager must auto-generate and set a randomized password during a check-out operation.

  Uncheck this box if you do not want the password to be reset during the check-out operation.

Note:

- For higher security, the Password must be changed on check-in and Password must be reset on check-out options are both enabled by default to require password changes, but they can be disabled if required. For example, some enterprises may only require that passwords be reset every 30 days.
- If your enterprise prefers that passwords not be automatically managed at all; that they are only changed through human intervention, disable all three of these Password Lifecycle Rules options.

  After disabling these three options, the only way to manually change passwords is by using the **Reset Password** option (described in Section 5.1.3.5.2, "Resetting an Account Password"). Oracle Privileged Account Manager is still useful in this case, as you can reset and centrally manage passwords for multiple systems from one place by using Oracle Privileged Account Manager.

---

4. Select the Password Complexity Rules tab to change one or more of the parameters that define the default password requirements.

Parameter	Description
Characters for Password	Specify the minimum and maximum number of characters required.
Alphabetic Characters	Specify the minimum number of alphabetic characters required.
Numeric Characters	Specify the minimum number of numeric characters required.
Alphanumeric Characters	Specify the minimum number of alphanumeric characters required.
Special Characters	Specify the minimum and maximum number of special characters (such as `*` or `@`) required.
Repeated Characters	Specify the minimum and maximum number of repeated characters allowed.
Unique Characters	Specify the minimum number of unique characters required.
Uppercase Characters	Specify the minimum number of uppercase characters required.
Lowercase Characters	Specify the minimum number of lowercase characters required.
Start with Character (not digit)	Specify the first character required to start a password.
Required Characters	Specify characters that are required in a password.

Parameter	Description
Allowed Characters	Specify which characters are permitted in a password.
Disallowed Characters	Specify which characters are not permitted in a password.
Disallowed as Password	Enable (check) the Account Name box to prohibit the use of an account name in the password.

5. Select the Privileged Accounts tab to review which accounts are currently using the Default Password Policy.

> **Note:** To specify a different Password Policy for any account listed in the table, click the Account Name link. When the Account page displays, select a different policy name from the **Password Policy** menu.

6. When you are finished editing the policy, click **Apply** to save your changes.

5.1.1.4 Modifying the Default Usage Policy

To modify the default Usage Policy,

1. Select **Usage Policies** from the Home tree.
2. When the Policies tab displays, select the **Default Usage Policy** link in the Search Results table to open the Usage Policy: Default Password Policy page with three tabs.
3. On the General Fields tab, you can only change content in the **Description** field.
4. Select the Usage Rules tab to change one of more of following parameter settings:

Parameter	Description
Timezone	Select a different time zone from the menu.
Permitted Usage Dates	Use the checkboxes and drop menus to change when grantees are allowed to use the account. Select one or more days of the week and the periods of time when grantees can access this account. (Default access is 24x7.)
Expiration Dates	Enable one of the following options to change when grantees' access to the account expires: ▪ **Automatically check in account**. Use the counter to specify the number of **minutes after last check out**. ▪ **Automatically check in account on this date**. Click the **Calendar** icon to open a Select Date and Time dialog. Use the month and year menus or click a day in the calendar to specify an expiration date. Use the hours, minutes, and seconds menus and enable the AM or PM buttons to specify an expiration time.

Note: If you are configuring a Usage Policy for a *shared* privileged account, it is prudent to configure an Automatic check-in option to ensure the account gets checked-in and the password gets cycled in a timely manner.

In addition, consider limiting how many users can access the shared account and further segregate these users by specifying when they can access the account. By specifying which days of the week and what times of the day each user can access the account, you minimize overlapping checkouts and improve Oracle Privileged Account Manager's auditing ability.

For more information about shared accounts, see Section 2.4.2, "Securing Shared Accounts."

5. Select the Grantees tab to view which grantees this policy is assigned.

Note: To specify a different Usage Policy for any grantee listed in the table, click the Account Name link. When the Account page displays, select a different policy name from the **Usage Policy** menu.

Tip: Clicking the active links in Grantee Name or Account Name columns enable you to navigate to other screens for additional information.

6. When you are finished editing the policy, click **Apply** to save your changes.

5.1.1.5 Creating a Password Policy

To create a Password Policy, use the following steps:

1. Select the Password Policies node from the Home tree.
2. When the Policies tab displays, click **Create Password Policy** at the top of the Search Results table.

   A new, Password Policy: *Untitled* page displays with three tabs.
3. Provide the following information on the General tab:
   a. **Policy Name**: Enter a name for the new policy.
   b. **Policy Status**: Click the button to specify whether the policy is **Active** or **Disabled**.

      Disabling a policy applies the Default Password Policy to all accounts and grants associated with that disabled policy. If you simply assigned a different policy to those accounts and grants, you would lose all information about the old policy assignment.

      Making the policy Active puts that policy into effect for the associated accounts and grants.
   c. Configure the **Password Lifecycle Rules** to allow Oracle Privileged Account Manager to auto-generate and set a randomized account password under certain conditions, as described in step 3 on page 5-3.

4. Use the parameters on the Password Complexity Rules tab to define the complexity rules requirements for passwords. Refer to the table provided in step 4 on page 5-5 for a description of these parameter settings.
5. Assign the policy to accounts or grantees using the instructions provided in Section 5.1.1.8, "Assigning Policies."

   After you assign this policy, you can select the Privileged Accounts tab to review which accounts are using this policy.
6. Click **Save**.

5.1.1.6 Creating a Usage Policy

To create a Usage Policy, use the following steps:

1. Select Usage Policies node from the Home tree.
2. When the Policies tab displays, click **Create Usage Policy** at the top of the Search Results table.

   A new, Usage Policy: *Untitled* page displays with three tabs.
3. Provide the following information on the General tab:
   a. **Policy Name**: Enter a name for the new policy.
   b. **Policy Status**: Click the button to specify whether the policy status is **Active** or **Disabled**.

      Disabling a policy applies the Default Usage Policy to all accounts and grants associated with that disabled policy. If you simply assigned a different policy to those accounts and grants, you would lose all information about the old policy assignment.

      Making the policy Active puts that policy into effect for the associated accounts and grants.
   c. **Description**: Enter a description of the policy.
4. Select the Usage Rules tab. Use the options on this page to define rules for using a privileged account. Refer to the table provided in step 4 on page 5-5 for a description of these parameter settings.
5. Assign the policy to accounts or grantees using the instructions provided in Section 5.1.1.8, "Assigning Policies."

   After you assign this policy, you can select the Grantees tab to review which users or groups are using this policy.
6. Click **Save**.

5.1.1.7 Searching for Policies

Use the following steps to search for a policy:

1. In the Home tree,
   - Select **Policies** to search all policies.
   - Select the **Password Policies** node or the **Usage Policies** node to search for policies that are the selected policy type.
2. When the Search Policies portlet displays, enter your search criteria into one or more of the following fields.
   - **Policy Name**: Enter all or any part of a policy name.

- **Policy Status**: Select **All** to search all policies. Select **Active** or **Inactive** to limit the search to just active or inactive policies.
- **Policy Type**: Select **All** to search all policies, or specify **Password Policy** or **Usage Policy** to limit the search to just the selected policy type.

Note: Selecting **Password Policies** or **Usage Policies** in step 1, automatically enters that policy type into the **Policy Type** field.

---

3. Click **Search**.

Review your search results in the Search Results table.

5.1.1.8 Assigning Policies

As previously stated, when you add a new privileged account, the Default Password Policy and Default Usage Policy are automatically assigned to that account.

To assign a different Password Policy or Usage Policy, you must first create the policy as described in Section 5.1.1.5, "Creating a Password Policy" or in Section 5.1.1.6, "Creating a Usage Policy."

Note:

- Administrators with the *Security Administrator* Admin Role can assign a Password Policy or a Usage Policy to an account. However, this role can only apply a Usage Policy at the account level.
- Administrators with the *User Manager* Admin Role can assign a Usage Policy to accounts at the *grantee-account pair* level. In other words, the User Manager can assign different Usage Policies to different grantees of the same account.

  The User Manager Admin Role cannot assign Password Policies.

5.1.1.8.1 Assigning Password Policies to Accounts You can assign Password Policies to an account from the Accounts page, from the Targets page, or from the Policies page.

From the Accounts Page

To assign a Password Policy from the Accounts page,

1. Use one of the following methods to locate the account:
   - Select the Accounts node in the Home tree, and then use the Search Accounts portlet to search for the account. See Section 5.1.3.3, "Searching for Privileged Accounts" for instructions.
   - Select the account's Target Type node or Domain node in the Home tree.

     For example, if you know the account is assigned to an LDAP target, select the **ldap** node.
2. When the Search Results display, click the account's Account Name link in the table to open the Account: *AccountName* page.
3. On the General tab, select a different policy name from the **Password Policy** menu.

4. After selecting the new policy, click **Test** to verify that the account can be managed by Oracle Privileged Account Manager. You should see a Test Succeeded dialog confirming the test was successful.
5. Click **Apply** to finish assigning the policy to the selected account.

From the Targets Page

To assign a Password Policy from the Targets page,

1. Use one of the following methods to locate the account:
   - Select the Targets node in the Home tree, and then use the Search Targets portlet to search for the account target. See Section 5.1.2.3, "Searching for Targets" for instructions.
   - Select the account's Target Type node or Domain node in the Home tree.

     For example, if you know the account is assigned to a UNIX target, select the **unix** node.
2. Click the account's Target Name link in the Search Results table to open the Target: *TargetName* page.
3. Click the Privileged Accounts tab to view a list of the accounts currently managed on the target.

   Notice that the table lists the Password Policy that is currently assigned to each account.
4. Locate the account and click the Account Name link.
5. When the General tab displays, select a different policy name from the **Password Policy** menu.
6. After selecting the new policy, click **Test** to verify that the account can be managed by Oracle Privileged Account Manager. You should see a Test Succeeded dialog confirming the test was successful.
7. Click **Apply** to finish assigning the policy to the selected account.

From the Policies Page

To assign a Password Policy from the Policies page,

1. Select the **Password Policies** node in the Home tree.
2. Locate the policy you want to assign in the Search Results table. Click the Policy Name link to open the Password Policy: *PolicyName* page.
3. Select the Privileged Accounts tab.
4. Locate the account and click the Account Name link to open the Account: *AccountName* page.
5. When the General tab displays, select a different policy name from the **Password Policy** menu.
6. After selecting the new policy, click **Test** to verify that the account can be managed by Oracle Privileged Account Manager. You should see a Test Succeeded dialog confirming the test was successful.
7. Click **Apply** to finish assigning the policy to the selected account.

5.1.1.8.2 Assigning a Usage Policy to Users and Groups When you add grantees to an account, as described in Section 5.1.4.2, "Granting Accounts to Users" or Section 5.1.4.3,

"Granting Accounts to Groups," Oracle Privileged Account Manager adds the user or group name to the Users or Groups table on the Grants tab and automatically assigns the Default Usage Policy.

You can assign a different Usage Policy from the Accounts page or from the Usage Policies page.

Note: When you create a new Usage Policy for an account, the new policy will not automatically be assigned to the existing grantees on that account. Oracle Privileged Account Manager allows you to assign customized policies to individual grantees, so you do not want the new policy to override those other policy assignments.

However, if you create a new policy for an account and then add new grantees, those (and future) grantees will automatically be associated with that policy because it has become the new default Usage Policy for the account.

From the Accounts Page

To assign a Usage Policy from the Accounts page,

1. Use one of the following methods to locate the account:
   - Select the Accounts node in the Home tree, and then use the Search Accounts portlet to search for the account. See Section 5.1.3.3, "Searching for Privileged Accounts" for instructions.
   - Select the account's Target Type node or Domain node in the Home tree.

     For example, if you know the account is assigned to an LDAP target, select the **ldap** node.
2. Locate the account's Account Name link to open the Account: *AccountName* page.
3. Select the Grants tab.
4. Locate the grantee in the Users or Groups table, and use the **Usage Policy** menu in that row to select a different policy.
5. Click **Apply** to add your changes.

From the Targets Page

To assign a Usage Policy from the Targets page,

1. Use one of the following methods to locate the account:
   - Select the Targets node in the Home tree, and then use the Search Targets portlet to search for the account target. See Section 5.1.2.3, "Searching for Targets" for instructions.
   - Select the account's Target Type node or Domain node in the Home tree.

     For example, if you know the account is assigned to an UNIX target, select the **unix** node.
2. Click the account's Target Name in the Search Results table to open that target.
3. When the Target: *TargetName* page displays, click the Grants tab to view a list of the grantees currently granted access to that account.

   Notice that the table lists the Usage Policy that is currently assigned to each grantee.

4. Locate the grantee in the Users or Groups table, and use the **Usage Policy** menu in that row to select a different policy.
5. Click **Apply** to finish assigning the policy to the selected account.

From the Policies Page

To assign a Usage Policy from the Policies page,

1. Select the **Usage Policies** node in the Home tree.
2. When the search results display, locate the policy you want to assign in the Search Results table. Click the Policy Name link to open the Usage Policy: *PolicyName* page.
3. Select the Grantees tab.
4. Locate the user or group name in the Grantees table and then click that grantee's Account Name link to open the account.
5. When the Account: *AccountName* page displays, click the Grants tab.
6. Locate the grantee in the Users or Groups table, and use the **Usage Policy** menu in that row to select a different policy.
7. Click **Apply** to add your changes.

5.1.1.9 Deleting Policies

To delete a policy, use the following steps:

1. Locate and select the policy to be deleted.
2. Click the **Delete** icon.
3. When the Confirm Remove dialog displays, click the **Remove** button.

   The policy will be deleted and all accounts using that policy will revert to using the applicable Default Policy.

5.1.2 Working with Targets

This section describes the different tasks you can perform when working with targets in Oracle Privileged Account Manager.

Note: You must be an Oracle Privileged Account Manager administrator with the *Security Administrator* Admin Role to add, edit, or remove targets.

The topics in this section include:

- What Are Targets?
- Adding Targets to Oracle Privileged Account Manager
- Searching for Targets
- Opening a Target
- Removing Targets from Oracle Privileged Account Manager

5.1.2.1 What Are Targets?

A target is a software system that contains, uses, and relies on user, system, or application accounts.

You cannot create targets in, or delete targets from, your environment by using Oracle Privileged Account Manager. Rather, Oracle Privileged Account Manager manages existing targets that were provisioned using other mechanisms.

When you "add" a target in Oracle Privileged Account Manager, you are creating a reference to that target. In effect, you are registering the target and asking Oracle Privileged Account Manager to manage it. When you "remove" a target from Oracle Privileged Account Manager, you are only removing that reference.

5.1.2.2 Adding Targets to Oracle Privileged Account Manager

Note: When adding a target of any Target Type, you must configure a service account (also called an *unattended* account) with privileges that enable that account to

- Search for accounts on the target system
- Modify the passwords of accounts on the target system

For additional information about service accounts, see the description on page 1-3.

Use the following steps to add a target for Oracle Privileged Account Manager to manage:

1. Log in to Oracle Privileged Account Manager and expand the Home accordion.
2. Select the **Targets** node to open the Targets page.
3. Click **Add**, located in the Search Results table toolbar to open a new Target: *Untitled* page displays with two tabs:.
   - **General**. Contains two areas with parameters used to specify Basic Configuration and Advanced Configuration information for the target.
   - **Privileged Accounts**. Lists the privileged accounts currently being managed on the target and enables you to add, open, and remove the accounts that are managed by that target.
4. Select a target type (ldap, unix, or database) from the **Target Type** menu.

   The Target: *Untitled* page refreshes and the target configuration parameters change, based on the selected target type. You must specify all of the required attributes (indicated by an asterisk ***** symbol).

   The following parameters are common to all target types:

   - **Target Name**: Enter a name for the new target.
   - **Description**: Enter a description for this target.
   - **Organization**: Enter the name of an organization to associate with the target.
   - **Domain**: Enter the domain of the target server.
   - **Host**: Enter the host name of the target server.

   The following table describes the remaining Basic Configuration parameters that are unique to each target type.

Table 5–2 Basic Configuration Parameters for Targets

For ldap Target Types	For unix Target Types	For database Target Types
TCP Port: Enter the TCP/IP port to use when communicating with the LDAP server. You can use the up/down arrow icons to increment this value.	**Port**: Enter the port used to connect with the UNIX server. For example, use port 22 for ftp, and port 23 for telnet. You can use the up/down arrow icons to increment this value.	**Database Connection URL**: Enter the JDBC URL used to identify the target system location. For example, **`Oracle`**`:jdbc:oracle:thin:@<`*`host`*`>:<`*`port`*`>:<`*`sid`*`>` Refer to the *Oracle Identity Manager Connector Guide for Database User Management* for information about which special options are supported.
SSL: Enable this box to use Secure Socket Layer (SSL) when connecting to the LDAP server. **Note**: For SSL connectivity, you must import an SSL certificate to the WebLogic server running Oracle Privileged Account Manager. For more information, see Section 3.3.2, "Configuring SSL Communication in Oracle Privileged Account Manager."	**Login User**: Enter the user name to use when connecting to this target.	**Admin User Name**: Enter the administrator's name to use when connecting to this target. **Note**: If you are using the **`sys`** user name, you must enter **`internal_logon=sysdba`** in the **Connection Properties** field located in the Advanced Configuration area. This entry is not required for "system."
Principal: Enter the distinguished name (DN) to use when authenticating to the LDAP server. For example, cn=admin	**Login User Password**: Enter the user's password.	**Admin User Password**: Enter the user's password.
Password: Enter the user's password.	**Login Shell Prompt**: Enter the shell prompt to display when you log in to the target. For example, **`$`** or **`#`**.	**Database Type**: Select the type of database (Oracle or MSSQL) for which the connector will be used. This connector supports the Oracle MSSQL, MySQL, DB2, and Sybase database types. You can also configure this connector to work with custom database types.
Base Contexts: Enter one or more starting points in the LDAP tree to use when searching the tree for users on the LDAP server or when looking for groups where the user is a member. Use a pipe (`|`) to separate values.	**Sudo authorization**: Enable this box if the user requires sudo authorization. Do not enable this box for the `root` user.	
Account User Name Attribute: Enter the attribute to be used as the account's user name. (Default is *uid*.)		

5. You can also specify these optional, advanced configuration parameters.

Table 5–3 Advanced Configuration Parameters for Targets

For ldap Target Types	For unix Target Types	For database Target Types
Uid Attribute: Enter the name of the LDAP attribute that is mapped to the `Uid` attribute.	**Command timeout**: Specify how long (in milliseconds) to wait for the command to complete before terminating that command.	**Connection Properties**: Enter connection properties to use while configuring a secured connection. These properties must be name-value pairs given in following format: `prop1=val1#prop2=val2`.
LDAP Filter for Retrieving Accounts: Enter an optional LDAP filter to control which accounts are returned from the LDAP resource. If you do not specify a filter, Oracle Privileged Account Manager returns only those accounts that include all of the specified object classes.		
Password Attribute: Enter the name of the LDAP attribute that holds the password. When changing a user's password, Oracle Privileged Account Manager sets the new password to this attribute.		
Account Object Classes: Enter one or more object classes to use when creating new user objects in the LDAP tree. Type each object class on its own line. Do not use commas or semicolons to separate entries. Some object classes require that you specify them in their class hierarchy, using a pipe (|) to separate the values.		

6. When you are finished, click **Test** to check the target's configuration.

   If the target's configuration settings are valid, a Test Succeeded message displays.

7. Click **Save** to add your new target on the Oracle Privileged Account Manager server.

You can now associate this target with a privileged account. For instructions, proceed to Section 5.1.3.2, "Adding Privileged Accounts into Oracle Privileged Account Manager."

5.1.2.3 Searching for Targets

If you have administrator privileges, you can search for targets using the following criteria or a combination of these items:

- Target Name
- Target Type
- Host Name
- Domain

To search for a target,

1. Select the Targets node, a target type node, or a domain node in the Home tree.
2. When the Targets tab displays, use the parameter fields in the Search Targets portlet to specify your search criteria.

   Note: If you started by selecting a target type node or a domain node, notice that Oracle Privileged Account Manager automatically inserts that information in the **Target Type** field or the **Domain** field.

3. Click **Search**.

   Review your search results in the Search Results table.

5.1.2.4 Opening a Target

You can open a target to review and edit the target's configuration parameters and its associated privileged account parameters.

Use one of the following methods to open a target:

- Click the target name (an active link) in the Search Results table.
- Select the target row and then click the **Open** icon.

The Target: *targetname* page opens where you can access the target and privileged account information.

5.1.2.5 Removing Targets from Oracle Privileged Account Manager

To remove a target, select the target from the Search Results table and then click the **Remove** icon.

5.1.3 Working with Privileged Accounts

This section describes the different tasks you can perform when working with privileged accounts in Oracle Privileged Account Manager.

Note: ***Administrators determine which accounts are privileged within a particular deployment, and they must configure Oracle Privileged Account Manager to manage those accounts.***

You must be an Oracle Privileged Account Manager administrator with the *Security Administrator* Admin Role to add and manage accounts.

The topics in this section include:

- What is a Privileged Account?
- Adding Privileged Accounts into Oracle Privileged Account Manager
- Searching for Privileged Accounts
- Opening an Account
- Managing Account Passwords
- Checking Out Accounts

- Checking In Accounts
- Removing Privileged Accounts from Oracle Privileged Account Manager

5.1.3.1 What is a Privileged Account?

An account on a target is considered *privileged* in a deployment when that account

- Is associated with elevated privileges
- Is used by multiple end-users on a task-by-task basis
- Requires its usage to be controlled and audited

You cannot create accounts in, or delete accounts from, your environment by using Oracle Privileged Account Manager. Oracle Privileged Account Manager only manages existing accounts that were provisioned using other mechanisms.

When you "add" an account in Oracle Privileged Account Manager, you are creating a reference to that account. In effect, you are registering the account and asking Oracle Privileged Account Manager to manage it. When you "remove" the account from Oracle Privileged Account Manager, you are only removing the reference to that account.

Oracle Privileged Account Manager enables you to manage both system and application accounts. As described in the following Managing System Accounts and Managing Application Accounts sections.

5.1.3.1.1 Managing System Accounts Oracle Privileged Account Manager's primary purpose is to manage privileged system accounts on a supported target system. Oracle Privileged Account Manager does not mandate what constitutes a privileged system account — it can manage any account on a target system. Administrators are responsible for identifying which accounts are privileged. A privileged account is typically a system account that allows a user to perform administration tasks.

Privileged accounts are suitable for management through Oracle Privileged Account Manager if they are used and shared by multiple individuals in the organization and administrators are required to track the use of these accounts.

Administrators perform the following steps to register an account as a privileged account to be managed by Oracle Privileged Account Manager:

1. Add the target to Oracle Privileged Account Manager (if this has not already been done). See Section 5.1.2.2, "Adding Targets to Oracle Privileged Account Manager" for instructions.
2. Add the identified privileged account to the target and assign a Password Policy. See Section 5.1.3.2, "Adding Privileged Accounts into Oracle Privileged Account Manager" and Section 5.1.1, "Working with Policies" for instructions.
3. Grant access to end users directly or by using LDAP roles/groups and assign a Usage Policy. See Section 5.1.4.2, "Granting Accounts to Users" and Section 5.1.1, "Working with Policies" for instructions.

5.1.3.1.2 Managing Application Accounts Applications use application accounts to connect to target systems at run time. Traditionally, administrators set up these accounts once during installation and then they are forgotten. Consequently, application accounts can potentially cause hidden vulnerabilities in your deployment. For example, passwords might become less secure over time because they were created using outdated policies or commonly used deployment passwords might be compromised.

Oracle Privileged Account Manager enables you to better manage application accounts. In particular, for applications that store their application accounts in the Credential Store. These applications consume the account credentials at run time from the Credential Store through the Credential Store Framework.

For example, because an application account is essentially a special version of a system account, you can register an application account in Oracle Privileged Account Manager as described in Section 5.1.3.1.1, "Managing System Accounts." You can then add the corresponding CSF mappings for every application that depends on that account, which is how CSF uniquely identifies a credential stored within CSF, and how an application finds its credential in CSF. For more information about CSF mapping, see "Guidelines for the Map Name" in the *Oracle Fusion Middleware Application Security Guide*.

If you register an account's CSF mappings with Oracle Privileged Account Manager, then every time the account's password changes, Oracle Privileged Account Manager can update the CSF entries that correspond to the registered mappings to reflect the new password and the applications continue to work without service interruption.

> **Note:** Oracle Privileged Account Manager updates, or synchronizes, CSF *only* when a password change occurs.

Additionally, you can apply a Password Policy to these applications that periodically cycles the account password. Cycling the password ensures that the application accounts are always compliant with the latest corporate policies and they remain secure. Oracle Privileged Account Manager performs this task with no service interruption.

Finally, its useful to note that Oracle Privileged Account Manager can support an account as both a system account (shared and used by multiple end-users) and as an application account (only used by an application at run time) at the same time. In this configuration, a human end-user who's been granted access can "check-out" the application account to perform manual administrative operations as that application without disrupting application functionality.

For more information about application accounts, review Section 1.2.4, "Oracle Privileged Account Manager-Managed CSF Credentials."

5.1.3.1.3 Sharing Accounts Oracle Privileged Account Manager enables you to specify whether an account is *shared* or *not shared*.

- **Shared accounts** enable multiple users to check out the account at the same time.
- **Unshared accounts** (Default) enable only one user to check out an account at a time.

Because unshared accounts are more secure, Oracle recommends that you designate an account as shared only if there are compelling business reasons to do so. If sharing is necessary, be sure to read Section 2.4.2, "Securing Shared Accounts."

> **Note:** If you configure a shared account, be aware that a user can still use the password after checking in the account. Oracle Privileged Account Manager does not reset the account password until the last user checks in the account.
>
> This is a security limitation for shared accounts.

5.1.3.2 Adding Privileged Accounts into Oracle Privileged Account Manager

> **Note:** Accounts are always added to a target, so you must add a target object before you can add an account. Refer to Section 5.1.2.2, "Adding Targets to Oracle Privileged Account Manager" for more information.

To add a new privileged account

1. Expand the Home accordion.
2. Use one of the following methods to locate the target where you want to add the account.
   - Expand the Targets node and select the target from the subtree.
   - Click the Targets node and search for the target by providing search criteria in the Search Targets pane.
3. Open the target by clicking the Target Name link in the Search Results table.
4. Select the **Privileged Accounts** tab.
5. Click **Add** in the Search Results table toolbar.

   The Account: *Untitled* page displays with three subtabs:

   - **General**: Use to specify information needed to add the account.
   - **Grants**: Use to associate users and groups (*grantees*) with the account.
   - **Credential Store Framework**: Use to add or remove Credential Store Framework (CSF) mappings for the account.

   Use these tabs and the instructions provided in the following sections to add an account:

   - Adding the Account
   - Adding Grantees
   - Adding CSF Mappings
6. When you are finished, click **Save**.

5.1.3.2.1 Adding the Account To add a new account you must complete the Step 1: Set Target and Step 2: Add Account sections on the General tab as follows:

1. If the **Target Name** is undefined, click the search icon.
2. When the Set Target dialog displays, enter a value in the **Target Name** field and click the **Search** button to locate the target where you want to add the account.

   For example, if you know the target name begins with "r," you can type an **`r`** into the **Target Name** field and click the **Search** button.
3. When the search results display in the Search Results table, select (check) the **Row** box next to a target name and then click **Set**.

   Note that the selected Target Name and its Target Type are displayed on the General tab.
4. In the Step 2: Add Account section, if the **Account Name** is undefined, click the search icon.

5. When the Set Account dialog displays, enter a value in the **Account Name** field and click the **Search** button to locate the account you want to add.

   For example, if you know the account name begins with "s," you can type an **s** into the **Account Name** field and click the **Search** button.

6. When the search results display in the Search Results table, select (check) the **Row** box next to an account name and then click **Set**.

   Note that the selected account is displayed as the Account Name on the General tab.

7. Enable the **Shared Account** box to allow multiple users to check out this account at the same time.

   Note: See Section 5.1.3.1.3, "Sharing Accounts" and Section 5.1.3.6, "Checking Out Accounts" for more information.

8. Specify a **Usage Policy** and a **Password Policy**.

   Note: Oracle Privileged Account Manager automatically assigns the Default Usage Policy and Default Password Policy to new accounts. However, Oracle Privileged Account Manager administrators with the *Security Administrator* or the *User Manager* Admin Role can create new policies.

   You can leave the default policies set or choose a different policy from the **Usage Policy** and **Password Policy** drop-down menus.

   For more information about policies, refer to Section 5.1.1, "Working with Policies."

9. Click **Test** to confirm that the account can be managed by Oracle Privileged Account Manager with these settings.

   If the account configuration settings are valid, a Test Succeeded message displays.

You can now add grantees and CSF mappings to the account. Continue to the following sections for more information.

5.1.3.2.2 Adding Grantees this section provides instructions for adding grantees to a privileged account.

Note: Adding a new account does not automatically grant you access to that account. You must complete the process for adding yourself as a grantee.

You must be an Oracle Privileged Account Manager administrator with the *User Manager* Admin Role to add, edit, or delete grantees.

To associate users and groups with a new account, select the Grants tab and then complete the following steps:

- To associate users, click **Add** from the Users table toolbar.

  1. In the Add Users dialog, enter a name into the **User Name** field and click the arrow icon to search for that user.

2. When the search results display, select (check) each user you want to associate with this account.
3. When you are finished adding users, click **Add** and then click **Close**.

   Oracle Privileged Account Manager adds those user names to the Users table on the Grants tab.

- To associate groups, click **Add** from the Groups table toolbar.
  1. In the Add Group dialog, enter a name into the **Group Name** field and click the arrow icon to search for that group.
  2. When the search results display, select (check) each group you want to associate with this account.
  3. When you are finished adding groups, click **Add** and then click **Close**.

     Oracle Privileged Account Manager adds those group names to the Groups table on the Grants tab.

5.1.3.2.3 Adding CSF Mappings Oracle Privileged Account Manager enables you to securely store and synchronize account credentials with the Oracle Credential Store Framework (CSF). This capability is useful for managing the lifecycle of application passwords stored in CSF.

When you configure CSF synchronization for an account, Oracle Privileged Account Manager changes the account password based on the assigned Usage Policy.

> **Note:** Oracle Privileged Account Manager updates, or synchronizes, CSF *only* when a password change occurs.

To add CSF mappings to an account, complete the following steps:

1. Select the Account Name link from the Search Results table.
2. When the Account: *AccountName* page displays, select the Credential Store Framework tab and click **Add**.
3. Enter the following information:
   - **Administration Server URL**. Enter the server URL in this format, protocol://*listen-address*:*listen-port*
   - **Username** and **Password**. Enter the user's credentials.
   - **Mapping**. Enter a map name.
   - **Key**. Enter a unique key to identify the credential.
4. Click **Add** again to create another mapping. You can create as many CSF mappings as needed.

5.1.3.3 Searching for Privileged Accounts

You can search for accounts by using one or more of the following parameters:

- Account name
- Target name
- Target type
- Domain

To search for accounts, use the following steps:

1. Select the **Accounts** node in the Home tree.
2. When the Accounts tab displays, enter your search criteria in the Search Accounts pane and then click **Search**.

   For example, to search for a list of all the accounts on a particular target, enter the **Target Name** and click **Search**. Your search results are displayed in the Search Results table.

   Note: You can use the **Status** menu, located above the Search Results table, to control the search results based on the account status. See the table in Section 3.4.5, "Working with a Search Results Table" for more information.

3. To perform another search, click **Reset**.

5.1.3.4 Opening an Account

You can open an account to view or edit the configuration parameters for that account.

Use one of the following methods to open an account:

- Click the account name (an active link) in the Search Results table.
- Select the account row and then click **Open Account**.

The Account: *accountname* page opens where you can access information about the associated target, general account parameters, the grantees, and the CSF mapping.

5.1.3.5 Managing Account Passwords

Oracle Privileged Account Manager provides two options for managing account passwords:

- **Show Password**. Displays the password for an account.

  If you forget the password for a checked- out account, you can use this feature to view that password again.

  Any user can use **Show Password** to review the current password for a account they have checked out. However, they cannot access passwords after the account is checked back in or view passwords for accounts that are checked out by other users. In these cases, clicking **Show Password** will cause an error.

  Administrators with the *Security Administration* or *User Manager* Admin Role, who can access all system and target service accounts, can use this feature to view current the password for both checked out and checked in privileged accounts.

- **Reset Password**. Resets the existing account password.

  If Security Administrators do not want to use randomized password generation, they can manually set a password of their choosing. For example, administrators might prefer to set a simple, easy-to-type password for one time use, such as during a system upgrade.

  Only administrators with the *Security Administration* Admin Role can reset account passwords.

See Section 5.1.3.5.1, "Showing an Account Password" and Section 5.1.3.5.2, "Resetting an Account Password" for instructions.

Note: You can also perform both password management actions by using the Oracle Privileged Account Manager command line tool. Refer to Section A.2.31, "`showpassword` Command" and Section A.2.21, "`resetpassword` Command" for instructions.

Oracle Privileged Account Manager audits both types of password management actions to keep track of password access.

5.1.3.5.1 Showing an Account Password To view the password for a selected account,

1. Select the account's row in the Search Results table.

Note: Do not click an active link in the table, such as the account name, or you will open the account

---

2. Click the **Show Password** icon located above the table.

   A message displays with the name of the selected account and its password.

5.1.3.5.2 Resetting an Account Password If necessary, you can manually reset the password for a selected account as follows:

1. Ensure the privileged account is checked in.

   You cannot perform a manual password reset if the account is in a checked-out state.

2. Select the account row in the Search Results table.

Note: Do not click an active link in the table, such as the account name, or you will open the account

---

3. Click the **Reset Password** icon located above the table.

   The Reset Password dialog displays.

4. Type a password into the **New Password** field and click **Save**.

   You can use a password string of your choosing. The string does not have comply with the Oracle Privileged Account Manager Password Policy because the Password Policy is used for randomized password generation.

   A message displays with the name of the selected account and its password.

5.1.3.6 Checking Out Accounts

Any administrator or end user can check out an account if they have been granted access to that account. (See Section 5.1.4, "Working with Grantees" for more information.)

Note: You must be an administrator with the *Security Administration* Admin Role to modify or remove an account.

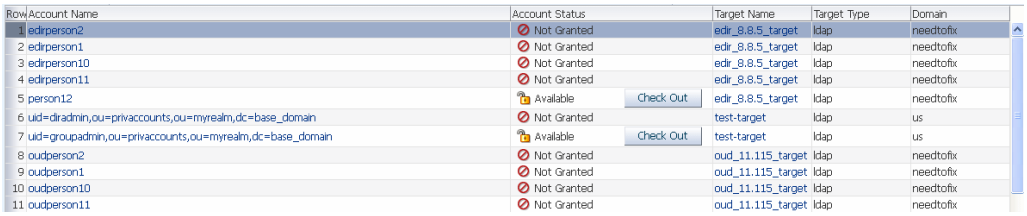
Privileged accounts are *not shared* by default, which means when one user checks out the account, it becomes unavailable to other users and prevents conflicting actions.

However, administrators can configure *shared* accounts, which enables multiple users to check out the account at the same time. (Refer to Section 5.1.3.1.3, "Sharing Accounts" for more information.)

The steps for checking out an account are as follows:

1. Expand the Accounts node on the Home accordion, and select the account target.
2. When the Accounts tab displays, locate the account you want to check out in the Search Results table.
   - If the account is available for check out, the Account Status is *Available* and the **Check-out** button is displayed.
   - If the account is not available for check out, then the Account Status is *Not Granted*.

Figure 5–1 Account Available for Checkout



3. Click the **Check-out** button.

   When the Check-Out Account dialog displays, you can enter a comment in the **Comments** field, and then click **Checkout**.

   If the check-out is successful,

   - For an *unshared* account, the Account Status changes to Checked-Out, the **Check Out** button changes to a **Check In** button, and Oracle Privileged Account Manager lists the account on the My Checked-out Accounts page.
   - For a *shared* account, the Account Status remains Available, the **Check Out** button remains, and Oracle Privileged Account Manager lists the account on the My Checked-out Accounts page.

5.1.3.7 Checking In Accounts

Any administrator or end user can check in accounts.

> **Note:** You can also use the Search Accounts page, the Oracle Privileged Account Manager command line tool, or the RESTful interface to check-in accounts.

The steps for checking in an account are as follows:

1. Select **My Checked-out Accounts** on the Home accordion.

   The My Checked-out Accounts page displays with all of your checked-out accounts listed in the Search Results table.
2. Select (check) the account(s) you want to check in.
3. Click the **Check-in** icon located above the table.

4. When the Check-in Accounts dialog displays, click the **Check In** button.

   If the check-in is successful, Oracle Privileged Account Manager removes the account name(s) from the My Checked-out Accounts table and the account becomes Available for check-out again.

5.1.3.8 Removing Privileged Accounts from Oracle Privileged Account Manager

You can remove a privileged account from Oracle Privileged Account Manager by using the Targets page or the Search Accounts page.

From the Target Page

To remove an account from a target,

1. Expand the Home accordion.
2. Locate the target from which you want to remove the account.
   - Expand the Targets node and select the target from the subtree.
   - Click the Targets node and search for the target by providing search criteria in the Search Targets pane.
3. Click the target name in the Search Results table to open the target.
4. Select the Privileged Accounts tab.
5. In the Search Results table, select the account to be removed and then click **Remove**.
6. When you are finished, click the **Apply** button located at the top of the page.

From the Search Accounts Page

To remove an account from the Search Accounts page,

1. Expand the Home accordion.
2. Click the Accounts node, target type node, or domain node in the Home tree to open the Search Accounts page.
3. Locate the account to be removed.
   - If you selected the Accounts node, use the fields in the Search Accounts section to search for the account. Your search results are displayed in the Search Results table.
   - If you selected a target type or domain node, the account displays in the Search Results table.
4. In the Search Results table, select the account to be removed, and then click **Remove**.
5. When you are finished, click the **Apply** button located at the top of the page.

5.1.4 Working with Grantees

This section describes the different tasks you can perform when working with grantees in Oracle Privileged Account Manager.

> **Note:** You must be an Oracle Privileged Account Manager administrator with the *User Manager* Admin Role to add, edit, or delete grantees.

The topics in this section are:

5.1.4.1 What Are Grantees?

Grantees are users or groups in the ID Store that have been granted access to a privileged account managed by an Oracle Privileged Account Manager administrator. Users cannot check out a privileged account unless they have been granted access to that account.

5.1.4.2 Granting Accounts to Users

Use the following steps to grant access to a privileged account:

1. Expand the Home accordion.
2. Click **Accounts** or a sub-node to locate the account to which you want to grant access.

   If necessary, use the Search Accounts portlet to search for the account as described on page 5-21.
3. Select the account name in the Search Results table.

   The General, Grants, and Credential Store Framework tabs display.
4. Select the Grants tab.

   If any users are already associated with this account, their names are listed in the table in the Users area.
5. Click **Add** to open the Add Users dialog.
6. In the Add Users dialog, enter all or part of a user name and then click the arrow icon to browse for the user name to add.

   For example, to grant access to the sec_admin user, you can type **sec** into this field and the search results will include any existing user name containing those letters.
7. Select (check) the user name and then click **Add** to add the selected user as a grantee.
8. Click **Close** to close the dialog.

   The new user's name displays in the table.

> **Note:** At this point, the Default Usage Policy is automatically assigned to the user. However, you can use the Usage Policy menu to select a different policy for that user.

5.1.4.3 Granting Accounts to Groups

Use the following steps to grant access to a privileged account:

1. Expand the Home accordion.

2. Click **Accounts** or a sub-node to locate the account to which you want to grant access.

   If necessary, use the Search Accounts portlet to search for the account as described on page 5-21.

3. Select the account name in the Search Results table.

   The General, Grants, and Credential Store Framework tabs display.

4. Select the Grants tab.

   If any groups are already associated with this account, their names are listed in the table in the Groups area.

5. Click **Add** to open the Add Groups dialog.

6. In the Add Groups dialog, enter all or part of a group name and then click the arrow icon to browse for the group name to add.

   For example, to grant access to the OPAM_USER_MANAGER group, you can type **opam** into this field and the search results will include any existing group names containing those letters.

7. Select (check) the group name and then click **Add** to add the selected group as a grantee.

8. Click **Close** to close the dialog.

   The new group name displays in the table.

> **Note:** At this point, the Default Usage Policy is automatically assigned to the group. However, you can use the Usage Policy menu to select a different policy for that group.

5.1.4.4 Searching for Grantees

If you have administrator privileges, you can search for grantees by using the following criteria or a combination of these items.

- For a user grantee
  - User Name
  - First Name
  - Last Name
  - Target Name
  - Account Name
- For a group grantee
  - Name
  - Description
  - Target Name
  - Account Name

Use the following steps to search for a grantee:

1. Select **Users** or **Groups** under the Grantees node on the Home tree.

2. When the Search User or Search Group portlet displays on the right, enter your search criteria into one or more of the fields provided.
3. Click **Search**.

Review your search results in the Search Results table.

5.1.4.5 Opening a Grantee

You can open a grantee to view information about that user or group grantee.

Use one of the following methods to open a grantee:

- Click the User name or the Group name (an active link) in the Search Results table.
- Select the User or Group row and then click the **Open** icon.

The User: *username* or the Group: *groupname* page opens where you can review the information about that grantee.

5.1.4.6 Removing Grantees from an Account

To remove one or more grantees from an account

1. Open the account and select the Grants tab.
2. Select the user or group row in the Search Results table.
3. Click the **Remove** icon.
4. When you are prompted to confirm the removal, click the **Remove** button to continue, (or **Cancel** to terminate the operation).

   The prompt closes and the user or group is removed from the table.

5.1.5 Working with Reports

Oracle Privileged Account Manager reports are real-time reports that provide information about the current status of accounts and targets being managed by Oracle Privileged Account Manager.

> **Note:** You must be an Oracle Privileged Account Manager administrator with the *Security Auditor* Admin Role to open and review Oracle Privileged Account Manager reports.

The topics in this section include:

- Working with Deployment Reports
- Working with Usage Reports
- Working with Failure Reports

To view a report, expand the Reports accordion and click a Report link. The report information is displayed in the Reports page on the right.

5.1.5.1 Working with Deployment Reports

Select the **Deployment Report** link to view information about how targets and privileged accounts are currently deployed.

Information about the deployment is organized into three portlet:

- **Target and Accounts Deployment table**. Provides a list of targets, including their target type and host names. Expand the arrow icon next to a target name to view the accounts associated with that target.

  Tip: You can click a link in the Target/Account column to open the configuration page for that target or account.

- **Target Distribution**. This portlet illustrates how targets are distributed within your deployment.
- **Account Distribution**. This portlet illustrates how accounts are distributed within your deployment, by Organization.

Use the **Show** and **Filter** drop-down menus to control how the report content is displayed. For example, use the **Show** menu to view all targets or filter the results to view a particular target. You can use the **Filter** menu to view the target and account distribution in bar chart, pie chart or tabular format.

5.1.5.2 Working with Usage Reports

Select the **Usage Report** link to view information about how privileged accounts are currently being used in your deployment. This information displays in the following portlets:

- **Account Usage**. This portlet provides a list of targets, the target types, host names, and the last checked out date. Expand the arrow icon next to a target name to view the accounts associated with that target.
- **Checked Out Accounts**. This portlet illustrates which targets are checked out within your deployment.

Use the **Show** and **Filter** drop-down menus to control how the report content is displayed. For example, select **Show** to view just currently checked out accounts or accounts that were checked out in the last hour, day, or week. You can use the **Filter** menu to view the report information as a bar chart, pie chart, or in tabular format.

5.1.5.3 Working with Failure Reports

The **Failure Report** provides information about the current state of target and account failures. This information displays in the following portlets:

- **Targets and Accounts Failures**. This portlet provides a list of targets, the target status, last error message, and the last failure date. Expand the arrow icon next to a target to view the accounts associated with that target.
- **Target Failures**. This portlet illustrates the target failures within your deployment.
- **Account Failures**. This portlet illustrates the account failures within your deployment.

Use the **Show** and **Filter** drop-down menus to control how the report content is displayed. For example, select **Show** to view the errors that occurred during the last 24 or 48 hours, the last week, or the last 30 days. You can use the **Filter** menu to view the report information as a bar chart, pie chart, or in tabular format.

5.2 Working with Self-Service

This section provides instructions for users working with Oracle Privileged Account Manager.

The topics include:

5.2.1 Self-Service Workflow

This section describes the basic workflow for self-service users:

1. Searching for an account
2. Checking out the account
3. Viewing checked-out accounts
4. Checking in accounts

5.2.2 Searching for Accounts

You can search for an account by following the instructions provided in Section 5.1.3.3, "Searching for Privileged Accounts."

5.2.3 Checking Accounts Out and In

To check out a privileged account granted to you, see Section 5.1.3.6, "Checking Out Accounts."

To check an account back in again, follow the instructions provided in Section 5.1.3.7, "Checking In Accounts."

5.2.4 Viewing Checked-Out Accounts

To review which accounts you currently have checked-out, select **My Checked-out Accounts** on the Home accordion.

The My Checked-out Accounts page displays with all of your checked-out accounts listed in the Search Results table.

5.3 Moving from a Test Environment to a Production Environment

For information about moving Oracle Fusion Middleware components from one environment to another, see "Moving from a Test to a Production Environment" in *Oracle Fusion Middleware Administrator's Guide*.

For information about moving Identity Management components, including Oracle Privileged Account Manager, from a test environment to a production environment, see "Moving Identity Management Components to a Target Environment" in *Oracle Fusion Middleware Administrator's Guide*.

6

Managing Oracle Privileged Account Manager Auditing and Logging

This chapter describes how to configure and use Oracle Privileged Account Manager's auditing and logging functionality.

The topics in this chapter include:

- Section 6.1, "Understanding Oracle Privileged Account Manager Auditing"
- Section 6.2, "Understanding Oracle Privileged Account Manager Logging"

6.1 Understanding Oracle Privileged Account Manager Auditing

Oracle Privileged Account Manager audits all security events that occur under its purview, which gives you better visibility into how privileged accounts are used within your organization and enables you to effectively manage sensitive information.

Specifically, the Oracle Privileged Account Manager audit logger logs any events that modify entity states; such as when you add, modify, or remove new accounts, targets, or policies.

The following table describes all of the event categories and event types for which an audit can be generated:

Table 6–1 Audited OPAM Events

Event Category	Event Types	Description
Account Management		Events related to managing *principal* accounts **Note**: A principal can be an end-user or a pseudo-user (a service within the system).
	Add Account	Adding users, groups, or any other principal accounts
	Change Password	Changes to user passwords
	Disable Account	Disabling users, groups, or any other principal accounts
	Enable Account	Enabling users, groups, or any other principal accounts
	Modify Account	Modifying account attributes
	Query Account	Queries to a user's account
	Remove Account	Removing users, groups, or any other principal accounts

Table 6–1 (Cont.) Audited OPAM Events

Event Category	Event Types	Description
Policy Management		Events related to managing policies
	Create Policy	Creating policies
	Delete Policy	Deleting policies
	Modify Policy	Modifying policies
	Query Policy	Querying policies
Target Management		Events related to managing targets
	Add Target	Adding targets
	Modify Target	Modifying targets
	Query Target	Querying targets
	Remove Target	Removing targets

Logging these audit events creates a processing history that allows reporting tools to gather statistics, as described in Section 6.1.2, "Understanding Oracle Privileged Account Manager Audit Reports."

6.1.1 Configuring Auditing in Oracle Privileged Account Manager

You can configure Oracle Privileged Account Manager to save audit events into a database or a file. When a database is not available, Oracle Privileged Account Manager saves its audit logs into this file,

`DOMAIN_HOME/servers/<opamserver>/logs/auditlogs/opam#11.1.2.0.0`

You can also configure Oracle Privileged Account Manager to deploy audit reports in BI Publisher (version 11.1.1.5.0 or higher), and you can use BI Publisher to view audit events in the database.

The following topics provide instructions for configuring auditing in Oracle Privileged Account Manager:

- Configuring File-Based Auditing in Oracle Privileged Account Manager
- Configuring Database-Based Auditing in Oracle Privileged Account Manager
- Deploying Oracle Privileged Account Manager Audit Reports in BI Publisher
- Setting the Audit Logging Levels

6.1.1.1 Configuring File-Based Auditing in Oracle Privileged Account Manager

Use the following steps to configure Oracle Privileged Account Manager:

> **Note:** These instructions assume you have already installed a WebLogic server.

1. Open a command window and change directory (`cd`) to

   `DOMAIN_HOME/config/fmwconfig/`

2. Edit the `jps-config.xml` file by changing the `audit.filterPreset` parameter from `None` to `All`, `Medium`, or `Low` depending on the type of events to be audited.

Note: See Section 6.1.1.4, "Setting the Audit Logging Levels" for more information.

For example,

```
<serviceInstance location="./audit-store.xml" provider="audit.provider"
name="audit.db">
<property name="audit.filterPreset" value="All"/>
<property name="audit.maxDirSize" value="0"/>
<property name="audit.maxFileSize" value="104857600"/>
<property name="audit.loader.jndi" value="jdbc/AuditDB"/>
<property name="audit.loader.interval" value="15"/>
<property name="audit.loader.repositoryType" value="File"/>
<property name="auditstore.type" value="file"/> </serviceInstance>
```

3. Restart the Oracle Privileged Account Manager server.

Note: For detailed information about starting a Managed Server, see "Starting or Stopping the Oracle Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

After the server restarts, audit logs will start appearing in this location:

DOMAIN_HOME/servers/<*opamserver*>/logs/auditlogs/opam#11.1.2.0.0

6.1.1.2 Configuring Database-Based Auditing in Oracle Privileged Account Manager

This section describes how to configure database-based auditing in Oracle Privileged Account Manager.

Prerequisites

If you want to generate audit reports from a database and BI Publisher, then you must install

- A database
- The Oracle Repository Creation Utility application, which is used to create a schema and load a repository into the database.

Note: For information about installing and working with the Repository Creation Utility, refer to *Oracle Fusion Middleware Repository Creation Utility User's Guide* available at http://www.oracle.com/technology/documentation/index.html

For information about installing and configuring BI Publisher, refer to "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

To configure database-based auditing:

1. Download the Repository Creation Utility `.zip` file from Oracle Technology Network (OTN):

   http://www.oracle.com/technology/

2. Run `./rcu` to load the audit schema into the database.

   By default, this step creates the `dev_iau` user in the database and loads tables under this user.

3. Log in to the WebLogic Server Administrative Console to configure WebLogic.

   http://*adminserver_host*:*adminserver_port*/console

4. Navigate to **Services** > **Data Sources**.

   Click **New** to create a new data source.

5. Enter the following information to create a JDBC data source.

   a. Type `jdbc/AuditDB` in the **Name** field.

   b. Leave the **JNDI Name** field blank.

   c. Select Oracle's Driver (Thin) for instance connections that are Versions 9.0.1 and later.

   d. Leave **Transaction Options** set to the default setting.

   e. Specify the DB name, host, and listener port.

   f. Specify the Audit DB user (for example, `dev_iau`) and apply it to both the Admin and Managed servers.

   g. Test the connection and apply it to both the Admin and Managed Servers.

   Note: Refer to "Create JDBC Data Sources" in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* for more information about creating a JDBC data source and deploying it on a server.

   ---

6. Edit the `jps-config.xml` file, located in *DOMAIN_HOME*`/config/fmwconfig/jps-config.xml`, as follows:

   a. Change the `<property value="File" name="audit.loader.repositoryType"/>` parameter to `<property value="Db" name="audit.loader.repositoryType"/>`.

   b. Change the `audit.filterPreset` parameter from `None` to `All`, `Medium`, or `Low` depending on the type of events to be audited.

   Note: See Section 6.1.1.4, "Setting the Audit Logging Levels" for more information.

   For example,

```
<serviceInstance location="./audit-store.xml" provider="audit.provider"
name="audit">
<property name="audit.filterPreset" value="All"/>
<property name="audit.maxDirSize" value="0"/>
<property name="audit.maxFileSize" value="104857600"/>
<property name="audit.loader.jndi" value="jdbc/AuditDB"/>
<property name="audit.loader.interval" value="15"/>
<property name="audit.loader.repositoryType" value="Db"/>
<property name="auditstore.type" value="file"/> </serviceInstance>
```

7. Restart the Oracle Privileged Account Manager server.

6.1.1.3 Deploying Oracle Privileged Account Manager Audit Reports in BI Publisher

This section describes how to deploy Oracle Privileged Account Manager audit reports in BI Publisher, a component used to manage and deliver reports.

Use the following steps:

1. Install and configure Oracle Business Intelligence Publisher (BI Publisher) version 11.1.1.5.0 or higher if it is not already installed.

   Refer to "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator* for instructions.

2. After installing BI Publisher, locate the following directory in the WebLogic domain:

   Note: BI Publisher can be deployed on the same host or in a different domain.

   BI_DOMAIN_HOME/config/bupublisher/repository/Reports

3. Locate the `opam_product_BIP11gReports_11_1_1_6_0.zip` file in the following directory:

   ORACLE_HOME/opam/reports

   Unzip this file into the `Reports` folder noted in step 2.

4. To set up the catalog and configure data sources, open a browser window and enter the URL for BI Publisher.

   The format for this URL is

   http://*hostname*:*port*/xmlpserver/

   For example

   http://*localhost*:7001/xmlpserver/

5. When the BI Publisher login page displays, log in as a user with WebLogic privileges and click **Sign In**.

6. Set up the catalog as follows:

   a. Select **Administration** > **System Maintenance** > **Server Configuration**.

   b. Open the Catalog dialog, select the BI Publisher - File System from the **Catalog Type** menu, and enter the following path in the **Path** field:

      BI_DOMAIN_HOME/config/bupublisher/repository/Reports

   c. Log in as an administrator.

   d. Click **Catalog** to open the `Shared Folder/ Oracle Privileged Account Manager` folder.

      Note: If this folder does not display, restart the application from the WebLogic console.

7. One JDBC (Oracle Privileged Account Manager JDBC) connection is required for Oracle Privileged Account Manager reports. Use the following steps to define an Oracle Privileged Account Manager JDBC connection and define the data sources:

   a. Click the Administration link found on the right side of the BI Publisher page.

      The BI Publisher Administration page displays. (Note the Data Sources section on this page.)

   b. Click the **JDBC Connection** link found in the Data Sources section.

   c. When the Data Sources page displays, click Add Data Source in the JDBC section to create a JDBC connection to your database.

   d. On the Add Data Source page, enter the following information:

Data Source Name	Oracle Privileged Account Manager JDBC
Driver Type	Select a driver type to suit your database (for example, Oracle 10g or Oracle 11g).
Database Driver Class	`oracle.jdbc.driver.OracleDriver` (Define a driver class to suit your database.)
Connection String	Provide the database connection details. For example, *hostname*:*port*:*sid*.
User name	Provide the Oracle Privileged Account Manager Audit DB user name.
Password	Provide the Oracle Privileged Account Manager Audit DB user password.

      If the connection to the database is established, a confirmation message is displayed indicating the success.

   e. Click Apply.

      You should see this newly defined connection (Oracle Privileged Account Manager JDBC) in the list of JDBC Data Sources.

   f. Navigate to Oracle Privileged Account Manager Audit Reports.

      The Catalog page is displayed as a tree structure on the left side of the page with details on the right.

   g. Expand `Shared Folders` and select the `Oracle Privileged Account Manager` folder to view all of the objects in that folder.

8. Use Oracle Identity Navigator to configure a connection to the BI Publisher server.

   Refer to "Creating a Connection to BI Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator* for the necessary instructions.

When you configure the connection successfully, the My Reports section of the Oracle Identity Navigator Dashboard page will contain the link, **Click here to create reports**. In addition, users with the Security Auditor role can now perform the following tasks:

- View Oracle Identity Management BI Publisher reports and audit reports

> **Note:** Oracle Privileged Account Manager provides a set of out-of-the box audit reports that are integrated with BI Publisher 11g and the Oracle Fusion Middleware Audit Framework. Oracle Privileged Account Manager generates these reports based on audit events logged in the audit store. Refer to Section 6.1, "Understanding Oracle Privileged Account Manager Auditing" for more information.

- Select and add reports to the My Reports list
- View and run any reports for which you have access privileges

You can now navigate in BI Publisher and use the Oracle Privileged Account Manager 11g BI reports.

6.1.1.4 Setting the Audit Logging Levels

To change the amount of audit logging provided by Oracle Privileged Account Manager, use the following steps:

1. Open a command window and change directory (`cd`) to

   DOMAIN_HOME`/config/fmwconfig/`

2. Locate the `jps-config.xml` file.
3. Change the `audit.filterPreset` parameter from `None` to one of the following settings:
   - `All`: Logs all event types.
   - `Medium`: Logs all event types in the `PolicyManagement` and `TargetManagement` categories, and the following event types in the `AccountManagement` category:
     - `ChangePassword`
     - `CheckinAccount`
     - `CreateAccount`
     - `DeleteAccount`
     - `DisableAccount`
     - `EnableAccount`
     - `ModifyAccount`
     - `QueryAccount`
   - `Low`: Logs the following event types
     - In the `AccountManagement` category: `ChangePassword`, `CheckinAccount`, `CreateAccount`, `DeleteAccount`, `DisableAccount`, `EnableAccount`, and `ModifyAccount`
     - In the `PolicyManagement` category: `CreatePolicy`, `DeletePolicy`, and `ModifyPolicy`
   - In the `TargetManagement` category: `CreateTarget`, `DeleteTarget`, and `ModifyTarget`

   For example,

   ```
   <serviceInstance location="./audit-store.xml" provider="audit.provider"
   name="audit">
   ```

```
<property value="All" name="audit.filterPreset"/>
<property value="0" name="audit.maxDirSize"/>
<property value="104857600" name="audit.maxFileSize"/>
<property value="jdbc/AuditDB" name="audit.loader.jndi"/>
<property value="15" name="audit.loader.interval"/>
<property value="File" name="audit.loader.repositoryType"/>
<property value="file" name="auditstore.type"/> </serviceInstance>
```

4. Restart the Oracle Privileged Account Manager server.

> **Note:** For detailed information about starting a Managed Server, see "Starting or Stopping the Oracle Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

After the server restarts, audit logs will start appearing in the following location:

DOMAIN_HOME/servers/<*opamserver*>/logs/auditlogs/opam#11.1.2.0.0

6.1.2 Understanding Oracle Privileged Account Manager Audit Reports

Oracle Privileged Account Manager supplies a set of default audit reports that are integrated with BI Publisher 11g and the Oracle Fusion Middleware Audit Framework. Oracle Privileged Account Manager generates these reports based on the audit events logged in the audit store.

The default audit report types include:

- Error and Exception reports, such as authentication and authorization failures
- User Activities reports, including account check-out and check-in history
- Operational reports, including grantee assignments and any targets, accounts, and policies that have been added, edited, or removed
- All Events reports, including all audit events that have been logged in the audit store

Oracle Privileged Account Manager audit reports can show who checked out an account and on which system it was checked out, justifications, requests for a system that is already checked out, and requests for a system to which a user does not have privileges.

For example, the following figure shows a typical Oracle Privileged Account Manager audit report as viewed in BI Publisher.

> **Note:** You can view Oracle Privileged Account Manager audit reports in BI Publisher.

Figure 6–1 Example Oracle Privileged Account Manager Audit Report

ORACLE

Oracle Privileged Account Manager

Category	Event	User ID	Status	Target	Resource ID	Time
AccountManagement	QueryAccount	sec_admin	1	Query Accounts: type - , domain - , name -		4/10/12 4:40 PM Pacific Time
TargetManagement	QueryTarget	sec_admin	1	Query Target: Get Target Attributes"		4/10/12 4:40 PM Pacific Time
TargetManagement	CreateTarget	sec_admin	1			4/10/12 4:40 PM Pacific Time
TargetManagement	QueryTarget	sec_admin	1	bldap	2b92b7603d9949bda81805b73fb5b5da	4/10/12 4:40 PM Pacific Time
TargetManagement	QueryTarget	sec_admin	1	Query Target: Get Target Type Tree		4/10/12 4:40 PM Pacific Time
AccountManagement	CreateAccount	sec_admin	1			4/10/12 4:41 PM Pacific Time
TargetManagement	QueryTarget	sec_admin	1	bldap	2b92b7603d9949bda81805b73fb5b5da	4/10/12 4:41 PM Pacific Time
AccountManagement	QueryAccount	sec_admin	1	bldap:cn=John Andersons,ou=Field Support,ou=IT,ou=Americas,o=IMC,c=us	b7fe15205746440fa749a98bcdae8ac3	4/10/12 4:41 PM Pacific Time
AccountManagement	QueryAccount	sec_admin	1	bldap:cn=John Andersons,ou=Field Support,ou=IT,ou=Americas,o=IMC,c=us	b7fe15205746440fa749a98bcdae8ac3	4/10/12 4:41 PM Pacific Time
AccountManagement	CreateAccount	sec_admin	1			4/10/12 4:41 PM Pacific Time
TargetManagement	QueryTarget	sec_admin	1	bldap	2b92b7603d9949bda81805b73fb5b5da	4/10/12 4:41 PM Pacific Time
AccountManagement	QueryAccount	sec_admin	1	bldap:cn=John Andersons,ou=Field Support,ou=IT,ou=Americas,o=IMC,c=us	b7fe15205746440fa749a98bcdae8ac3	4/10/12 4:41 PM Pacific Time
AccountManagement	QueryAccount	sec_admin	1	bldap:uid=abc_test,cn=users,c=us	0042faf28e254ff3b7fd153965e11415	4/10/12 4:41 PM Pacific Time
AccountManagement	QueryAccount	sec_admin	1	bldap:uid=abc_test,cn=users,c=us	0042faf28e254ff3b7fd153965e11415	4/10/12 4:41 PM Pacific Time
AccountManagement	CreateAccount	sec_admin	1			4/10/12 4:41 PM Pacific Time
TargetManagement	QueryTarget	sec_admin	1	bldap	2b92b7603d9949bda81805b73fb5b5da	4/10/12 4:41 PM Pacific Time
AccountManagement	QueryAccount	sec_admin	1	bldap:cn=John	b7fe15205746440fa749a98bcdae8	4/10/12 4:41 PM Pacific Time

Notice that this report provides the following information:

- **Category**: Event category
- **Event**: Type of event that occurred
- **User ID**: User that initiated the event
- **Status**: Event results, where 1 is success and 0 is a failure
- **Target**: Target on which the event occurred
- **Resource ID**: Resource identifier
- **Time**: Date and time the event occurred

6.2 Understanding Oracle Privileged Account Manager Logging

The Oracle Privileged Account Manager generic logger takes care of all logs not recorded by the audit logger, which includes debugging statements and exception messages. Processing tools can use these logs to diagnose problems that occur within the Oracle Privileged Account Manager server.

Oracle Privileged Account Manager-related log files are stored in the following locations:

DOMAIN_HOME/servers/*adminserver*/logs
DOMAIN_HOME/servers/*opamserver*/logs

6.2.1 Configuring Basic Logging

To change the out-of-the-box logging for Oracle Privileged Account Manager,

1. Manually edit the `opam-logging.xml` file, which is located in the following directory:

   DOMAIN_HOME`/config/fmwconfig/opam`

2. Restart the OPAM server (usually the Managed Server).

> **Note:** For more information about implementing logging functionality and setting log levels, refer to "Logging Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference* and "Managing Log Files and Diagnostic Data" in the *Oracle Fusion Middleware Administrator's Guide*.

6.2.2 Example Logging Data

This figure shows some example logging data as viewed from the WebLogic console.

Figure 6–2 Example Logging Report

Date	Subsystem	Severity	Message ID	Message
Oct 13, 2011 10:48:25 AM PDT	OPAM	Info	BEA-000000	UIResource/getAccount
Oct 13, 2011 10:48:27 AM PDT	OPAM	Info	BEA-000000	PrivilegedAccountResource/updateAccount
Oct 13, 2011 10:48:28 AM PDT	OPAM	Info	BEA-000000	UIResource/getAccount
Oct 13, 2011 10:48:44 AM PDT	OPAM	Info	BEA-000000	PrivilegedAccountResource/checkout
Oct 13, 2011 10:48:48 AM PDT	OPAM	Info	BEA-000000	ContextManager added session 7920930130191964with result = true
Oct 13, 2011 10:50:26 AM PDT	OPAM	Info	BEA-000000	UIResource/getAllCheckedOutAccounts
Oct 13, 2011 10:50:35 AM PDT	OPAM	Info	BEA-000000	PrivilegedAccountResource/checkIn
Oct 13, 2011 10:50:39 AM PDT	OPAM	Info	BEA-000000	ContextManager removed session 7920930130191964with result = true

Notice that this report provides the following information:

- Date and timestamp when the event occurred
- Subsystem on which the event occurred
- Message severity
- Message ID
- Message describing the operation that was performed

Part III

Advanced Administration

This part provides information about performing advanced administration tasks for Oracle Privileged Account Manager, and it contains the following chapters:

- Configuring Oracle Privileged Account Manager for Integrated Solutions

7

Configuring Oracle Privileged Account Manager for Integrated Solutions

This chapter explains how to configure Oracle Privileged Account Manager for integration with commonly used directory and identity management technologies and contains the following topics:

- Section 7.1, "Integrating with Oracle Identity Manager"
- Section 7.2, "Integrating with Oracle Access Management Access Manager"

7.1 Integrating with Oracle Identity Manager

This section describes how you can use Oracle Identity Manager to manage access to the LDAP groups that are also Oracle Privileged Account Manager grantees.

Integration with Oracle Identity Manager enables Oracle Privileged Account Manager to

- Manage the identity lifecycle from hiring to retirement
- Provide a native ability to automate adding and removing users to the proper LDAP groups based on their HR system updates
- Provide the ability to manually request access to accounts
- Support the ability to get approvals for requests
- Support reporting that you can use for attestation reporting; either to augment or in-lieu of Oracle Privileged Account Manager's own reporting.

The topics in this section include:

- Overview
- Configuring Oracle Privileged Account Manager for the Integration
- Integrating the Oracle Identity Manager Core
- Configuring an Oracle Identity Manager Administrator

7.1.1 Overview

Oracle Privileged Account Manager is optimized for managing shared and privileged accounts, such as root on an UNIX system.

Oracle Privileged Account Manager determines which users can check out passwords for accounts on a target, based on the grants those users have received. Grants can be

made directly or through membership in groups. The groups themselves can be static or dynamic.

Ideally, the LDAP groups should match your enterprise roles. For example, if you have a "Data Center Product UNIX Administrators" enterprise role, you should have a corresponding LDAP group. The benefit of this match is that you can use these groups to control access to other applications besides Oracle Privileged Account Manager target-accounts.

Note: To create an LDAP group, contact your LDAP administrator.

7.1.2 Configuring Oracle Privileged Account Manager for the Integration

To configure Oracle Privileged Account Manager for integration with Oracle Identity Manager, you must be an Oracle Privileged Account Manager administrator and perform the following tasks:

- Use a specific Oracle Privileged Account Manager account on an Oracle Privileged Account Manager target.
- Assign an LDAP group that restricts access to the Oracle Privileged Account Manager target-account to only the members of that LDAP group. However, you can assign multiple LDAP groups.

7.1.3 Integrating the Oracle Identity Manager Core

Oracle Identity Manager provides the following features to support this integration:

- LDAP connector(s) to manage LDAP groups
- Populate the resource catalog with proper enterprise roles and entitlements. Oracle Privileged Account Manager target-accounts are entitlements because Oracle Identity Manager is not actually granting direct access to the actual account only a representation of that account.

Refer to the Oracle Identity Manager documentation for more detailed information about accounts, entitlements, and roles.

7.1.4 Configuring an Oracle Identity Manager Administrator

You must configure an Oracle Identity Manager administrator who can perform the following tasks:

- Configure an Oracle Identity Manager rule that assigns users to the proper LDAP groups based on a business rule when you add users to Oracle Identity Manager (either manually through the user screen or automatically by using an HR/text feed).
- Use Oracle Identity Manager's native functionality to build requests for items in the Oracle Identity Manager resource catalog to ensure that the Oracle Identity Manager catalog is properly populated. Oracle Identity Manager enables users to request access to entitlements contained in the Oracle Identity Manager catalog.
- Set approver fields to the proper values. For example, in situations where one employee requests access to the email account of another employee who will be away from the office for an extended period of time.
- Handle "firecall" requests, where an Oracle Privileged Account Manager user must access a system that is outside the normal business process.

Firecall requests are handled based upon your business requirements and business rules. For example, if the Oracle Privileged Account Manager user is authorized for a target, but the access policy prevents that user from getting the password, then the Oracle Privileged Account Manager administrator can temporarily change the access policy for that target-account.

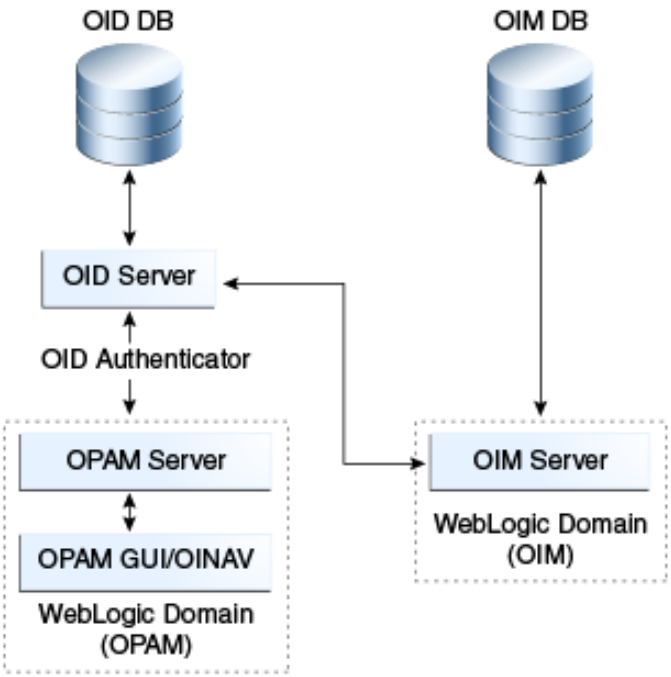
If the user cannot wait for Oracle Identity Manager, the Oracle Privileged Account Manager administrator can manually direct access (for example, add a specific grantee to the account) instead.

7.1.5 Managing Oracle Identity Manager Workflows

Oracle Privileged Account Manager leverages Oracle Identity Manager for workflow support. The integration points include:

- Access to privileged accounts granted to roles in Oracle Privileged Account Manager by an Oracle Privileged Account Manager Admin
- End users can request membership in these roles via Oracle Identity Manager
- Standard Oracle Identity Manager workflow used to approve these requests
- Membership in the requested role results in end user getting access to the corresponding privileged accounts in Oracle Privileged Account Manager

Figure 7–1 Oracle Identity Manager Workflow Topology



7.2 Integrating with Oracle Access Management Access Manager

This section explains how Oracle Access Management Access Manager (Access Manager) integrates with Oracle Privileged Account Manager. Using this integration scenario, you can protect Oracle Privileged Account Manager with Access Manager using a WebGate agent.

The topics in this section include:

7.2.1 Before You Begin

Before starting the procedure described in Section 7.2.2, "Enabling Single Sign-On," be aware of the following:

- The instructions assume that you configured Oracle Internet Directory as the Identity Store; however, other component configurations are possible. Refer to the system requirements and certification documentation on Oracle Technology Network for more information about supported configurations.
- In addition, the instructions describe a specific example of using Access Manager to protect URLs. Although they outline the general approach for this type of configuration, you are not limited to using the exact steps and components described here. For example, Oracle Internet Directory is one of several identity stores certified with Access Manager 11*g*.
- You can use Oracle Adaptive Access Manager as an authentication option with Access Manager. Oracle Adaptive Access Manager provides strong-authentication and risk-based authorization that can be used to provide layered security for Oracle Privileged Account Manager.

  To enable Oracle Adaptive Access Manager with Oracle Privileged Account Manager, select Access Manager as the authentication option for the WebGate that is protecting Oracle Privileged Account Manager.
- If you deployed Oracle Identity Navigator with Oracle Privileged Account Manager, and you are using Oracle Identity Navigator as the user interface for Oracle Privileged Account Manager, you can also protect Oracle Identity Navigator with Access Manager while enabling Oracle Single Sign-On.

  Refer to "Integrating with Oracle Identity Navigator" in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite* for instructions.
- Oracle Privileged Account Manager is protected by the domain agent out-of-the-box.

7.2.2 Enabling Single Sign-On

By default, the Access Manager 11g agent provides Single Sign On functionality for Oracle Privileged Account Manager and the following Identity Management consoles:

- Oracle Identity Manager
- Access Manager
- Oracle Adaptive Access Manager
- Oracle Authorization Policy Manager
- Oracle Identity Navigator

The Access Manager agent can only protect consoles in a single domain. If your environment spans multiple domains, you can use Access Manager 11g WebGate for Oracle HTTP Server 11g. Configuring Oracle Privileged Account Manager for WebGate-based single sign-on is the same as configuring Oracle Identity Navigator. Refer to "Integrating with Oracle Identity Navigator" in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

You can use Access Manager to enable Single Sign On for the Oracle Privileged Account Manager's user interface by using any Access Manager authentication scheme as the challenge method.

The prerequisites are as follows:

- Oracle HTTP Server has been installed.

  When installing Oracle HTTP Server, deselect Oracle WebCache and associated selected components with WebLogic domain.

- Access Manager 11*g* has been installed and configured properly.
- Oracle HTTP Server 11g has been installed and configured as a front-ending proxy web server for Oracle Privileged Account Manager.
- Access Manager 11g WebGate for Oracle HTTP Server 11g has been installed on the Oracle HTTP Server 11*g*.

> **See Also:** *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for details about installation of the listed components.

The high-level steps for enabling Single Sign On in Oracle Privileged Account Manager are as follows:

1. Use the Access Manager Administration Console to configure a new resource for the agent under which the Oracle Privileged Account Manager URL is to be protected. For information, see Section 7.2.2.1, "Configure a New Resource for the Agent."
2. Configure Oracle HTTP Server to point to the Access Manager domain which has the resources and policies configured. For information, see Section 7.2.2.2, "Configure Oracle HTTP Server for the Access Manager Domain."
3. Use the Administration Console to add the two new identity providers, namely the Access Manager Identity Asserter and the Oracle Internet Directory Authenticator. For information, see Section 7.2.2.3, "Add New Identity Providers.".
4. Use a WLST command to enable access to more than one application using multiple tabs in a browser session. For information, see Section 7.2.2.4, "Configure Access to Multiple Applications."

7.2.2.1 Configure a New Resource for the Agent

Perform these steps in the Access Manager administration console:

1. Select the **Policy Configuration** tab.
2. Under **Application Domains**, select the agent under which the Oracle Privileged Account Manager URL is to be protected (for example, `-OIMDomain`).
3. Choose **Resources** and click the **create** icon to add a new resource. Enter the type, host identifier and value, (`/oinav/…/*`) and click the **Apply** button.
4. Choose Protected Policy or the policy whose authentication schema is the LDAP schema. In the resources table, click the **add** icon and choose the Oracle Privileged Account Manager URL (`/oinav/…/*`) from the drop-down list.
5. Repeat the step for Authorization Policy.

7.2.2.2 Configure Oracle HTTP Server for the Access Manager Domain

Perform these steps to ensure that Oracle HTTP Server front ends the Oracle WebLogic Server container where Oracle Privileged Account Manager is installed.

1. Navigate to the Oracle HTTP Server server `config` directory, for example, `/scratch/mydir1/oracle/product/11.1.1/as_1/instances/instance1/config/OHS/ohs1`), and find the `mod_wl_ohs.conf` file.
2. In the `<IfModule mod_weblogic.c>` block, add the host and the port number of the Oracle Privileged Account Manager URL to be protected. For example:

   ```
   MatchExpression /oinav* WebLogicHost=host WebLogicPort=port
   ```

3. Restart the Oracle HTTP Server server in the OHS install `bin` directory, for example, `/scratch/mydir1/oracle/product/11.1.1/as_1/instances/instance1/bin`) by executing the following command:

   ```
   -./opmnctl restartproc ias=component=ohs1
   ```

7.2.2.3 Add New Identity Providers

Perform these steps to add two new identity providers:

1. Using the Administration Console, navigate to **Security Realms**, then **myrealm**, then **Providers**.
2. Add these two providers: Access Manager Identity Asserter and Oracle Internet Directory Authenticator.
3. Set the Control Flag of the Access Manager Identity Asserter to `Required`.
4. Update the following settings in the Oracle Internet Directory Authenticator:
   - Set the Control Flag to `Sufficient`
   - Select the **Provider specific** tab and make the necessary changes, supplying the host, port, and other credentials of the Oracle Internet Directory server. Configure the correct LDAP setting in the Oracle Internet Directory Authenticator.

   The users and Groups in the LDAP will be reflected in the console.
5. Re-order the providers as follows:
   a. Access Manager Identity Asserter
   b. Authenticator
   c. Default Authenticator
   d. Default Identity Asserter
6. Restart Oracle WebLogic Server.
7. Enter the protected Oracle Privileged Account Manager URL, which will have the host and port from the Oracle HTTP Server install:

   ```
   http://OHSHost:OHSPort/oinav/faces/idmNag.jspx
   ```

7.2.2.4 Configure Access to Multiple Applications

The following applies when Single Sign On protection is provided by an 11*g* Access Manager Server. Perform these steps to configure access to applications using multiple tabs in a single browser session by changing to FORM cache mode.

1. Stop the Access Manager Managed Servers.

2. Execute the following online Access Manager WLST command:

   ```
   configRequestCacheType(type='FORM')
   ```

3. Restart the Access Manager Managed Servers.

Part IV

Appendixes

This part contains the following appendixes:

- Working with the Command Line Tool
- Working with Oracle Privileged Account Manager's RESTful Interface
- Troubleshooting Oracle Privileged Account Manager

A

Working with the Command Line Tool

You can use the Oracle Privileged Account Manager command line tool to perform many of the same tasks you perform from the Oracle Privileged Account Manager's Console.

> **Note:** Globalization support for the Oracle Privileged Account Manager command line tool is not available for this release. The command line tool messages and help are only provided in English.

This appendix describes how to launch and use the command line tool. The topics include:

- Section A.1, "Launching the Command Line Tool"
- Section A.2, "Oracle Privileged Account Manager Commands"

A.1 Launching the Command Line Tool

Use the following steps to launch the Oracle Privileged Account Manager command line tool:

1. Open a command window and change directory to *ORACLE_HOME*/opam/bin.
2. At the prompt, type one of the following commands to launch the Console:
   - **On UNIX systems, type:** `opam.sh`
   - **On Windows systems, type:** `opam.bat`

   Invoking the command line tool, automatically connects you to the Oracle Privileged Account Manager server.

   You can invoke the Oracle Privileged Account Manager command line tool from a remote client by providing the Oracle Privileged Account Manager server's URL (running on the same machine or on a different machine) in the **`-url`** option.

Note: For security purposes, the Oracle Privileged Account Manager server only responds to SSL traffic.

When you provide the Oracle Privileged Account Manager server target to the Oracle Privileged Account Manager command line tool (or to Oracle Privileged Account Manager's web-based Console), you must provide the SSL endpoint as https://*hostname*:*sslport*/opam.

By default, webLogic responds to SSL on port 7002. The default Oracle Privileged Account Manager server SSL port is 18102. You can use the WebLogic console to check the port for your particular instance.

A.2 Oracle Privileged Account Manager Commands

This section describes the commands that you can use with the Oracle Privileged Account Manager command line tool.

The topics in this section include

A.2.1 Issuing Commands

Use the following syntax to issue any of the Oracle Privileged Account Manager commands:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x <opam-command>
```

where:

Option	Description
-url <*url*>	Provide the URL address for the Oracle Privileged Account Manager server. **Note**: If you do not specify a URL for this option, it defaults to `https://hostname:18102/opam`.
-u <*username*>	Provide your log-in user name.
-p <*password*>	Provide your log-in password.
-debug	Run the debugger.
-x <*opam-command*>	Run the specified Oracle Privileged Account Manager command.

For example:

```
-url https://hostname:sslport/opam -u <username> [-p <password>] [debug]
-x addtarget -targetname <targetname> -host <hostname> -port 22
-organization <organization>
```

A.2.2 addaccount Command

Use the addaccount command to add a privileged account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x addaccount <options>
```

The following table describes the options you can use with this command:

Option	Description
-targetid <*target id*>	Identify the target GUID value of a configured target.
-accountname <*accounttname*>	Provide a name for the new account.
[-help]	*Optional*. Displays usage options for this command.

A.2.3 addtarget Command

Use the addtarget command to add a target.

Command Syntax:

```
[[-url <url>] -u <username> [-p <password>] [-debug] -x addtarget <options>
```

Oracle Privileged Account Manager supports multiple target types, and the parameters they require can vary. These parameters should be discovered at run time, *before* you execute an `addtarget` command.

For example,

- Execute the following command to see a list of supported target types:

  ```
  sh opam.sh –url <OPAM url> -u <security admin user>
  -p <security admin user password> -x addtarget –help
  ```

  For example, if https://*hostname*:*sslport*/opam is the Oracle Privileged Account Manager server URL, execute the following command:

  ```
  sh opam.sh -url https://hostname:sslport/opam -u sec_admin -p welcome1
  -x addtarget -help
  ```

- Execute the following command to see a list of the required and optional attributes for a specified target type:

  ```
  sh opam.sh –url <OPAM url> -u <security admin user>
  -p <security admin user password> -x addtarget
  –targettype <any supported target type> –help
  ```

  For example, to see a list of attributes for the LDAP target type with https://*hostname*:*sslport*/opam as the Oracle Privileged Account Manager server URL, execute the following command:

  ```
  sh opam.sh -url https://hostname:sslport/opam -u sec_admin -p welcome1
  -x addtarget -targettype ldap -help
  ```

The following table describes the parameters required for LDAP targets.

Note: You must specify all multi-valued attributes in this format: `value1|value2|...`

Option	Description
-targetname <*targetname*>	Provide a name for the target.
-targettype <ldap | unix | database> <*type-specific attributes*>	Specify a target type and provide any type-specific attributes.
-domain <*domain*>	Provide a domain name.
-host <*host*>	Provide the host name.
-port <*port*>	Provide the TCP/IP port number used to communicate with the LDAP server.
-ssl <*ssl*>	*Optional*. Specify to connect to the LDAP server using SSL.
-principal <*principal*>	Provide the distinguished name with which to authenticate to the LDAP server.
-credentials <*credentials*>	Provide the principal's password.

Option	Description
-baseContexts <*baseContexts*> [Multi-Valued]	Specify one or more starting points in the LDAP tree to use when searching the tree. Searches are performed when discovering users from the LDAP server or when looking for groups in which the user is a member.
-accountNameAttribute <*accountNameAttribute*>	Specify the attribute that holds the account's user name.
[-description <*description*>]	Provide a description of the target.
[-organization <*organization*>]	Provide the organization name.
[-uidAttribute <*uidAttribute*>]	Provide the name of the LDAP attribute that is mapped to the `UID` attribute. (Defaults to *`uid`*)
[-accountSearchFilter <*accountSearchFilter*>]	*Optional*. Provide an LDAP filter to control which accounts are returned from the LDAP resource. If you do not specify a filter, then only accounts that include all specified object classes will be returned. (Defaults to *`(uid=*)`*)
[-passwordAttribute <*passwordAttribute*>]	*Optional*. Specify the name of the LDAP attribute that holds the password. When changing a user's password, Oracle Privileged Account Manager sets the new password to this attribute. (Defaults to *`userpassword`*)
[-accountObjectClasses <*accountObjectClasses*>] [Multi-Valued]	Specify the objectclass or objectclasses to use when creating new user objects in the LDAP tree. When entering more than one objectclass, put each entry on its own line and do not use commas or semicolons to separate multiple object classes. Some objectclasses may require that you specify all objectclasses in the class hierarchy. (Defaults to *`"top|person|organizationalPerson|inetOrgPerson"`*)

A.2.4 `checkin` and `checkout` Commands

Use the `checkin` command to check in privileged accounts and the `checkout` command to check out privileged accounts.

> **Note:** The `checkout` operation also provides a password for you to use.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x checkin <options>

[-url <url>] -u <username> [-p <password>] [-debug] -x checkout <options>
```

The following table describes the options you can use with these commands:

Option	Description
-accountid <*account id*>	Identify the account to be checked-out or checked-in.
[-help]	*Optional*. Displays usage options for this command.

A.2.5 `displayallaccounts` Command

Use the `displayallaccounts` command to display a listing of all accounts.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displayallaccounts
<options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.6 `displayallgroups` Command

Use the `displayallgroups` command to display a listing of all groups.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displayallgroups <options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.7 `displayalltargets` Command

Use the `displayalltargets` command to display a listing of all targets.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displayalltargets <options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.8 `displayallusers` Command

Use the `displayallusers` command to display a listing of all users.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displayallusers <options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.9 `displaycheckedoutaccounts` Command

Use the `displaycheckedoutaccounts` command to display a listing of a user's checked out accounts.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displaycheckedoutaccounts
<options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.10 `displaydomaintree` Command

Use the `displaydomaintree` command to display a domain tree.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displaydomaintree <options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.11 `displaytargettypetree` Command

Use the `displaytargettypetree` command to display a target type tree.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x displaytargettypetree
<options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

A.2.12 `export` and `import` Commands

Use the `export` command to export data stored in Oracle Privileged Account Manager, such as targets and accounts, to XML format. Use the `import` command to import data to OPAM from XML file. These options are useful for performing

- Bulk operations, such as querying or loading large volumes of data
- Back-up and recovery operations, such as periodically backing up Oracle Privileged Account Manager data to XML
- Migration operations, such as exporting data from one Oracle Privileged Account Manager instance and importing it to another instance

Note: You must be an administrator with the *Security Administrator* Admin Role to use these commands.

The `export` command exports all Oracle Privileged Account Manager data; including targets, accounts, policies, and grants.

Note: Exporting accounts also exports the passwords for those accounts. For added security, you can export the passwords in an encrypted format by using the `-encpassword` and `-enckeylen` options.

Be sure to note the encryption password and *encryption key length* because you must provide that same password for decryption during the import operation.

You can create an import XML file from previously exported data or you can manually create the file. If you previously exported the XML file with an encryption password, then you must provide the same password for decryption during import.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x export <options>

[-url <url>] -u <username> [-p <password>] [-debug] -x import <options>
```

The following table describes the options you can use with the `export` and `import` commands:

Option	Description
-f *<export file>*	Specify an export file name.
-encpassword *<encryption password>*	Specify a password to use when encrypting/decrypting account passwords.
-enckeylen *<key length for password encryption>*	Specify the minimum key length for an encryption/decryption password. (Defaults to 128 bits)
-log *<log file location>*	Specify a file name and location for the log file. (Defaults to `log.txt`)
[-help]	*Optional*. Displays usage options for this command.

The XML schema for an import or export file is located in the following file:

```
ORACLE_HOME/opam/jlib/OPAMBulkTool.xsd
```

The following example shows some sample XML definitions of Oracle Privileged Account Manager elements.

Example A–1 Sample XML Definition of Oracle Privileged Account Manager Elements

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<OPAMData xmlns="http://www.example.org/OPAMBulkTool"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.example.org/OPAMBulkTool OPAMBulkTool.xsd">
  <usagepolicy>
    <name value="Accounting Usage Policy"/>
    <status value="active"/>
    <description value="null"/>
```

```
  <globaldefault value="n"/>
  <dateorduration value="duration"/>
  <expiremin value="30"/>
  <expiredate value="08/08/2088"/>
  <expiretime value="11:30am"/>
  <timezone value="America/Los_Angeles"/>
  <usagedays>
    <day fromtime="12:0am" totime="12:0am" value="monday"/>
    <day fromtime="12:0am" totime="12:0am" value="tuesday"/>
    <day fromtime="12:0am" totime="12:0am" value="wednesday"/>
    <day fromtime="12:0am" totime="12:0am" value="thursday"/>
    <day fromtime="12:0am" totime="12:0am" value="friday"/>
    <day fromtime="12:0am" totime="12:0am" value="saturday"/>
    <day fromtime="12:0am" totime="12:0am" value="sunday"/>
  </usagedays>
</usagepolicy>
<passwordpolicy>
  <name value="Accounting Password Policy"/>
  <status value="active"/>
  <description value=""/>
  <globaldefault value="n"/>
  <changepassevery value="30-days"/>
  <changepasscheckout value="y"/>
  <changepasscheckin value="y"/>
  <passwordlength max="20" min="8"/>
  <minalphabets value="1"/>
  <minnumeric value="1"/>
  <minalphanumeric value="2"/>
  <specialchars max="5" min="1"/>
  <repeatedchars max="1" min="0"/>
  <minuniquechars value="1"/>
  <minuppercasechars value="1"/>
  <minlowercasechars value="1"/>
  <startwithchar value="n"/>
  <accountnameaspass value="n"/>
</passwordpolicy>
<target>
  <type name="database"/>
  <name value="AccountsDB"/>
  <attributes>
    <attributeName name="domain" value="Accounting"/>
    <attributeName name="host" value="localhost"/>
    <attributeName name="jdbcUrl" value="jdbc:oracle:thin:@dbhost:1521:orcl"/>
    <attributeName name="loginUser" value="system"/>
    <attributeName name="loginPassword" value="welcome1"/>
    <attributeName name="dbType" value="Oracle"/>
    <attributeName name="description" value="Accounting Database"/>
    <attributeName name="organization" value="Accounting"/>
    <attributeName name="connectionProperties" value=""/>
  </attributes>
</target>
<account>
  <name value="ACCT_DBA"/>
  <target name="AccountsDB"/>
  <passwordpolicy name="Accounting Password Policy"/>
  <grantee>
    <user name="johndoe"/>
    <user name="janedoe"/>
  </grantee>
  <shared value="false"/>
```

```
    <status value="checkedIn"/>
  </account>
</OPAMData>
```

A.2.13 `getglobalconfig` Command

Use the `getglobalconfig` command to view the OPAM Global Config configuration entry, which enables you to access and manage various Oracle Privileged Account Manager server properties.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x getglobalconfig <options>
```

The following table describes the options you can use with this command:

Option	Description
[-help]	*Optional*. Displays usage options for this command.

> **Note:** You use the `modifyglobalconfig` command to modify the server properties. Refer to `modifyglobalconfig` Command for more information.

A.2.14 `grantgroupaccess` Command

Use the `grantgroupaccess` command to give a group access to a privileged account.

```
[-url <url>] -u <username> [-p <password>] [-debug] -x grantgroupaccess <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account to which the group is granted access.
-groupname <*group name*>	Identify the group to be given access.
[-help]	*Optional*. Displays usage options for this command.

A.2.15 `grantuseraccess` Command

Use the `grantuseraccess` command to give a user access to a privileged account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x grantuseraccess <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account to which the user is granted access.
-userid <*user id*>	Identify the user to be given access.
[-help]	*Optional*. Displays usage options for this command.

A.2.16 `modifyglobalconfig` Command

Use the `modifyglobalconfig` command to manage the following Oracle Privileged Account Manager server properties in the OPAM Global Config configuration entry:

- **policyenforcerinterval**. Interval (in seconds) in which Oracle Privileged Account Manager checks accounts and then automatically checks-in the accounts that have exceeded the expiration time defined in the Usage Policy. (Default is 3600 seconds)
- **passwordcyclerinterval**. Interval (in seconds) in which Oracle Privileged Account Manager checks and then resets the password for any accounts that have exceeded the maximum password age defined in the Password Policy. (Default is 3600 seconds)

> **Note:** to access these properties, you must use the `getglobalconfig` command to view the OPAM Global Config configuration entry. Refer to `getglobalconfig` Command for more information.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x modifyglobalconfig
<options>
```

The following table describes the options you can use with this command:

Option	Description
-propertyname <*property name*>	Specifies which server property to be modified.
-propertyvalue <*property value*>	Specifies the interval (in seconds).
[-help]	*Optional*. Displays usage options for this command.

For example,

```
-x modifyglobalconfig -propertyname policyenforcerinterval -propertyvalue 600
```

See Also:

`getglobalconfig` Command

A.2.17 `removeaccount` Command

Use the `removeaccount` command to remove a privileged account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x removeaccount <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account to be removed.
[-help]	*Optional*. Displays usage options for this command.

A.2.18 `removegroupaccess` Command

Use the `removegroupaccess` command to remove a group's access to a privileged account.

```
[-url <url>] -u <username> [-p <password>] [-debug] -x removegroupaccess <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account where access is being removed.
-groupname <*group name*>	Identify the group whose access is being removed.
[-help]	*Optional*. Displays usage options for this command.

A.2.19 `removetarget` Command

Use the `removetarget` command to remove a target.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x removetarget <options>
```

The following table describes the options you can use with this command:

Option	Description
-targetid <*target id*>	Identify the target to be removed.
[-help]	*Optional*. Displays usage options for this command.

A.2.20 `removeuseraccess` Command

Use the `removeuseraccess` command to remove a user's access to a privileged account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x removeuseraccess <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account where access is being removed.
-userid <*user id*>	Identify the user whose access is being removed.
[-help]	*Optional*. Displays usage options for this command.

A.2.21 `resetpassword` Command

Use the `resetpassword` command to manually reset the password for an account you have checked out. When you execute this command, Oracle Privileged Account Manager returns the account details and prompts you to enter a new password.

Note: For most users, if the account has already been checked back in, you will get an error.

If you are an administrator with the *Security Administrator* or *User Manager* Admin Role, you can use this command to reset a password for both checked out and checked-in accounts.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] -x resetpassword -accountid <accountid>
```

No options are used with this command.

A.2.22 `retrieveaccount` Command

Use the `retrieveaccount` command to get information about a privileged account, such as which target the account is on. This information does not include passwords.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x retrieveaccount <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account to be retrieved.
[-help]	*Optional*. Displays usage options for this command.

A.2.23 `retrievegrantees` Command

Use the `retrievegrantees` command to get information about the grantees on a privileged account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x retrievegrantees <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify from which account the grantees are to be retrieved.
[-help]	*Optional*. Displays usage options for this command.

A.2.24 `retrievegroup` Command

Use the `retrievegroup` command to get information about groups on a privileged account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x retrievegroup <options>
```

The following table describes the options you can use with this command:

Option	Description
-groupname <*group name*>	Provide the name of the group to retrieve.
[-help]	*Optional*. Displays usage options for this command.

A.2.25 `retrievetarget` Command

Use the `retrievetarget` command to get information about a target.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x retrievetarget <options>
```

The following table describes the options you can use with this command:

Option	Description
-targetid <*target id*>	Identify the target to be retrieved.
[-help]	*Optional*. Displays usage options for this command.

A.2.26 `retrieveuser` Command

Use the `retrieveuser` command to get information about a user.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x retrieveuser <options>
```

The following table describes the options you can use with this command:

Option	Description
-userid <*user id*>	Identify the user to be retrieved.
[-help]	*Optional*. Displays usage options for this command.

A.2.27 `searchaccount` Command

Use the `searchaccount` command to search for an account.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x searchaccount <options>
```

The following table describes the options you can use with this command:

Option	Description
-accountid <*account id*>	Identify the account to search for.
[-help]	*Optional*. Displays usage options for this command.

For example, the following search will return all targets:

```
https://<host name>:<port>/opam/target/search?
```

Whereas, the following search will return all targets whose type contains `ldap` and `org`:

```
https://<host name>:<port>/opam/target/search?type=ldap&org=us
```

A.2.28 `searchgroup` Command

Use the `searchgroup` command to search for a group.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x searchgroup <options>
```

The following table describes the options you can use with this command:

Option	Description
[-groupname <*group name*>]	*Optional*. Provide the name of the group to search for.
[-description <*description*>]	*Optional*. Provide a description of the group.
[-accountname <*account name*>]	*Optional*. Provide the name of the account to search.
[-targetname <*target name*>]	*Optional*. Provide the name of the target to search.
[-help]	*Optional*. Displays usage options for this command.

A.2.29 `searchtarget` Command

Use the `searchtarget` command to search for a target.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x searchtarget <options>
```

The following table describes the options you can use with this command:

Option	Description
[-targettype <ldap | solaris | oracledb>]	*Optional*. Identify the type of target to search for as LDAP, Solaris, or Oracle DB.
[-domain <*domain*>]	*Optional*. Provide a domain to search.
[-targetname <*target name*>]	*Optional*. Provide the target name to search for.
[-help]	*Optional*. Displays usage options for this command.

A.2.30 `searchuser` Command

Use the `searchuser` command to search for a user.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] [-debug] -x searchuser <options>
```

The following table describes the options you can use with this command:

Option	Description
[-userid <*user id*>]	*Optional*. Search for the user by the user ID.
[-firstname <*first name*>]	*Optional*. Provide the user's first name.
[-lastname <*last name*>]	*Optional*. Provide the user's last name.
[-accountname <*account name*>]	*Optional*. Provide the name of the account to search.
[-targetname <*target name*>]	*Optional*. Provide the name of the target to search.
[-help]	*Optional*. Displays usage options for this command.

A.2.31 `showpassword` Command

Use the `showpassword` command to view the password for an account you have checked out. When you execute this command, Oracle Privileged Account Manager returns the account details and the password.

Note: If the account has already been checked back in, you will get an error.

If you are an administrator with the *Security Administrator* or *User Manager* Admin Role, you can use this command to view a password for both checked out and checked-in accounts.

Command Syntax:

```
[-url <url>] -u <username> [-p <password>] -x showpassword -accountid <accountid>
```

No options are used with this command.

B

Working with Oracle Privileged Account Manager's RESTful Interface

While Oracle Privileged Account Manager can be consumed through several client interfaces, its fundamental access mechanism or layer is encapsulated in its RESTful interfaces.

All interactions with Oracle Privileged Account Manager's server that are being used by external parties, such as a non-Oracle Privileged Account Manager server, are exposed through RESTful interfaces. All externally visible Oracle Privileged Account Manager resources are modeled by URIs, while standard HTTP operations are mapped to relevant Oracle Privileged Account Manager operations on those resources.

This appendix describes Oracle Privileged Account Manager's RESTful interface. The specific APIs that are exposed through this interface are documented in the following sections:

- Section B.1, "Target Resource"
- Section B.2, "Account Resource"
- Section B.3, "UI Resource"
- Section B.4, "User Resource"
- Section B.5, "Group Resource"
- Section B.6, "Usage Policy Resource"
- Section B.7, "Password Policy Resource"
- Section B.8, "Policy Resource"

Note: You can also use Oracle Privileged Account Manager's web-based Console or command line tool to perform tasks described in this appendix.

Refer to Chapter 5, "Configuring and Managing Oracle Privileged Account Manager" or Appendix A, "Working with the Command Line Tool" for more information.

B.1 Target Resource

The APIs described in this section include:

- Get Target Attributes
- Add a Target

- Verify a Target
- Retrieve a Target
- Update a Target
- Remove a Target
- Search for Targets
- Get Available Accounts
- Retrieve Accounts Registered on a Target
- Get Target Types

B.1.1 Get Target Attributes

Use this API to retrieve a list of the attributes that are associated with all of the target types.

You can use the list of supported target types, along with these attributes, to create the JSON object required to add a target. Refer to Section B.1.2, "Add a Target" for more information.

Note: You must have a JSON browser extension, such as Firefox JSONview, to create the JSON object.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/attributes/{locale}
Method	`GET`
Returns on Success	Status code 200 and the JSON representation of target types, along with the attributes associated with them.

Sample URI

https://*opam_server_host*:*opam_ssl_port*/opam/target/attributes/en

Example B–1 JSON Output of Supported Target Types with Attributes

```
{
   "TargetAttributes":[
      {
         "TargetType":"ldap",
         "DisplayName":"ldap",
         "BasicAttributes":[
            {
               "name":"targetName",
               "type":"string",
               "description":"",
               "label":"Target Name",
               "mask":"false",
               "array":"false",
               "required":"true"
            },
            {
               "name":"description",
               "type":"string",
               "description":"",
               "label":"Description",
```

```
      "mask":"false",
      "array":"false",
      "required":"false"
   },
   {
      "name":"organization",
      "type":"string",
      "description":"",
      "label":"Organization",
      "mask":"false",
      "array":"false",
      "required":"false"
   },
   {
      "name":"domain",
      "type":"string",
      "description":"",
      "label":"Domain",
      "mask":"false",
      "array":"false",
      "required":"true"
   },
   {
      "name":"host",
      "type":"string",
      "description":"",
      "label":"Host",
      "mask":"false",
      "array":"false",
      "required":"true"
   },
   {
      "name":"port",
      "type":"int",
      "description":"TCP/IP port number used to communicate with the LDAP server.",
      "label":"TCP Port",
      "default":"",
      "mask":"false",
      "array":"false",
      "required":"true"
   },
   {
      "name":"ssl",
      "type":"boolean",
      "description":"Select the check box to connect to the LDAP server using SSL.",
      "label":"SSL",
      "default":"false",
      "mask":"false",
      "array":"false",
      "required":"true"
   },
   {
      "name":"principal",
      "type":"string",
      "description":"The distinguished name with which to authenticate
         to the LDAP server.",
      "label":"Principal",
      "default":"",
      "mask":"false",
      "array":"false",
```

```
            "required":"true"
         },
         {
            "name":"credentials",
            "type":"string",
            "description":"Password for the principal.",
            "label":"Password",
            "default":"",
            "mask":"true",
            "array":"false",
            "required":"true"
         },
         {
            "name":"baseContexts",
            "type":"string",
            "description":"One or more starting points in the LDAP tree that will be used
               when searching the tree. Searches are performed when discovering users from
               the LDAP server or when looking for the groups of which a user is a member.",
            "label":"Base Contexts",
            "default":[

            ],
            "mask":"false",
            "array":"true",
            "required":"true"
         },
         {
            "name":"accountNameAttribute",
            "type":"string",
            "description":"Attribute which holds the account's user name.",
            "label":"Account User Name Attribute",
            "default":"uid",
            "mask":"false",
            "array":"false",
            "required":"true"
         }
      ],
      "AdvancedAttributes":[
         {
            "name":"uidAttribute",
            "type":"string",
            "description":"The name of the LDAP attribute which is mapped
               to the Uid attribute.",
            "label":"Uid Attribute",
            "default":"uid",
            "mask":"false",
            "array":"false",
            "required":"false"
         },
         {
            "name":"accountSearchFilter",
            "type":"string",
            "description":"An optional LDAP filter to control which accounts are returned
               from the LDAP resource. If no filter is specified, only accounts that include
               all specified object classes are returned.",
            "label":"LDAP Filter for Retrieving Accounts",
            "default":"(uid=*)",
            "mask":"false",
            "array":"false",
            "required":"false"
```

```
            },
            {
               "name":"passwordAttribute",
               "type":"string",
               "description":"The name of the LDAP attribute which holds the password.
                  When changing an user's password, the new password is set to this attribute.",
               "label":"Password Attribute",
               "default":"userpassword",
               "mask":"false",
               "array":"false",
               "required":"false"
            },
            {
               "name":"accountObjectClasses",
               "type":"string",
               "description":"The object class or classes that will be used when
                  creating new user objects in the LDAP tree. When entering more than one
                  object class, each entry should be on its own line; do not use commas or
                  semi-colons to separate multiple object classes. Some object classes
                  may require that you specify all object classes in the class hierarchy.",
               "label":"Account Object Classes",
               "default":[
                  "top",
                  "person",
                  "organizationalPerson",
                  "inetOrgPerson"
               ],
               "mask":"false",
               "array":"true",
               "required":"false"
            }
         ]
      }
   ]
}
```

Where:

- **TargetAttributes** is an array of objects, where each object represents a target type.
- **TargetType** is the target type.
- **DisplayName** is how the target type name should display.
- **BasicAttributes** is an array of objects, where each object represents basic attributes for the target type.
- **AdvancedAttributes** is an array of objects, where each object represents advanced attributes for the target type.
- **name** is the attribute name to use when constructing the target JSON to create a target.
- **type** is the attribute type. Acceptable values include `string`, `int`, `boolean`, or `lov` (list of values).
- **description** is a helpful description of the attribute.
- **label** is how the attribute name should display.
- **default** is a default value for the attribute.

  Specify a single value if the `array` parameter is **false** or specify an array of values if `array` is **true**.

- **mask** hides sensitive values, such as credentials.
  - Specify `true` to hide attributes.
  - Specify `false` if hiding attributes is not necessary.
- **array** indicates whether the attribute is single-valued or an array of multiple values.
  - Specify `true` if the attribute is an array of multiple values.
  - Specify `false` if the attribute is single-valued.
- **required** indicates whether the attribute are mandatory or optional.
  - Specify `true` for mandatory attributes.
  - Specify `false` for optional attributes.

B.1.2 Add a Target

Use this API to add a target.

> **Note:** First, you must obtain a list of attributes for the target type as described in Section B.1.1, "Get Target Attributes." You use these attributes to create the JSON object sent in the body.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target
Method	`POST`
Body	JSON representation of target for addition/test
Returns on Success	Status code 201 Created and Location

Example B–2 Sample JSON Representation of Target for Addition

```
{
   "target":{
      "targetType":"ldap",
      "targetName":"hhsharma-ldap2",
      "host":"opam_server_host",
      "domain":"berkeley",
      "description":"Ldap target",
      "organization":"ST-US",
      "credentials":"welcome",
      "uidAttribute":"uid",
      "port":"9876",
      "passwordAttribute":"userpassword",
      "principal":"cn=orcladmin",
      "accountSearchFilter":"(uid=*)",
      "baseContexts":[
         "cn=Users,c=US"
      ],
      "ssl":"false",
      "accountObjectClasses":[
         "top",
         "person",
         "organizationalPerson",
         "inetOrgPerson"
      ],
      "accountNameAttribute":"uid"
```

```
   }
}
```

Sample Output

https://*opam_server_host*:*opam_ssl_port*/opam/target/9bbcbbb087174ad1900ea691a2573b61 as the Location.

Where:

- **target** is the target JSON object.
- **targetName** is the name of the target.
- **targetType** is the target type.

All of the other attributes are dynamic and they correspond to the attributes in Section B.1.1, "Get Target Attributes."

B.1.3 Verify a Target

Use this API to verify a target.

> **Note:** First, you must obtain a list of attributes for the target type. Refer to Section B.1.1, "Get Target Attributes," to create the JSON object to be sent in the body.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/test
Method	`PUT`
Body	JSON representation of target for addition/test
Returns on Success	Status code 200

Example B–3 Sample JSON Representation of Target for Addition/Verification

```
{
   "target":{
      "targetType":"ldap",
      "targetName":"hhsharma-ldap2",
      "host":"opam_server_host",
      "domain":"berkeley",
      "description":"Ldap target",
      "organization":"ST-US",
      "credentials":"welcome",
      "uidAttribute":"uid",
      "port":"9876",
      "passwordAttribute":"userpassword",
      "principal":"cn=orcladmin",
      "accountSearchFilter":"(uid=*)",
      "baseContexts":[
         "cn=Users,c=US"
      ],
      "ssl":"false",
      "accountObjectClasses":[
         "top",
         "person",
         "organizationalPerson",
         "inetOrgPerson"
```

```
      ],
      "accountNameAttribute":"uid"
   }
}
```

Where:

- **target** is the target JSON object.
- **targetName** is the name of the target.
- **targetType** is the target type.

All of the other attributes are dynamic and they correspond to the attributes in Section B.1.1, "Get Target Attributes."

B.1.4 Retrieve a Target

Use this API to retrieve a target.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/{targetUID}
Method	GET
Body	
Returns on Success	Status code 200 and JSON representation of target

Example B–4 Sample JSON Representation of Target

```
{
   "target":{
      "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
      "targetType":"ldap",
      "targetName":"hhsharma-ldap",
      "host":"opam_server_host",
      "domain":"berkeley",
      "description":"Ldap target",
      "organization":"ST-US",
      "credentials":"welcome",
      "uidAttribute":"uid",
      "port":"9876",
      "passwordAttribute":"userpassword",
      "principal":"cn=orcladmin",
      "accountSearchFilter":"(uid=*)",
      "baseContexts":[
         "cn=Users,c=US"
      ],
      "ssl":"false",
      "accountObjectClasses":[
         "top",
         "person",
         "organizationalPerson",
         "inetOrgPerson"
      ],
      "accountNameAttribute":"uid",
      "accounts":[
         {
            "account":{
               "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
                  /c11066278022489aad758aec69d9727d"
            }
```

```
         },
         {
            "account":{
               "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
                  /3740553e999a4f6aa8e8f9286d320cb4"
            }
         }
      ]
   }
}
```

Where:

- **target** is the target JSON object.
- **targetUID** is the target's unique identifier.
- **targetName** is the name of the target.
- **targetType** is target type.
- **accounts** is an array of accounts that are associated with the target.
- **account** is the account JSON object containing the account's URI.
- **uri** is the account's URI.

All of the other attributes are dynamic and they correspond to the attributes in Section B.1.1, "Get Target Attributes."

B.1.5 Update a Target

Use this API to update a target.

You can change all of the attributes, except `targetType` and `targetUID`, and you can change multiple attributes at a time.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/{targetUID}
Method	`PUT`
Body	JSON representation of Target Modification
Returns on Success	Status code 201

Example B–5 Sample JSON Object to Modify Target

```
{
   "modifications":[
      {
         "modification":{
            "host":"opam_server_host:opam_ssl_port
         }
      },
      {
         "modification":{
            "port":"6000"
         }
      }
   ]
}
```

Where:

- **targetUID** is the target's unique identifier.
- **modifications** is an array of modification JSON objects.
- **modification** is a JSON object representing the modification of a single attribute.

For this API, you must update the `host` and `port` attributes on the target. Their value is updated to the value provided with them.

B.1.6 Remove a Target

Use this API to delete a target.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/{targetUID}
Method	`DELETE`
Body	
Returns on Success	Status code 200

B.1.7 Search for Targets

Use this API to search for a target using any of the following request parameters:

- `type`
- `domain`
- `org`
- `name`
- `hostname`

All of these parameters are optional.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/search?param1=value1&param2=value2
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of Target Collection

Sample URIs:

https://*opam_server_host*:*opam_ssl_port*/opam/target/search?	Returns all targets
https://*opam_server_host*:*opam_ssl_port*/opam/target/search?type=ldap&org=us	Returns all targets whose type contains `ldap` and org contains `us`.

Example B–6 Sample JSON Representation of Target Collection

```
{
   "Target Collection":[
      {
         "target":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/target\
               /9bbcbbb087174ad1900ea691a2573b61",
            "type":"ldap",
            "name":"hhsharma-ldap",
```

```
            "host":"opam_server_host",
            "domain":"berkeley"
         }
      },
      {
         "target":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/target\
               /ac246a162ce948c7b1cdcc17dfc92c15",
            "type":"ldap",
            "name":"hhsharma-ldap2",
            "host":"opam_server_host:opam_ssl_port",
            "domain":"berkeley"
         }
      }
   ]
}
```

Where:

- **Target Collection** is an array of target JSON objects.
- **target** is the target JSON object.
- **uri** is the target resource URI.
- **type** is the target type.
- **hostname** is the target's host name.
- **name** is the target name.
- **org** is the target's organization.
- **domain** is the target's domain.

B.1.8 Get Available Accounts

Use this API to retrieve all of the accounts present on the target system.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/attributes/{locale}
Method	GET
Body	
Returns on Success	Status code 200 OK and JSON representation of account collection

Example B–7 Sample JSON Representation of Account Collection

```
{
   "AvailableAccounts":[
      {
         "accountName":"SCOTT",
         "accountUid":"SCOTT"
      },
      {
         "accountName":"BLAKE",
         "accountUid":"BLAKE "
      },
      {
         "accountName":"JONES",
         "accountUid":"JONES"
      }
   ]
```

```
}
```

Where:

- **AvailableAccounts** is an array of the accounts present on the target system.
- **accountName** is the account name.
- **accountUID** is the account's unique identifier.

B.1.9 Retrieve Accounts Registered on a Target

Use this API to retrieve all the accounts on the target that are registered with Oracle Privileged Account Manager.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/{targetUID}/accounts
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of URI collection of accounts

Example B–8 Sample JSON Representation of URI Collection of Accounts

```
{
   "URI Collection":[
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /3740553e999a4f6aa8e8f9286d320cb4",
            "accountName":"sherlock"
         }
      },
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /c11066278022489aad758aec69d9727d",
            "accountName":"himanshu"
         }
      }
   ]
}
```

Where:

- **URI Collection** is an array of accounts on a target that are registered with Oracle Privileged Account Manager.
- **account** is the account JSON object.
- **uri** is the account's URI.
- **accountName** is the account name.

B.1.10 Get Target Types

Use this API to retrieve a list of all supported target types.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/target/types

Method	GET
Body	
Returns on Success	Status code 200 and JSON representation of supported target types

Example B–9 Sample JSON Representation of Supported Target Types

```
{
   "targettypes":[
      "ldap",
      "unix",
      "database"
   ]
}
```

Where:

- **targettypes** are the supported target types.

B.2 Account Resource

The APIs described in this section include:

- Add an Account to a Target
- Verify an Account
- Retrieve an Account
- Reset Password
- Update an Account
- Remove an Account
- Grant a User/Role Access to an Account
- Remove a User's/Role's Access to an Account
- Retrieve Grantees on an Account
- Check Out an Account
- Check In an Account
- Retrieve Users Who Checked Out an Account
- Show Password

B.2.1 Add an Account to a Target

Use this API to add an account to the target. This API does not create an account on the target system, but it registers the existing account with the OPAM target.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account
Method	POST
Body	JSON representation for account addition/verification
Returns on Success	Status code 201 and Location

Example B–10 Sample JSON Representation of Account for Addition/Verification

```
{
   "account":{
      "accountName":"lucie",
      "passwordpolicy":"passwordpolicy2",
      "shared":"true",
      "targetUID":"9bbcbbb087174ad1900ea691a2573b61"
   }
}
```

Where:

- **account** is the account JSON object.
- **accountName** is the name of the account.
- **passwordpolicy** is the policy ID of the Password Policy applicable to the account. This parameter is optional. By default, this parameters uses the global Default Password Policy.
- **shared** indicates the shared status of the account. This value is a Boolean and the default setting is `false`.
- **targetUID** is the target's unique identifier.

B.2.2 Verify an Account

Use this API to verify whether the account is present on the target system.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/test
Method	`PUT`
Body	JSON representation for account addition/verification
Returns on Success	Status code 200

Example B–11 Sample JSON Representation of Account Addition/Verification

```
{
   "account":{
      "accountName":"lucie",
      "passwordpolicy":"passwordpolicy2",
      "shared":"true",
      "targetUID":"9bbcbbb087174ad1900ea691a2573b61"
   }
}
```

Where:

- **account** is the account JSON object.
- **accountName** is the name of the account.
- **passwordpolicy** is the policy ID of the Password Policy applicable to the account. This parameter is optional. By default, this parameters uses the global Default Password Policy.
- **shared** indicates the shared status of the account. This value is a Boolean and the default setting is `false`.
- **targetUID** is the target's unique identifier.

B.2.3 Retrieve an Account

Use this API to retrieve an account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of account

Example B–12 Sample JSON Representation of Account

```
{
   "account":{
      "accountUID":"3f74a85e39e64432ba917a2e60fa15aa",
      "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
      "accountName":"lucie",
      "shared":true,
      "status":"checkedIn",
      "usagepolicy":"usagepolicy1",
      "passwordpolicyname":"Default Password Policy",
      "passwordpolicy":"passwordpolicy2",
      "grantees":{
         "users":[
            "opamuser1"
         ],
         "roles":[
            "opamgroup1"
         ]
      }
   }
}
```

Where:

- **account** is the account JSON object.
- **accountUID** is the account's unique identifier.
- **accountName** is the name of the account.
- **passwordpolicy** is the policy ID of the Password Policy applicable to the account.
- **passwordpolicyname** is the name of the applicable Password Policy.
- **shared** indicates the shared status of the account. This value is a Boolean and the default setting is `false`.
- **targetUID** is target's unique identifier.
- **status** indicates whether the account has been checked in by anyone. Acceptable values are `checkedIn` and `checkedOut`.
- **grantees** are grantees of the account.
- **users** are users who have been granted the account. Each value is the user's login ID/UID.
- **roles** are groups or roles that have been granted the account. Each value is a group name of the group.

B.2.4 Reset Password

Use this API to reset the password on the account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}/resetpassword
Method	`PUT`
Body	JSON representation of the new password
Returns on Success	Status code 200

Example B–13 Sample JSON Representation of the New Password

```
{
   "password":"welcome1"
}
```

Where:

- **accountUID** is the account's unique identifier.

B.2.5 Update an Account

Use this API to update an account. You can change multiple attributes at a time. Only usagepolicy and shared attributes can be updated.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}
Method	`PUT`
Body	JSON representation of account modifications
Returns on Success	Status code 200

Example B–14 Sample JSON Representation of Account Modifications

```
{
   "modifications":[
      {
         "modification":{
            "passwordpolicy":"passwordpolicy2"
         }
      },
      {
         "modification":{
            "shared":"false"
         }
      }
   }
}
```

Where:

- **accountUID** is the account's unique identifier.
- **modifications** are an array of modification JSON objects.
- **modification** is a JSON object representing the modification of a single attribute.

B.2.6 Remove an Account

Use this API to remove an account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID
Method	DELETE
Body	
Returns on Success	Status code 200

Where:

- **accountUID** is the account's unique identifier.

B.2.7 Grant a User/Role Access to an Account

Use this API to grant a user or role access to an account. Multiple users and roles can be granted the access at a time.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}
Method	PUT
Body	JSON representation for adding grantees
Returns on Success	Status code 200

Example B–15 Sample JSON Representation for Adding Grantees

```
{
   "modifications":[
      {
         "modification":{
            "usagepolicy":"usagepolicy1",
            "role":"opamgroup1",
            "operation":"add"
         }
      },
      {
         "modification":{
            "usagepolicy":"usagepolicy1",
            "user":"opamuser1",
            "operation":"add"
         }
      }
   ]
}
```

Where:

- **accountUID** is the account's unique identifier.
- **modifications** are an array of modification JSON objects.
- **modification** is a JSON object representing the modification of a single attribute.
- **role** indicates that a group has to be granted an access. This parameter value is the group name.
- **user** indicates that a user has to be granted an access. This parameter value is the user login id.
- **usagepolicy** indicates the Usage Policy identifier to be applied to the grant.

- **operation** indicates the type of operation to be performed. Acceptable values include:
  - **add** indicates grant.
  - **delete** indicates revocation.
  - **replace** indicates replacement of usagepolicy with a new value.

B.2.8 Remove a User's/Role's Access to an Account

Use this API to remove a user's access or a role's access to an account. You can revoke multiple user and role grants at a time.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}
Method	`PUT`
Body	JSON representation for removing grantees
Returns on Success	Status code 200

Example B–16 Sample JSON Representation for Removing Grantees

```
{
   "modifications":[
      {
         "modification":{
            "usagepolicy":"usagepolicy1",
            "role":"opamgroup1",
            "operation":"delete"
         }
      },
      {
         "modification":{
            "usagepolicy":"usagepolicy1",
            "user":"opamuser1",
            "operation":"delete"
         }
      }
   ]
}
```

Where:

- **accountUID** is the account's unique identifier.
- **modifications** are an array of modification JSON objects.
- **modification** is a JSON object representing a single modification.
- **role** indicates that a group has to be granted an access. This parameter value is the group name.
- **user** indicates that a user has to be granted an access. This parameter value is the user login id.
- **usagepolicy** indicates the Usage Policy identifier to be applied to the grant.
- **operation** indicates the type of operation to be performed. Acceptable values include:
  - **add** indicates a grant.
  - **delete** indicates a revocation.

– **replace** indicates the replacement of the usagepolicy with a new value.

B.2.9 Retrieve Grantees on an Account

Use this API to retrieve all the grantees of an account. A grantee can be a user or a role.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}/grantees
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of Grantees

Example B–17 Sample JSON Representation of Grantees

```
{
   "grantees":{
      "users":[
         "opamuser1"
      ],
      "roles":[
         "opamgroup1"
      ]
   }
}
```

Where:

- **grantees** are grantees of the account.
- **user**s are the users who have been granted the account. Each value is the user's login ID/UID.
- **roles** are the groups or roles who have been granted the account. Each value is a group name.

B.2.10 Check Out an Account

Use this API to check out an account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}/checkout
Method	`PUT`
Body	
Returns on Success	Status code 200 and JSON representation of account token

Example B–18 Sample JSON Representation of Account Token

```
{
   "accountToken":{
      "accountName":"lucie",
      "accountUID":"3f74a85e39e64432ba917a2e60fa15aa",
      "accountPassword":"GJN8p2ol"
   }
}
```

Where:

- **accountUID** is the account's unique identifier.

- **accountName** is the name of the account.
- **accountpassword** is the account password.

B.2.11 Check In an Account

Use this API to check in an account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}/checkin
Method	`PUT`
Body	
Returns on Success	Status code 200

B.2.12 Retrieve Users Who Checked Out an Account

Use this API to retrieve a list of all users who have currently checked out an account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}/whocheckedout
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of users who checked out the account.

Example B–19 Sample JSON Representation of Users Who Checked Out the Account

```
{
   "users":[
      {
         "user":{
            "uid":"sec_admin",
            "lastname":"sec_admin",
            "dn":"uid=sec_admin,ou=people,ou=myrealm,dc=base_domain",
            "expiryTime":1338765551,
            "checkoutTime":1338333551,
            "timezone":"America\/Los_Angeles"
         }
      }
   ]
}
```

Where:

- **uid** is the user's unique identifier.
- **lastname** is the user's last name.
- **dn** is the distinguished name of the user.
- **expiryTime** is the expiration time of the check out session. This parameter value is the UNIX time.
- **checkoutTime** is the time at which the account was checked out. This parameter value is the UNIX time.
- **timezone** indicates the time zone applicable to `expiryTime` and `checkOutTime`.

B.2.13 Show Password

Use this API to retrieve and display the password associated with an account.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/account/{accountUID}/showpassword
Method	`PUT`
Body	
Returns on Success	Status code 200 and JSON representation of account token

Example B–20 Sample JSON Representation of Account Token

```
{
   "accountToken":{
      "accountName":"lucie",
      "accountUID":"3f74a85e39e64432ba917a2e60fa15aa",
      "accountPassword":"GJN8p2ol"
   }
}
```

Where:

- **accountUID** is the account's unique identifier.
- **accountName** is the name of the account.
- **accountPassword** is the account password.

B.3 UI Resource

The APIs described in this section include:

- Search Accounts
- Get All Checked Out Accounts

B.3.1 Search Accounts

Use this API to search accounts using one or more of the following search request parameters:

- `type`
- `domain`
- `org`
- `name`
- `accountname`

All of these parameters are optional.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/ui/allaccounts/search?param1=val1&param2=val2
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of account collection

Example B–21 Sample JSON Representation of Account Collection

```
{
   "AccountCollection":[
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /3740553e999a4f6aa8e8f9286d320cb4",
            "accountUID":"3740553e999a4f6aa8e8f9286d320cb4",
            "accountName":"sherlock",
            "status":"checkedOut",
            "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
            "targetName":"hhsharma-ldap",
            "targetType":"ldap",
            "domain":"berkeley",
            "disabled":"false",
            "grantees":{
               "users":[

               ],
               "roles":[

               ]
            }
         }
      },
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /c11066278022489aad758aec69d9727d",
            "accountUID":"c11066278022489aad758aec69d9727d",
            "accountName":"himanshu",
            "status":"checkedIn",
            "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
            "targetName":"hhsharma-ldap",
            "targetType":"ldap",
            "domain":"berkeley",
            "disabled":"true",
            "grantees":{
               "users":[

               ],
               "roles":[

               ]
            }
         }
      },
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /154034fc5b5548caad7721e198815709",
            "accountUID":"154034fc5b5548caad7721e198815709",
            "accountName":"lucie",
            "status":"checkedIn",
            "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
            "targetName":"hhsharma-ldap",
            "targetType":"ldap",
            "domain":"berkeley",
            "disabled":"true",
            "grantees":{
```

```
                "users":[

                ],
                "roles":[

                ]
             }
          }
       }
    ],
    "count":3
}
```

Where:

- **disabled** indicates the user's grant access to the account.
  - If set to `true`, the user has grant access to the account.
  - If set to false, the user is an administrator who can view the account, but cannot check out the account.

For all other attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.3.2 Get All Checked Out Accounts

Use this API to retrieve a list of all accounts that have been checked out by the logged in user.

URI	https://*opam_server_host*:*opam_ssl_port*/ui/allaccounts/mycheckedout
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of account collection

Example B–22 Sample JSON Representation of Account Collection

```
{
   "AccountCollection":[
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /3740553e999a4f6aa8e8f9286d320cb4",
            "accountUID":"3740553e999a4f6aa8e8f9286d320cb4",
            "accountName":"sherlock",
            "status":"checkedOut",
            "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
            "targetName":"hhsharma-ldap",
            "targetType":"ldap",
            "domain":"berkeley",
            "policyname":"Default Usage Policy",
            "policyid":"usagepolicy1",
            "expiryTime":1338765551,
            "timezone":"America\/Los_Angeles",
            "grantees":{
               "users":[

               ],
               "roles":[
```

```
                ]
             }
          },
          "count":1
       }
    ]
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.4 User Resource

The APIs described in this section include:

- Get a User
- Search Users
- Advanced Search for Users

B.4.1 Get a User

Use this API to retrieve a user.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/user/{uid}
Method	GET
Body	
Returns on Success	Status code 200 and JSON representation of user

Example B–23 Sample JSON Representation of User

```
{
   "user":{
      "uid":"opamuser1",
      "lastname":"opamuser1",
      "usertype":"End-User",
      "opamrole":[

      ],
      "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain",
      "accounts":[
         {
            "accountUID":"3740553e999a4f6aa8e8f9286d320cb4",
            "accountName":"sherlock",
            "targetType":"ldap",
            "targetName":"hhsharma-ldap",
            "targetDomain":"berkeley"
         },
         {
            "accountUID":"154034fc5b5548caad7721e198815709",
            "accountName":"lucie",
            "targetType":"ldap",
            "targetName":"hhsharma-ldap",
            "targetDomain":"berkeley"
         }
      ]
```

```
   }
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.4.2 Search Users

Use this API to search for users. This API is a contains search, using one or more of the following parameters:

- `firstname`
- `lastname`
- `UID` (unique identifier)
- `mail`

URI	https://*opam_server_host*:*opam_ssl_port*/opam/user/search/{searchKeyWord}
Method	`GET`
Body	
Returns on Success	Status 200 and JSON representation of users

Example B–24 Sample JSON Representation of Users

```
{
   "users":[
      {
         "user":{
            "uid":"opamenduser1",
            "firstname":"opamenduser1",
            "lastname":"opamenduser1",
            "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"opamenduser2",
            "lastname":"opamenduser2",
            "dn":"uid=opamenduser2,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"opamuser1",
            "lastname":"opamuser1",
            "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
         }
      }
   ]
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.4.3 Advanced Search for Users

Use this API to search for users. This API is a contains search, using one or more of the following parameters:

- `uid`
- `lastname`
- `firstname`

All of these parameters are optional.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/user/advancedsearch?param1=val1&param2=val2
Method	`GET`
Body	
Returns on Success	Status 200 and JSON representation of users

Example B–25 Sample JSON Representation of Users

```
{
   "users":[
      {
         "user":{
            "uid":"OracleSystemUser",
            "lastname":"OracleSystemUser",
            "dn":"uid=OracleSystemUser,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"weblogic",
            "lastname":"weblogic",
            "dn":"uid=weblogic,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"app_config",
            "lastname":"app_config",
            "dn":"uid=app_config,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"sec_admin",
            "lastname":"sec_admin",
            "dn":"uid=sec_admin,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"user_manager",
            "lastname":"user_manager",
            "dn":"uid=user_manager,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
```

```
            "uid":"sec_auditor",
            "lastname":"sec_auditor",
            "dn":"uid=sec_auditor,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"opamenduser1",
            "firstname":"opamenduser1",
            "lastname":"opamenduser1",
            "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"opamenduser2",
            "lastname":"opamenduser2",
            "dn":"uid=opamenduser2,ou=people,ou=myrealm,dc=base_domain"
         }
      },
      {
         "user":{
            "uid":"opamuser1",
            "lastname":"opamuser1",
            "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
         }
      }
   ]
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.5 Group Resource

The APIs described in this section include:

- Get Group
- Search Groups
- Advanced Search for Groups

B.5.1 Get Group

Use this API to retrieve a group.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/group/{name}
Method	GET
Body	
Returns on Success	Status code 200 and JSON representation of group

Example B–26 Sample JSON Representation of Group

```
{
   "group":{
      "name":"opamgroup1",
      "dn":"cn=opamgroup1,ou=groups,ou=myrealm,dc=base_domain",
```

```
      "description":"",
      "users":[
         {
            "uid":"opamenduser1",
            "firstname":"opamenduser1",
            "lastname":"opamenduser1",
            "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
         },
         {
            "uid":"opamuser1",
            "lastname":"opamuser1",
            "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
         }
      ],
      "groups":[
         {
            "group":{
               "name":"opamsubgroup1",
               "dn":"cn=opamsubgroup1,ou=groups,ou=myrealm,dc=base_domain",
               "description":""
            }
         },
         {
            "group":{
               "name":"opamsubgroup2",
               "dn":"cn=opamsubgroup2,ou=groups,ou=myrealm,dc=base_domain",
               "description":""
            }
         }
      ],
      "accounts":[
         {
            "accountUID":"c11066278022489aad758aec69d9727d",
            "accountName":"himanshu",
            "targetType":"ldap",
            "targetName":"hhsharma-ldap",
            "targetDomain":"berkeley"
         }
      ]
   }
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.5.2 Search Groups

Use this API to search for groups. This API is a contains search, using the `group name` parameter.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/group/search/{searchKeyWord}
Method	`GET`
Body	
Returns on Success	Status 200 and JSON representation of groups

Example B–27 Sample JSON Representation of Groups

```
{
```

```
"groups":[
   {
      "group":{
         "name":"opamgroup1",
         "dn":"cn=opamgroup1,ou=groups,ou=myrealm,dc=base_domain",
         "description":"",
         "users":[
            {
               "uid":"opamenduser1",
               "firstname":"opamenduser1",
               "lastname":"opamenduser1",
               "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
            },
            {
               "uid":"opamuser1",
               "lastname":"opamuser1",
               "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
            }
         ]
      }
   },
   {
      "group":{
         "name":"opamgroup2",
         "dn":"cn=opamgroup2,ou=groups,ou=myrealm,dc=base_domain",
         "description":"",
         "users":[
            {
               "uid":"opamenduser1",
               "firstname":"opamenduser1",
               "lastname":"opamenduser1",
               "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
            },
            {
               "uid":"opamuser1",
               "lastname":"opamuser1",
               "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
            }
         ]
      }
   },
   {
      "group":{
         "name":"opamsubgroup1",
         "dn":"cn=opamsubgroup1,ou=groups,ou=myrealm,dc=base_domain",
         "description":"",
         "users":[

         ]
      }
   },
   {
      "group":{
         "name":"opamsubgroup2",
         "dn":"cn=opamsubgroup2,ou=groups,ou=myrealm,dc=base_domain",
         "description":"",
         "users":[

         ]
      }
```

```
      },
      {
         "group":{
            "name":"OPAM_APPLICATION_CONFIGURATOR",
            "dn":"cn=OPAM_APPLICATION_CONFIGURATOR,ou=groups,ou=myrealm,dc=base_domain",
            "description":"OPAM_APPLICATION_CONFIGURATOR",
            "users":[
               {
                  "uid":"app_config",
                  "lastname":"app_config",
                  "dn":"uid=app_config,ou=people,ou=myrealm,dc=base_domain"
               }
            ]
         }
      },
      {
         "group":{
            "name":"OPAM_SECURITY_ADMIN",
            "dn":"cn=OPAM_SECURITY_ADMIN,ou=groups,ou=myrealm,dc=base_domain",
            "description":"OPAM_SECURITY_ADMIN",
            "users":[
               {
                  "uid":"sec_admin",
                  "lastname":"sec_admin",
                  "dn":"uid=sec_admin,ou=people,ou=myrealm,dc=base_domain"
               }
            ]
         }
      },
      {
         "group":{
            "name":"OPAM_SECURITY_AUDITOR",
            "dn":"cn=OPAM_SECURITY_AUDITOR,ou=groups,ou=myrealm,dc=base_domain",
            "description":"OPAM_SECURITY_AUDITOR",
            "users":[
               {
                  "uid":"sec_auditor",
                  "lastname":"sec_auditor",
                  "dn":"uid=sec_auditor,ou=people,ou=myrealm,dc=base_domain"
               }
            ]
         }
      },
      {
         "group":{
            "name":"OPAM_USER_MANAGER",
            "dn":"cn=OPAM_USER_MANAGER,ou=groups,ou=myrealm,dc=base_domain",
            "description":"OPAM_USER_MANAGER",
            "users":[
               {
                  "uid":"user_manager",
                  "lastname":"user_manager",
                  "dn":"uid=user_manager,ou=people,ou=myrealm,dc=base_domain"
               }
            ]
         }
      }
   ]
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.5.3 Advanced Search for Groups

Use this API to search for users whose request parameters could be *groupname*. All of the parameters are optional.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/group/advancedsearch?param1=val1&param2=val2
Method	`GET`
Body	
Returns on Success	Status 200 and JSON representation of groups

Example B–28 Sample JSON Representation of Groups

```
{
   "groups":[
      {
         "group":{
            "name":"AdminChannelUsers",
            "dn":"cn=AdminChannelUsers,ou=groups,ou=myrealm,dc=base_domain",
            "description":"AdminChannelUsers can access the admin channel.",
            "users":[

            ],
            "accounts":[

            ]
         }
      },
      {
         "group":{
            "name":"Administrators",
            "dn":"cn=Administrators,ou=groups,ou=myrealm,dc=base_domain",
            "description":"Administrators can view and modify all resource attributes
               and start and stop servers.",
            "users":[
               {
                  "uid":"weblogic",
                  "lastname":"weblogic",
                  "dn":"uid=weblogic,ou=people,ou=myrealm,dc=base_domain"
               }
            ],
            "accounts":[

            ]
         }
      },
      {
         "group":{
            "name":"AppTesters",
            "dn":"cn=AppTesters,ou=groups,ou=myrealm,dc=base_domain",
            "description":"AppTesters group.",
            "users":[

            ],
            "accounts":[
```

```
      ]
   }
},
{
   "group":{
      "name":"CrossDomainConnectors",
      "dn":"cn=CrossDomainConnectors,ou=groups,ou=myrealm,dc=base_domain",
      "description":"CrossDomainConnectors can make inter-domain calls from
         foreign domains.",
      "users":[

      ],
      "accounts":[

      ]
   }
},
{
   "group":{
      "name":"Deployers",
      "dn":"cn=Deployers,ou=groups,ou=myrealm,dc=base_domain",
      "description":"Deployers can view all resource attributes and deploy applications.",
      "users":[

      ],
      "accounts":[

      ]
   }
},
{
   "group":{
      "name":"Monitors",
      "dn":"cn=Monitors,ou=groups,ou=myrealm,dc=base_domain",
      "description":"Monitors can view and modify all resource attributes
         and perform operations not restricted by roles.",
      "users":[

      ],
      "accounts":[

      ]
   }
},
{
   "group":{
      "name":"Operators",
      "dn":"cn=Operators,ou=groups,ou=myrealm,dc=base_domain",
      "description":"Operators can view and modify all resource attributes and
         perform server lifecycle operations.",
      "users":[

      ],
      "accounts":[

      ]
   }
},
{
```

```
   "group":{
      "name":"OracleSystemGroup",
      "dn":"cn=OracleSystemGroup,ou=groups,ou=myrealm,dc=base_domain",
      "description":"Oracle application software system group.",
      "users":[
         {
            "uid":"OracleSystemUser",
            "lastname":"OracleSystemUser",
            "dn":"uid=OracleSystemUser,ou=people,ou=myrealm,dc=base_domain"
         }
      ],
      "accounts":[

      ]
   }
},
{
   "group":{
      "name":"OPAM_APPLICATION_CONFIGURATOR",
      "dn":"cn=OPAM_APPLICATION_CONFIGURATOR,ou=groups,ou=myrealm,dc=base_domain",
      "description":"OPAM_APPLICATION_CONFIGURATOR",
      "users":[
         {
            "uid":"app_config",
            "lastname":"app_config",
            "dn":"uid=app_config,ou=people,ou=myrealm,dc=base_domain"
         }
      ],
      "accounts":[

      ]
   }
},
{
   "group":{
      "name":"OPAM_SECURITY_ADMIN",
      "dn":"cn=OPAM_SECURITY_ADMIN,ou=groups,ou=myrealm,dc=base_domain",
      "description":"OPAM_SECURITY_ADMIN",
      "users":[
         {
            "uid":"sec_admin",
            "lastname":"sec_admin",
            "dn":"uid=sec_admin,ou=people,ou=myrealm,dc=base_domain"
         }
      ],
      "accounts":[

      ]
   }
},
{
   "group":{
      "name":"OPAM_USER_MANAGER",
      "dn":"cn=OPAM_USER_MANAGER,ou=groups,ou=myrealm,dc=base_domain",
      "description":"OPAM_USER_MANAGER",
      "users":[
         {
            "uid":"user_manager",
            "lastname":"user_manager",
            "dn":"uid=user_manager,ou=people,ou=myrealm,dc=base_domain"
```

```
            }
         ],
         "accounts":[

         ]
      }
   },
   {
      "group":{
         "name":"OPAM_SECURITY_AUDITOR",
         "dn":"cn=OPAM_SECURITY_AUDITOR,ou=groups,ou=myrealm,dc=base_domain",
         "description":"OPAM_SECURITY_AUDITOR",
         "users":[
            {
               "uid":"sec_auditor",
               "lastname":"sec_auditor",
               "dn":"uid=sec_auditor,ou=people,ou=myrealm,dc=base_domain"
            }
         ],
         "accounts":[

         ]
      }
   },
   {
      "group":{
         "name":"opamgroup1",
         "dn":"cn=opamgroup1,ou=groups,ou=myrealm,dc=base_domain",
         "description":"",
         "users":[
            {
               "uid":"opamenduser1",
               "firstname":"opamenduser1",
               "lastname":"opamenduser1",
               "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
            },
            {
               "uid":"opamuser1",
               "lastname":"opamuser1",
               "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
            }
         ],
         "accounts":[

         ]
      }
   },
   {
      "group":{
         "name":"opamgroup2",
         "dn":"cn=opamgroup2,ou=groups,ou=myrealm,dc=base_domain",
         "description":"",
         "users":[
            {
               "uid":"opamenduser1",
               "firstname":"opamenduser1",
               "lastname":"opamenduser1",
               "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
            },
            {
```

```
                "uid":"opamuser1",
                "lastname":"opamuser1",
                "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
             }
          ],
          "accounts":[

          ]
       }
    },
    {
       "group":{
          "name":"opamsubgroup1",
          "dn":"cn=opamsubgroup1,ou=groups,ou=myrealm,dc=base_domain",
          "description":"",
          "users":[

          ],
          "accounts":[

          ]
       }
    },
    {
       "group":{
          "name":"opamsubgroup2",
          "dn":"cn=opamsubgroup2,ou=groups,ou=myrealm,dc=base_domain",
          "description":"",
          "users":[

          ],
          "accounts":[

          ]
       }
    }
 ]
}
```


For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource."

B.6 Usage Policy Resource

The APIs described in this section include:

- Create a Usage Policy
- Retrieve a Usage Policy
- Update a Usage Policy
- Delete a Usage Policy

B.6.1 Create a Usage Policy

Use this API to create a Usage Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/usagepolicy

Method	POST
Body	JSON representation for Usage Policy creation
Returns on Success	Status code 201

Example B–29 Sample JSON Representation for Usage Policy Creation

```
{
   "usagepolicy":{
      "policystatus":"active",
      "policyname":"Default Usage Policy",
      "description":"Default Usage Policy",
      "dateorduration":"duration",
      "expireddateminutesfromcheckout":7200,
      "expireddate":"08\/08\/2088",
      "expireddatehour":0,
      "expireddateminutes":0,
      "expireddateamorpm":"am",
      "timezone":"America\/Los_Angeles",
      "usagedates":[
         {
            "day":"saturday",
            "fromhour":"12",
            "fromminutes":"0",
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         },
         {
            "day":"wednesday",
            "fromhour":"12",
            "fromminutes":"0",
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         },
         {
            "day":"sunday",
            "fromhour":"12",
            "fromminutes":"0",
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         },
         {
            "day":"friday",
            "fromhour":"12",
            "fromminutes":"0",
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         },
         {
            "day":"tuesday",
            "fromhour":"12",
            "fromminutes":"0",
```

```
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         },
         {
            "day":"thursday",
            "fromhour":"12",
            "frommminutes":"0",
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         },
         {
            "day":"monday",
            "fromhour":"12",
            "frommminutes":"0",
            "fromamorpm":"am",
            "tohour":"12",
            "tominutes":"0",
            "toamorpm":"am"
         }
      ]
   }
}
```

For attribute definitions, refer to Section B.1, "Target Resource" and Section B.2, "Account Resource." All parameters are optional, except `policyname`.

B.6.2 Retrieve a Usage Policy

Use this API to retrieve a Usage Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/usagepolicy/{policyid}
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of Usage Policy

Example B–30 Sample JSON Representation of Usage Policy

```
{
   "usagepolicy":{
      "policyid":"usagepolicy1",
      "policystatus":"active",
      "policyname":"Default Usage Policy",
      "description":"Default Usage Policy",
      "globaldefault":"y",
      "dateorduration":"duration",
      "expireddateminutesfromcheckout":7200,
      "expireddate":"08\/08\/2088",
      "expireddatehour":0,
      "expireddateminutes":0,
      "expireddateamorpm":"am",
      "timezone":"America\/Los_Angeles",
      "usagedates":[
         {
            "day":"saturday",
```

```
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
    },
    {
        "day":"wednesday",
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
    },
    {
        "day":"sunday",
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
    },
    {
        "day":"friday",
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
    },
    {
        "day":"tuesday",
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
    },
    {
        "day":"thursday",
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
    },
    {
        "day":"monday",
        "fromhour":"12",
        "fromminutes":"0",
        "fromamorpm":"am",
        "tohour":"12",
        "tominutes":"0",
        "toamorpm":"am"
```

```
      }
   ],
   "accounts":[
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /c11066278022489aad758aec69d9727d",
            "accountUID":"c11066278022489aad758aec69d9727d",
            "accountName":"himanshu",
            "status":"checkedIn",
            "targetName":"hhsharma-ldap",
            "targetType":"ldap",
            "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
            "domain":"berkeley",
            "grantees":{
               "users":[

               ],
               "roles":[
                  {
                     "role":{
                        "name":"Administrators",
                        "usagepolicy":"usagepolicy1",
                        "usagepolicyname":"Default Usage Policy",
                        "description":"Administrators can view and modify all resource
                            attributes and start and stop servers."
                     }
                  },
                  {
                     "role":{
                        "name":"opamgroup1",
                        "usagepolicy":"usagepolicy1",
                        "usagepolicyname":"Default Usage Policy",
                        "description":""
                     }
                  },
                  {
                     "role":{
                        "name":"opamgroup2",
                        "usagepolicy":"usagepolicy1",
                        "usagepolicyname":"Default Usage Policy",
                        "description":""
                     }
                  }
               ]
            }
         }
      },
      {
         "account":{
            "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
               /3740553e999a4f6aa8e8f9286d320cb4",
            "accountUID":"3740553e999a4f6aa8e8f9286d320cb4",
            "accountName":"sherlock",
            "status":"checkedOut",
            "targetName":"hhsharma-ldap",
            "targetType":"ldap",
            "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
            "domain":"berkeley",
            "grantees":{
```

```
            "users":[
               {
                  "user":{
                     "uid":"sec_admin",
                     "usagepolicy":"usagepolicy1",
                     "usagepolicyname":"Default Usage Policy",
                     "lastname":"sec_admin",
                     "dn":"uid=sec_admin,ou=people,ou=myrealm,dc=base_domain"
                  }
               },
               {
                  "user":{
                     "uid":"opamenduser1",
                     "usagepolicy":"usagepolicy1",
                     "usagepolicyname":"Default Usage Policy",
                     "firstname":"opamenduser1",
                     "lastname":"opamenduser1",
                     "dn":"uid=opamenduser1,ou=people,ou=myrealm,dc=base_domain"
                  }
               },
               {
                  "user":{
                     "uid":"opamenduser2",
                     "usagepolicy":"usagepolicy1",
                     "usagepolicyname":"Default Usage Policy",
                     "lastname":"opamenduser2",
                     "dn":"uid=opamenduser2,ou=people,ou=myrealm,dc=base_domain"
                  }
               },
               {
                  "user":{
                     "uid":"opamuser1",
                     "usagepolicy":"usagepolicy1",
                     "usagepolicyname":"Default Usage Policy",
                     "lastname":"opamuser1",
                     "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
                  }
               }
            ],
            "roles":[

            ]
         }
      }
   },
   {
      "account":{
         "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\
            /account\/154034fc5b5548caad7721e198815709",
         "accountUID":"154034fc5b5548caad7721e198815709",
         "accountName":"lucie",
         "status":"checkedIn",
         "targetName":"hhsharma-ldap",
         "targetType":"ldap",
         "targetUID":"9bbcbbb087174ad1900ea691a2573b61",
         "domain":"berkeley",
         "grantees":{
            "users":[
               {
                  "user":{
```

```
                        "uid":"opamuser1",
                        "usagepolicy":"usagepolicy1",
                        "usagepolicyname":"Default Usage Policy",
                        "lastname":"opamuser1",
                        "dn":"uid=opamuser1,ou=people,ou=myrealm,dc=base_domain"
                     }
                  },
                  {
                     "user":{
                        "uid":"opamenduser2",
                        "usagepolicy":"usagepolicy1",
                        "usagepolicyname":"Default Usage Policy",
                        "lastname":"opamenduser2",
                        "dn":"uid=opamenduser2,ou=people,ou=myrealm,dc=base_domain"
                     }
                  }
               ],
               "roles":[

               ]
            }
         }
      }
   ]
}
```

Where:

- **usagepolicy** is a usagepolicy JSON object.
- **policyid** is the Usage Policy's unique identifier.
- **policystatus** is set to active or disabled.
- **policyname** is a name of the policy
- **description** is a description of the policy.
- **globaldefault** indicates whether the policy is the global default policy or not.
- **dateorduration** indicates how the expiration time is calculated.
  - If set to `date`, then `expireddate`, `expireddatehour`, `expireddateminutes`, and `expireddateamorpm` are used.
  - If set to `duration`, then `expireddateminutesfromcheckout` is used.

  Where:
  - **expireddate** is the date of expiration.
  - **expireddatehour.hour** are integer values between 0 and 12.
  - **expireddateminutes.minutes** are integer values between 0 and 60.
  - **expireddateamorpm** is a.m. or p.m.
  - **expireddateminutesfromcheckout** are minutes from checkout.
- **timezone** is a time zone for the Usage Policy.
- **usagedates** is an array, where each value represents the check out time for individual days.

- **day** is a day of the week, where acceptable values are `sunday`, `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, and `saturday`.

Use the following attributes to indicate a range from and to:

- **fromhour** is an integer value between 0 and 12.
- **fromminutes** is a n integer value between 0 and 60.
- **fromamorpm** is a.m. or p.m.
- **tohour** is a ***n*** integer value between 0 and 12.
- **tominutes** is a n integer value between 0 and 60.
- **toamorpm** is a.m. or p.m.

B.6.3 Update a Usage Policy

Use this API to update a Usage Policy. You can update all attributes, except `policyid`, and you can update multiple attributes at a time.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/usagepolicy/{policyid}
Method	`PUT`
Body	JSON representation of Usage Policy modification
Returns on Success	Status code 200

Example B–31 Sample JSON Representation of Usage Policy Modification

```
{
   "modifications":[
      {
         "modification":{
            "usagedates":[
               {
                  "day":"saturday",
                  "fromhour":"12",
                  "fromminutes":"0",
                  "fromamorpm":"am",
                  "tohour":"12",
                  "tominutes":"0",
                  "toamorpm":"am"
               },
               {
                  "day":"wednesday",
                  "fromhour":"12",
                  "fromminutes":"0",
                  "fromamorpm":"am",
                  "tohour":"12",
                  "tominutes":"0",
                  "toamorpm":"am"
               }
            ]
         }
      },
      {
         "modification":{
            "expireddatehour":2
         }
      }
```

```
   ]
}
```

Where:

- **modifications** are an array of modification JSON objects.
- **modification** is a JSON object representing a single attribute.

You must update the `usagedates` and `expireddatehour` attributes on the target. Their value is updated to the value provided with them.

B.6.4 Delete a Usage Policy

Use this API to delete a Usage Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/usagepolicy/{policyid}
Method	`DELETE`
Body	
Returns on Success	Status 200

B.7 Password Policy Resource

The APIs described in this section include:

- Create a Password Policy
- Retrieve a Password Policy
- Delete a Password Policy
- Update a Password Policy

B.7.1 Create a Password Policy

Use this API to create a Password Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/passwordpolicy
Method	`POST`
Body	JSON representation for Password Policy creation
Returns on Success	Status code 201

Example B–32 Sample JSON Representation for Password Policy Creation

```
{
   "passwordpolicy":{
      "policystatus":"active",
      "policyname":"Default Password Policy",
      "description":"Default Password Policy",
      "passwordchangedurationunit":"days",
      "passwordchangedurationvalue":30,
      "changeoncheckin":"y",
      "changeoncheckout":"y",
      "passwordcharsmin":8,
      "passwordcharsmax":8,
      "passwordalphabeticmin":1,
      "passwordnumericmin":1,
```

```
      "passwordalphanumericmin":2,
      "passworduniquemin":1,
      "passworduppercasemin":1,
      "passwordlowercasemin":1,
      "passwordspecialmin":0,
      "passwordspecialmax":0,
      "passwordrepeatedmin":0,
      "passwordrepeatedmax":1,
      "startingchar":"n",
      "isaccountnameallowed":"n",
      "requiredchars":[
         "a",
         "h",
         "j"
      ],
      "allowedchars":[
         "b",
         "t",
         "y",
         "p",
         "u",
         "r",
         "o",
         "k",
         "1",
         "2",
         "=",
         "M",
         "a",
         "h",
         "j"
      ],
      "disalloweddchars":[
         "7",
         "8",
         "l"
      ]
   }
}
```

All attributes are optional, except `policyname`.

B.7.2 Retrieve a Password Policy

Use this API to retrieve a Password Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/passwordpolicy/{policyid}
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of Password Policy

Example B–33 Sample JSON Representation of Password Policy

```
{
   "passwordpolicy":{
      "policyid":"passwordpolicy2",
      "policystatus":"active",
      "policyname":"Default Password Policy",
```

```
"description":"Default Password Policy",
"globaldefault":"y",
"passwordchangedurationunit":"days",
"passwordchangedurationvalue":30,
"changeoncheckin":"y",
"changeoncheckout":"y",
"passwordcharsmin":8,
"passwordcharsmax":8,
"passwordalphabeticmin":1,
"passwordnumericmin":1,
"passwordalphanumericmin":2,
"passworduniquemin":1,
"passworduppercasemin":1,
"passwordlowercasemin":1,
"passwordspecialmin":0,
"passwordspecialmax":0,
"passwordrepeatedmin":0,
"passwordrepeatedmax":1,
"startingchar":"n",
"isaccountnameallowed":"n",
"requiredchars":[
   "a",
   "h",
   "j"
],
"allowedchars":[
   "b",
   "t",
   "y",
   "p",
   "u",
   "r",
   "o",
   "k",
   "1",
   "2",
   "=",
   "M",
   "a",
   "h",
   "j"
],
"disalloweddchars":[
   "7",
   "8",
   "l"
],
"accounts":[
   {
      "account":{
         "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
            /3740553e999a4f6aa8e8f9286d320cb4",
         "accountUID":"3740553e999a4f6aa8e8f9286d320cb4",
         "accountName":"sherlock",
         "status":"checkedOut",
         "targetName":"hhsharma-ldap",
         "targetType":"ldap",
         "domain":"berkeley",
         "grantees":{
            "users":[
```

```
                ],
                "roles":[

                ]
             }
          }
       },
       {
          "account":{
             "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
                /c11066278022489aad758aec69d9727d",
             "accountUID":"c11066278022489aad758aec69d9727d",
             "accountName":"himanshu",
             "status":"checkedIn",
             "targetName":"hhsharma-ldap",
             "targetType":"ldap",
             "domain":"berkeley",
             "grantees":{
                "users":[

                ],
                "roles":[

                ]
             }
          }
       },
       {
          "account":{
             "uri":"https:\/\/opam_server_host:opam_ssl_port\/opam\/account\
                /154034fc5b5548caad7721e198815709",
             "accountUID":"154034fc5b5548caad7721e198815709",
             "accountName":"lucie",
             "status":"checkedIn",
             "targetName":"hhsharma-ldap",
             "targetType":"ldap",
             "domain":"berkeley",
             "grantees":{
                "users":[

                ],
                "roles":[

                ]
             }
          }
       }
    ]
  }
}
```

Where:

- **passwordpolicy** is a passwordpolicy JSON object.
- **policyid** is the policy's unique identifier.
- **policystatus** is the policy's status, where acceptable values are `active` or `disabled`.
- **policyname** is the policy name

- **description** is a description of the policy.
- **globaldefault** indicates whether the policy is a global default or not.
- **dateorduration** indicates how the expiration time is calculated.
  - If set to `date`, then `expireddate`, `expireddatehour`, `expireddateminutes`, and `expireddateamorpm` are used.
  - If set to `duration`, then `expireddateminutesfromcheckout` is used.

  Where:
  - **expireddate** is the date of expiration.
  - **expireddatehour.hour** are integer values between 0 and 12.
  - **expireddateminutes.minutes** are integer values between 0 and 60.
  - **expireddateamorpm** is a.m. or p.m.
  - **expireddateminutesfromcheckout** are minutes from checkout.
- **timezone** is a time zone for the Usage Policy.
- **usagedates** is an array, where each value represents the check out time for individual days.
- **day** is a day of the week, where acceptable values are `sunday`, `monday`, `tuesday`, `wednesday`, `thursday`, `friday`, and `saturday`.

For other attribute definitions, refer to Section B.2, "Account Resource."

B.7.3 Delete a Password Policy

Use this API to delete a Password Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/passwordpolicy/{policyid}
Method	`DELETE`
Body	
Returns on Success	Status 200

B.7.4 Update a Password Policy

Use this API to update a Usage Policy. You can update all of the attributes, except `policyid`, and you can update multiple attributes at a time.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/passwordpolicy/{policyid}
Method	`PUT`
Body	JSON representation for Password Policy modification
Returns on Success	Status code 201

Example B–34 Sample JSON Representation of Password Policy Modification

```
{
   "modifications":[
      {
         "modification":{
            "disalloweddchars":[
               "4",
```

```
                "6"
             ]
          }
       },
       {
          "modification":{
             "passwordalphabeticmin":2
          }
       }
    ]
}
```

Where:

- **modifications** is an array of modification JSON objects.
- **modification** is a JSON object representing a single attribute.

You must update the `disalloweddchars` and `passwordalphabeticmin` attributes on the target. These attribute values are updated to the values provided with them.

B.8 Policy Resource

The APIs described in this section include:

- Search for Policies
- Get Default Policies

B.8.1 Search for Policies

Use this API to search for the accounts. This API is a contains search, using one or more of the following parameters:

- `policystatus`
- `policyname`
- `accountname`

All of the parameters are optional.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/policy/search?param1=val1&param2=val2
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of policies

Example B–35 Sample JSON Representation of Policies

```
{
   "usagepolicies":[
      {
         "policyname":"Default Usage Policy",
         "policyid":"usagepolicy1",
         "policystatus":"active",
         "globaldefault":"y"
      }
   ],
   "passwordpolicies":[
      {
```

```
         "policyname":"Default Password Policy",
         "policyid":"passwordpolicy2",
         "policystatus":"active",
         "globaldefault":"y"
      }
   ]
}
```

Where:

- **usagepolicies** are an array of Usage Policies.
- **passwordpolicies** are an array of Password Policies.
- **policyname** is the policy name.
- **policyid** is the policy's unique identifier.
- **policystatus** is the policy status, where acceptable values are `active` or `disabled`.

B.8.2 Get Default Policies

Use this API to get the Default Usage Policy and Default Password Policy.

URI	https://*opam_server_host*:*opam_ssl_port*/opam/policy/default
Method	`GET`
Body	
Returns on Success	Status code 200 and JSON representation of policies

Example B–36 Sample JSON Representation of Policies

```
{
   "usagepolicies":[
      {
         "policyname":"Default Usage Policy",
         "policyid":"usagepolicy1",
         "policystatus":"active"
      }
   ],
   "passwordpolicies":[
      {
         "policyname":"Default Password Policy",
         "policyid":"passwordpolicy2",
         "policystatus":"active"
      }
   ]
}
```

Where:

- **usagepolicies** is an array of Usage Policies.
- **passwordpolicies** is an array of Password Policies.
- **policyname** is the policy name.
- **policyid** is the policy's unique identifier.
- **policystatus** is the policy status, where acceptable values are `active` or `disabled`.

This attribute only returns the default policies, Default Usage Policy and Default Password Policy.

C

Troubleshooting Oracle Privileged Account Manager

This appendix describes how to diagnose and solve common problems that you might encounter when using Oracle Privileged Account Manager.

The information in this appendix is organized into the following sections:

C.1 Common Problems and Solutions

This section describes some common problems and provides information to help you resolve those problems.

The topics include:

C.1.1 Console Cannot Connect to Oracle Privileged Account Manager Server

Oracle Privileged Account Manager Console cannot connect to the Oracle Privileged Account Manager server.

Reason

If the Console is not connecting to the Oracle Privileged Account Manager server, then you might have a configuration problem with the Console or with Oracle Platform Security Services Trust.

Solution

- Verify that your host and port information is correct. Confirm that the generated URL displayed on the Console is responsive.
- Ensure that you correctly completed all of the configuration steps described in "Post-Installation Tasks" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

C.1.2 Console Changes Are Not Reflected in Other, Open Pages

When you have multiple browser windows or Console tabs open against the same Oracle Privileged Account Manager Console, updates made in one window or tab are not immediately reflected in the other windows or tabs.

Reason

The Oracle Privileged Account Manager Console does not proactively push updates to the browser.

Solution:

Refresh the browser window or tab.

C.1.3 Cannot Access Targets or Accounts

Your attempts to access targets and privileged accounts are failing. You cannot check-out, check-in, or test.

Reason

The ICF connector being used by Oracle Privileged Account Manager is having issues interacting with the target system.

Solution:

- Verify that the target system is up, and that the privileged account of interest exists.
- Increase Oracle Privileged Account Manager's logging level to **`TRACE:32`** (its finest level) and review the trace logs to determine where the failure occurs.

  Problems are often caused by environmental issues that can be identified using the trace logs and remedied by fixing the configuration on the target system. Refer to Chapter 6, "Managing Oracle Privileged Account Manager Auditing and Logging" for more information.
- You might have a connector issue. Submit a bug that includes a reproducible test case, target system details, and trace logs.

C.1.4 Cannot Add Database Targets

This section describes issues that can prevent you from adding database targets:

C.1.4.1 Cannot Connect to Oracle Database with `sysdba` Role

Your attempts to connect to Oracle Database using the `sysdba` role are failing with the following error message:

```
Invalid Connection Details, see server log for details.
```

Reason

To connect to Oracle Database as a user with `sysdba` role, you must configure the **Advanced Properties** option with the value, **`internal_logon=sysdba`**.

You must also specify this setting for the Oracle Database `SYS` account, which must connect with the `sysdba` role. The Oracle Database `SYS` user is a special account and if you do not use this role, then the connection might fail. However, it is a better practice to create an Oracle Privileged Account Manager service account instead of using `SYS`.

Solution:

Perform the following steps to connect to Oracle Database as a user with the **sysdba** role:

> **Note:** These configuration steps are not necessary if you are connecting as a normal user.

1. Open the target's General tab and expand **Advanced Configuration** to view the configuration options.
2. Enter the `internal_logon=sysdba` value into the **Connection Properties** field.
3. Click **Test** to retest the connection.
4. **Save** your changes.

C.1.4.2 Cannot Find Special Options for Adding a Database Target

You cannot find configuration options for connecting to database targets such as Oracle RAC Database or for using Secure Socket Layer (SSL).

Reason

Oracle Privileged Account Manager uses a Generic Database connector where special configuration options for specific database target systems are not exposed in a clean or intuitive manner.

Solution:

Define special connectivity options for database targets by modifying the **Database Connection URL** and **Connection Properties** parameter values.

> **Note:**
>
> - See Section 5.1.2.2, "Adding Targets to Oracle Privileged Account Manager" for information about these parameters.
> - Refer to the *Oracle Identity Manager Connector Guide for Database User Management* for information about which special options are supported.

C.1.5 Cannot Add an Active Directory LDAP Target

An LDAP target using Microsoft Active Directory fails when you test the connection, search for accounts, or check out passwords.

Reason

Active Directory defaults require specific configuration, so you must change the generic default values for the LDAP target. Oracle Privileged Account Manager uses a Generic LDAP connector where special or custom configuration options for specific LDAP target systems are not obvious. (Usually, only Active Directory LDAP targets cause issues.)

Solution:

When adding the LDAP target, you must

- Use SSL to communicate with Active Directory.
  - Import the SSL certificates into the WebLogic instance running Oracle Privileged Account Manager. Refer to Section 3.3.2, "Configuring SSL Communication in Oracle Privileged Account Manager" for more information.
  - From the Targets page, set the **TCP Port** to your Active Directory SSL port and enable the **SSL** checkbox. (see Table 5–2)
- Specify the following **Advanced Configuration** parameters (see Table 5–3):
  - Set **Password Attribute** to **`unicodepwd`**
  - Set **Advanced Configuration** > **Account Object Classes** to **`top|person|organizationalPerson|user`**.
- Specify an attribute that is suitable for data in Active Directory, such as `uid` or `samaccountname`, for the **Account User Name Attribute**, **Uid Attribute**, and **LDAP Filter for Retrieving Accounts** configuration parameters (described in Table 5–2 and Table 5–3).

C.1.6 Grantee Cannot Perform a Checkout

A grantee's attempt to checkout an account is failing with an `Insufficient Privileges` error.

Reason

The username is case-sensitive for Oracle Privileged Account Manager grants, but not always for WebLogic authentication.

Solution:

Ensure that you enable the **Use Retrieved User Name As Principal** option for the authenticator being used for your production ID Store. Refer to Section 4.3.1, "Configuring the External Identity Store" for more information.

C.1.7 Cannot View Roles from the Configured Remote ID Store

When you try to grant to a user or group, you cannot view all roles from the configured remote ID Store.

Reason

You logged into Oracle Privileged Account Manager with a user ID that has been retrieved from a user, on an authenticator that is not pointing to your ID Store. The culprit is usually the DefaultAuthenticator.

Solution:

Perform the following actions:

- Set the Control Flag for all authenticators to `SUFFICIENT`.
- Verify that the user who is logging in exists on the remote ID store.
- Verify that the user has the relevant Oracle Privileged Account ManagerAdmin Roles. (Refer to Section 2.3.1, "Administration Role Types" for more information.)
- Ensure those Oracle Privileged Account ManagerAdmin Roles exist on the remote ID Store.

C.1.8 Group Membership Changes Are Not Immediately Reflected in Oracle Privileged Account Manager

You have an indirect grant through group membership and updates to that group membership are not immediately reflected in Oracle Privileged Account Manager.

For example, if you assign a user to a Oracle Privileged Account Manager administration role or to a group granted with a Oracle Privileged Account Manager privileged account, you may not be able to view these changes right away.

Reason

WebLogic caches group memberships from Identity Store providers by default.

Solution:

Modify the caching settings in your WebLogic Authenticator and Asserter configuration to suit your requirements.

Note: For more information, refer to "Optimizing the Group Membership Caches" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

C.1.9 Cannot Use Larger Key Sizes for Export/Import

You are unable to use key sizes larger than 128-bits for export or import operations.

Reason

The default JRE installation does not contain the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6.

Solution:

Apply the JCE patch, available for download from `http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html`

C.2 Diagnosing Oracle Privileged Account Manager Problems

This section provides information about how to diagnose Oracle Privileged Account Manager problems.

The topics include:

- Increase the Log Level
- Examine Exceptions in the Logs

C.2.1 Increase the Log Level

When an Oracle Privileged Account Manager error occurs, you can gather more information about what caused the error by generating complete logs that include debug information and connector logging. the following steps:

1. Set the Oracle Privileged Account Manager logging level to the finest level, which is **`TRACE:32`**.

   Note:

   - For more information about Oracle Privileged Account Manager logging, refer to Chapter 6, "Managing Oracle Privileged Account Manager Auditing and Logging."
   - For instructions about how to set logging levels, refer to "Logging Implementation Guidelines" *Oracle Containers for J2EE Developer's Guide*.

2. Repeat the task or procedure where you originally encountered the error.
3. Examine the log information generated using the DEBUG level.

C.2.2 Examine Exceptions in the Logs

Examining the exceptions logged to the Oracle Privileged Account Manager log file can help you identify various problems.

You can access Oracle Privileged Account Manager's diagnostic log in the following directories:

```
DOMAIN_HOME/servers/Adminserver/logs
DOMAIN_HOME/servers/opamserver/logs
```

C.3 Need More Help?

You can find more solutions on My Oracle Support (formerly MetaLink) at http://support.oracle.com. If you do not find a solution for your problem, log a service request.

Glossary

account

An account on a target.

ADF

Oracle Application Development Framework. An end-to-end development framework, built on top of the Enterprise Java platform, that provides integrated infrastructure solutions for the various layers of an application and an easy way to develop on top of those layers.

authentication provider

A security provider that manages and enforces authentication rules.

For more detailed information, refer to "Configuring Authentication Providers" in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

BI Publisher

An Oracle reporting product that can create and manage formatted reports from different data sources.

bootstrap user

A default administrator (`weblogic` user) who is a member of the Administrators group. This user can create and assign users to Oracle Privileged Account Manager Admin Roles and can map users from the domain identity store to Oracle Privileged Account Manager Common Admin Roles.

Credential Store Framework

See ***CSF***.

CRUD

Create, Read, Update, and Delete. Basic functions of persistent storage or a database.

CSF

Credential Store Framework. An OPSS component that primarily provides secure storage for credentials.

DOMAIN_HOME

An environment variable that is usually

MIDDLEWARE_HOME`/user_projects/domains/<`*domain_name*`>`

Grantee

A user, group, or role that has been granted access to a *privileged account*.

ICF

Identity Connector FrameWork. A component that provides basic provisioning, reconciliation, and other functions required by all Oracle Identity Manager and Oracle Waveset connectors.

Identity Connector FrameWork

See ***ICF***.

identity propagation

Process in which the OPSS Trust Service Asserter examines and validates a token, and then asserts that the identity performing a RESTful call against the Oracle Privileged Account Manager server is the one contained in the token.

JSON representation

JavaScript Object Notation. A lightweight, human-readable data format that is taken from JavaScript and used to exchange information between a browser and a server.

ldifmigrator tool

Oracle Internet Directory Data Migration Tool. Converts LDIF files output from other directories or application-specific repositories into a format recognized by Oracle Internet Directory.

Oracle Privileged Account Manager client

Component that resides with the Oracle Privileged Account Manager target to provide passwords to the system for unattended connections.

Oracle Privileged Account Manager server

Component that handles password requests, generates passwords, protects the password keystore, etc.

Oracle Privileged Account Manager target

Component that has its privileged passwords managed by Oracle Privileged Account Manager.

OPSS

Oracle Platform Security Services. A standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.

Oracle Application Development Framework

See ***ADF***.

Oracle Internet Directory Data Migration Tool

See ***ldifmigrator tool***.

Oracle Platform Security Services

See ***OPSS***.

Password Policy

Captures the password construction requirements enforced by a specific *target* on an associated *privileged account*. Administrators use this policy to construct the password value that Oracle Privileged Account Manager uses to reset a password on a privileged account. Every privileged account managed by Oracle Privileged Account Manager has an associated Password Policy.

privileged account

An account on a target that is deemed "privileged" in a deployment and is under Oracle Privileged Account Manager's purview. Accounts are usually privileged when

- They are associated with elevated privileges
- They are used by multiple end-users on a task-by-task basis
- Their use must be controlled and audited

Repository Creation Utility

Oracle Repository Creation Utility. An application that you can use to create a schema and load a repository into the database.

Representational State Transfer

See ***REST***.

resources

Representation of targets and accounts.

REST

Representational State Transfer. Software architecture style for distributed hypermedia systems like the World Wide Web. Conforming to REST constraints is otherwise known as being *RESTful*.

SAML

Security Assertion Markup Language. An XML-based open standard product provided by the OASIS Security Services Technical Committee that enables the exchange of authentication and authorization data between security domains.

Security Assertion Markup Language

See ***SAML***

service account

An account that Oracle Privileged Account Manager uses when it connects to a target system and to perform all Oracle Privileged Account Manager-related operations (such as discovering accounts, resetting passwords, and so forth) on that target system, Service accounts require some special privileges and properties. Service accounts are sometimes referred to as *unattended accounts*.

shiphome

The directory where you downloaded and extracted Oracle Privileged Account Manager.

target

A software system that contains, uses, and relies on accounts (user, system, or application).

unattended accounts

See *service account*.

Usage Policy

Defines the constraints around when and how a grantee can use a privileged account. Each privileged account managed by Oracle Privileged Account Manager has an associated Usage Policy.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W