



# System Integrator's Guide (Printable)

Added by K-2, last edited by K-2 on Feb 04, 2010

## Sun Role Manager 5.0.3 System Integrator's Guide

### About This Guide

This guide describes how to integrate Sun™ Role Manager 5.0.3 software with other applications in a heterogeneous IT environment. Included in this guide is information about how to integrate with Sun Identity Manager, which is Sun's resource provisioning solution.

### Who Should Read This Guide

The *Sun Role Manager 5.0.3 System Integrator's Guide* is written for deployment engineers and service providers who are responsible for integrating Sun Role Manager with other IT systems.

- System administrators and service providers who need information about how to monitor and administer the Sun Role Manager software at a systems level should see the ***Sun Role Manager 5.0.3 System Administrator's Guide***.
- Compliance officers and IT specialists who need to configure and maintain role management and compliance functionality should see the ***Sun Role Manager 5.0.3 Business Administrator's Guide***.
- Business managers and other users in a supervisory role who need information about how to use the Sun Role Manager 5.0.3 software to grant employees and partners access to applications, check for access violations, and so on should see the ***Sun Role Manager 5.0.3 User's Guide***.

## Integrating With Sun Identity Manager

### Overview

Sun™ Role Manager software (Role Manager) and Sun Identity Manager software work together seamlessly when integrated using the Service Provisioning Mark-Up Language (SPML). When integrated, Identity Manager serves as the automated provisioning and identity synchronization solution, while Role Manager defines the Role-based Access Control (RBAC) framework, the attestation process, and the approach to Segregation Of Duties (SoD) policy enforcement. Rather than assigning individual access entitlements, the RBAC framework allows organizations to assign and unassign roles as a means of controlling user access on various applications.

The Role Manager Identity Warehouse makes it possible for Role Manager to manage users and their identities across various target systems. Before Role Manager features can be utilized, however, the Identity Warehouse of users and their entitlements must be built. If Sun Identity Manager is already in use, building the Identity Warehouse is as easy as connecting to Identity Manager and importing the user entitlement information that is stored in the Identity Manager repository. Roles are then assigned to users, either based on their actual entitlements or business-level attributes. These roles can be exported to Sun Identity Manager for user management and provisioning purposes. Additionally, revocations made during the certification campaigns can also be sent from Role Manager to Identity Manager so that remediation can take place.

# The Combined Solution

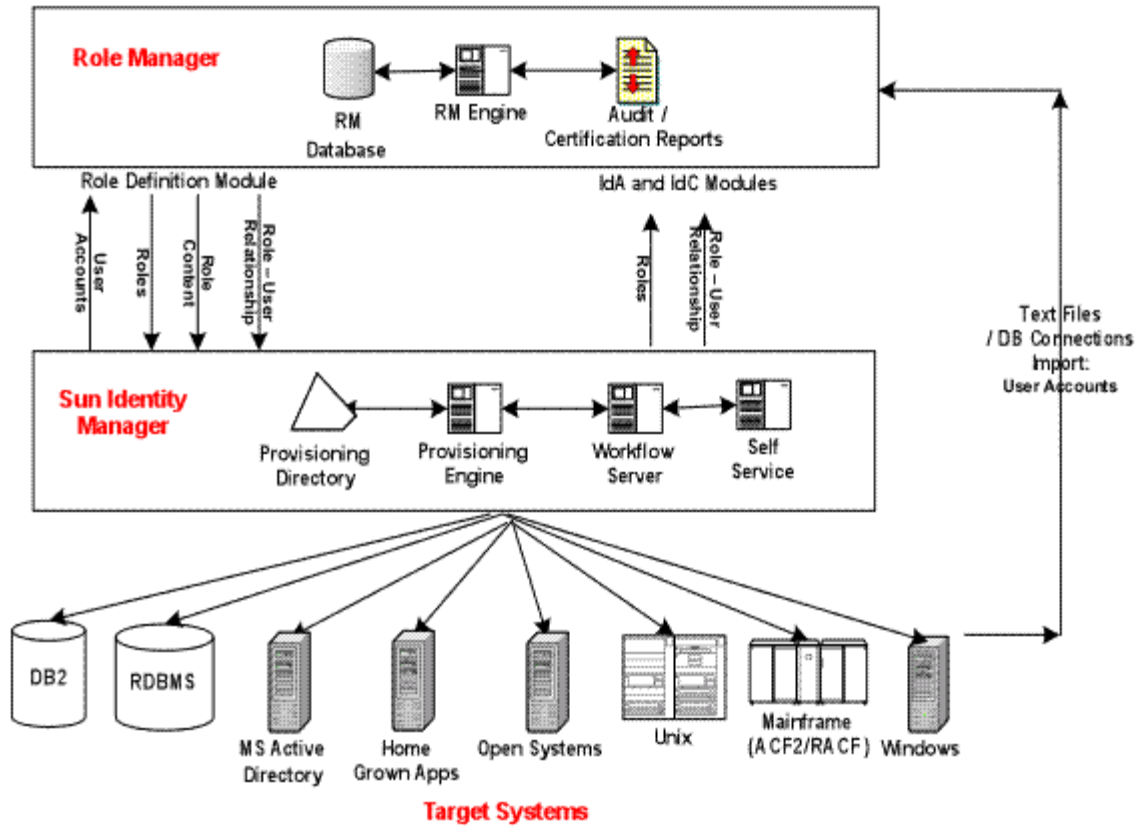


Refer to the [Sun Role Manager 5.0.3 User's Guide](#) for explanations of attributes, attribute categories, resource types, and other concepts.

Sun Role Manager and Sun Identity Manager share the following integration points:

- Identity Manager *users* are imported into Role Manager
- Identity Manager *resources* are imported into Role Manager
- Identity Manager *resource metadata* is imported into Role Manager
- Identity Manager *user accounts* are imported into Role Manager
- Role Manager *roles* and *role content* are exported to Identity Manager
- Closed Loop Compliance

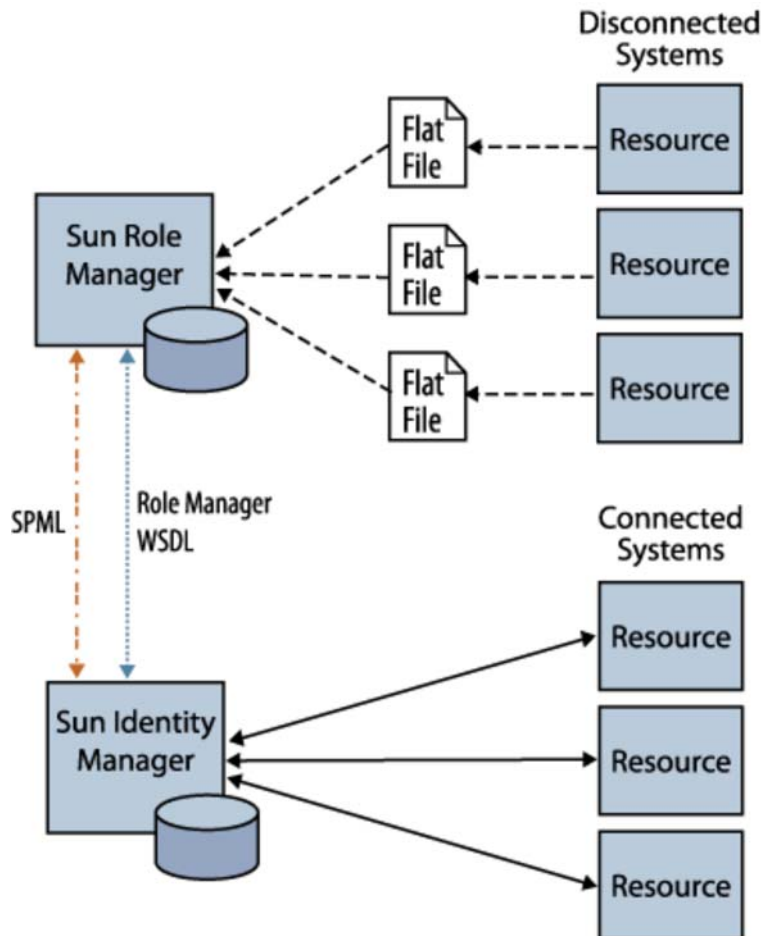
**Note** - See the [Role Manager Importing](#) chapter in the [Sun Role Manager 5.0.3 Business Administrator's Guide](#) for more information about the import process.



## Integration Architecture

As illustrated in the following figure, Identity Manager and Role Manager use SPML and Web Services (WSDL) to communicate. SPML calls are used when Role Manager initiates requests, and Web Services are used when Identity Manager initiates the requests.

User and entitlement data can be imported into Role Manager using flat files. In an environment where Sun Identity Manager is already deployed, however, (or is in the process of being deployed) Role Manager can connect to Identity Manager using SPML to import the user and entitlement data of managed resources. Role Manager can also be used to export roles and user-role membership, and send revocations back to Identity Manager.



[top](#)

## Integrating Sun Role Manager With Sun Identity Manager

This section describes how to configure Sun Role Manager and Sun Identity Manager so that the two products can be used together.

### ▼ To Configure Sun Role Manager and Sun Identity Manager to Work Together

*Before You Begin –*

- **At least version 8.1.0.7 of Sun Identity Manager and at least version 5.0.3 of Sun Role Manager are required.**
- Sun Identity Manager should be installed and configured with the Sun Identity Manager Gateway.
- In a production environment, Sun Identity Manager and Sun Role Manager should be deployed on separate application servers.
- If you are installing Sun Identity Manager on the Tomcat application server, you need to install the Metro 1.5 webservices JAR files. This step is required to ensure that the Web Services Adapter works correctly and to prevent errors when accessing the Sun Identity Manager `/debug/Gateway.jsp` page. Download the Metro 1.5 JAR files from the following URL:  
<https://metro.dev.java.net/1.5>

1. In Identity Manager, import the SPML Exchange File so that Identity Manager can receive (and respond to) SPML requests sent from Role Manager. The SPML Exchange File (`rm_idm_init.xml`) is supplied with Role Manager.  
 See [Step 1: To Import the Identity Manager SPML Exchange File](#) for details.
2. In Role Manager, create a Role Manager user that Identity Manager will use to connect to Role Manager using Web Services.  
 See [Step 2: To Create a Role Manager User That Identity Manager Will use to Connect](#) for details.

3. In Identity Manager, create an Identity Manager user that Role Manager will use to invoke SPML calls to Identity Manager. See [Step 3: To Create an Identity Manager User That Role Manager Will use to Connect](#) for details.
4. In Role Manager, designate Identity Manager as the provisioning server.  
See [Step 4: To Designate Identity Manager as the Provisioning Server](#) for details.
5. In Identity Manager, add Role Manager Web Services so that Identity Manager can send requests to (and receive responses from) Role Manager.  
See [Step 5: To Configure Identity Manager to use Role Manager Web Services](#) for details.
6. In Identity Manager, configure the User Deferred Task Scanner. This step is required so that real-time Separation of Duties (SoD) processing will work properly.  
See [Step 6: To Configure the User Deferred Task Scanner](#) for details.
7. In Identity Manager, configure the User Form so that Role Manager can authenticate over SPML.  
See [Step 7: To Configure the User Form so That Role Manager can Authenticate Over SPML](#) for details.
8. Configure Role Manager for closed loop remediation. For details, see [Understanding Closed Loop Compliance](#).


## ▼ Step 1: To Import the Identity Manager SPML Exchange File

1. Copy the `rm_idm_init.xml` file, which is located in the Role Manager `conf/spml` directory, to the Identity Manager server.
2. Log in to Sun Identity Manager.
3. Choose Configure > Import Exchange File.
4. Click Browse and navigate to the `rm_idm_init.xml` file.
5. Click Import.  
The exchange file import status is displayed on the Admin Console.
6. Restart the Identity Manager application server.

## ▼ Step 2: To Create a Role Manager User That Identity Manager Will use to Connect

1. Log in to Sun Role Manager.
2. Create a user that Identity Manager can use to connect to Role Manager using Role Manager Web Services.  
For help creating a Role Manager user, see the *Sun Role Manager 5.0.3 Business Administrator's Guide*, "Role Manager Access Control" chapter, [To Create, Update, and Delete a Role Manager User](#) task.
  - a. Assign the user the `SRMAdmin` system role.
  - b. Save the user.

## ▼ Step 3: To Create an Identity Manager User That Role Manager Will use to Connect

1. Log in to Sun Identity Manager.
2. Create a user that Role Manager can use to invoke SPML calls to Identity Manager.  
For help creating an Identity Manager user, see the *Sun Identity Manager Business Administrator's Guide*, "Administration" chapter, [To Create an Administrator](#)  task.
  - a. If you are using Oracle Waveset 8.1.1, assign the user the "Identity Analytics Admin" admin role, and skip to step c. Otherwise, in at least version 8.1.0.7 of Sun Identity Manager, assign the user the following capabilities:
    - Create User
    - Deprovision User
    - Update User
    - Unlink User
    - Unassign User
    - Rename User
    - Enable User
    - Disable User
    - View User
    - Role Administrator
  - b. Assign the user control of the `Top` organization.
  - c. Assign the user the Empty Form as its User Form.
  - d. Save the user.

## ▼ Step 4: To Designate Identity Manager as the Provisioning Server

1. Log in to Sun Role Manager.
2. Choose Administration > Configuration.
3. Click Provisioning Servers.
4. Click New Provisioning Server Connection.

The New Provisioning Server Connection wizard asks you to choose the type of provisioning server connection to create.

5. From the Type of Provisioning Server Connection drop-down menu, select Sun and click Next.
6. Complete the form:
  - **Connection Name** - Type a new connection name for Sun Identity Manager. This connection name is used during the import process instead of the host name and port.
  - **SPML URL** - Format the SPML URL as follows: `http://IdentityManagerApplicationServerName:PortNumber/idm/servlet/rpcrouter2`  
For example:  
`http://localhost:8080/idm/servlet/rpcrouter2`
  - **Username** - Type a user name that Role Manager will use to connect to Identity Manager. You should have created a special Identity Manager user account for this purpose in step 3. Do not use the `configurator` account.
  - **Password** - Type the password that Role Manager will use to connect to Identity Manager.
  - **Test Connection** - Click to test whether the connection was successfully established between Sun Identity Manager and Sun Role Manager. This will help you in troubleshooting connection issues.
  - **Role Consumer** - Select this box to export roles and role content from Role Manager to Identity Manager on a real-time basis. Sun recommends that you select this option.
  - **Role Update Schedule** - Choose to schedule when to send updates back to Identity Manager.
    - **Now** - Updates roles in Identity Manager as soon as they are updated in Role Manager.
    - **Later** - Schedules the update of roles to take place on a daily, weekly, or monthly basis, or just one time, and schedules the time and date for the update task to start.

## ▼ Step 5: To Configure Identity Manager to use Role Manager Web Services

Identity Manager needs to be configured to use Role Manager Web Services. Identity Manager uses Role Manager web service calls to both send requests to Role Manager, and receive responses. To configure Role Manager Web Services, use the Identity Manager resource wizard.

1. Log in to Sun Identity Manager.
2. Choose the Resources tab and verify that the List Resources subtab is selected.
3. Locate the Resource Type Actions drop-down list and select New Resource.  
The New Resource page opens.
4. Select the Sun Role Manager Web Services resource type from the drop-down list, and click New. (If this resource type is not listed, you need to enable it. See "Managing the Resources List" in the "Roles and Resources" chapter in the *Sun Identity Manager Business Administrator's Guide* for details.)  
The Resource Wizard Welcome Page opens.
5. Click Next to begin configuring the Role Manager Web Services resource.  
The Create Sun Role Manager Web Services Resource Wizard / Resource Parameters page opens.
6. Complete the form:
  - **Web Service Base URI** - Type the Uniform Resource Identifier (URI) for your Role Manager installation as follows:  
`http://server-name:port-number/rbacx`  
where *server-name* is the IP address or alias of the server on which Role Manager is running, and *port-number* is the port number of the application server that is listening to Role Manager calls.
  - **User** - Type the user name that Identity Manager will use to connect to Role Manager. You should have created a special Role Manager user account for this purpose in step 2. Do not use the `rbacxadmin` account.
  - **Password** - Type the password that Identity Manager will use to connect to Role Manager.
  - **Sun Role Manager Version** - Type the version number of Role Manager that Identity Manager is connecting to.
  - **Is SRM Configured** - Type `true` to enable Identity Manager to use Role Manager Web Services.
  - **Test Configuration** - Click to test the connection to Role Manager Web Services.

**Note** - Upon completing the wizard, additional form fields are unlocked. These fields include the following:

- **Process Check Policy Results Rule** - Value should be Sun Role Manager:Process Policy Result
- **Check Policy Compliance Violation Form** - Value should be Sun Role Manager Compliance Violation Form
- **Check Policy Status Rule** - Value should be Sun Role Manager:Risk Analysis Status
- **Compliance Violation Owners Rule** - Value should be Sun Role Manager:Compliance Violation Owners

7. Click Next.

The Create Sun Role Manager Web Services Resource Wizard / Account Attributes page opens.

8. Verify that the account attribute mappings on this page are correct and click Next.

The Create Sun Role Manager Web Services Resource Wizard / Identity Template page opens.

9. Verify that the attribute value in the Identity Template box is correct and click Save.

## ▼ Step 6: To Configure the User Deferred Task Scanner

The User Deferred Task Scanner in Identity Manager needs to be configured for a delay of one minute so that SoD processing will work properly. The scanner picks up SoD information after it has been retrieved from Role Manager using Role Manager web services.

1. Log in to Sun Identity Manager.
2. Choose Server Tasks > Manage Schedule.
3. Click User Deferred Task Scanner to edit the task.  
The Edit Task Schedule page opens.
4. Change the value in the Repeat Every box to a value of 1 Minutes.
5. Click Save.

## ▼ Step 7: To Configure the User Form so That Role Manager can Authenticate Over SPML

Within Identity Manger, the User Form of the user that Role Manager authenticates as over SPML needs to be set to "Empty Form."

1. Log in to Sun Identity Manager.
2. Choose the Accounts tab and verify that the List Accounts subtab is selected.
3. Click the user that you created in [step 3](#).  
The Edit User page opens.
4. Click the Security tab.
5. From the User Form drop-down box, select Empty Form.
6. Click Save.

Role Manager and Identity Manager are now configured to work together. To configure closed loop remediation, see [Understanding Closed Loop Compliance](#).

[top](#)

---

# Populating Sun Role Manager With User Information From Sun Identity Manager

Refer to the use cases in this section if you have user entitlements in Sun Identity Manager that you want to use to populate the Sun Role Manager Identity Warehouse. Importing users and roles from Identity Manager into Role Manager should be a one-time event that takes place when first configuring the systems.

## Use Case 1: Importing Global Users From Identity Manager Into Role Manager

Identity Manager saves information about users who are auto-provisioned. These users are imported into Role Manager as global

users before their accounts are pulled in.

## ▼ To Import Users From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Users.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by entering the Name and Description of the Job.
7. Choose one of the following tasks:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish.  
The import users job runs on the scheduled date and time.
9. Verify that the users are imported into Role Manager from Identity Manager by accessing the Users View in Role Manager (choose Identity Warehouse > User).

[top](#)

## Use Case 2: Importing Resource Metadata From Identity Manager Into Role Manager

A *resource type* in Identity Manager is a type of target system, whereas a *resource* is an instance of a resource type. For example, consider the case of four different Windows NT systems hosting four different sets of users. In this scenario, 'Windows NT' is the resource type, whereas the four individual system names are resources of type 'Windows NT.'

In the Role Manager integration with Identity Manager, information on resource metadata can be imported from Identity Manager to Role Manager. This eliminates the need to manually recreate resource metadata in Role Manager.

## ▼ To Import Resource Metadata From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Resource Metadata.  
The next page will prompt you to choose the resource from the list of available resources for which metadata on attributes needs to be imported.
5. Select the specific resource type.
6. Under Data Selection Source, select the appropriate Connection Name and click Next.
7. Complete the form by entering the Name and Description of the Job.
8. Choose one of the following:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
9. Click Finish to generate the Import Job.  
The import resource metadata job runs on the scheduled date and time.
10. Verify that the resource metadata was properly imported into Role Manager by accessing the Role Manager Resources Types tab (choose Configuration > Resources Types).

**Note:** Seven resource types in Sun Identity Manager are treated differently by Sun Role Manager. They are the following:

1. Simulated
2. Scripted JDBC
3. Database Table
4. External
5. Scripted Gateway



6. Scripted Host
7. Shell Script

Each resource within the above resource type is created as a resource\_type within Sun Role Manager. The naming convention is "ResourceName\_\_ResourceTypeName". This is because each resource is likely to have its own resource type metadata rather than a common metadata format.

## Use Case 3: Importing Resources From Identity Manager Into Role Manager

With out-of-the-box integration capabilities, Role Manager can import resources from Identity Manager to Role Manager. This eliminates the need to manually create the resources in Role Manager.

### ▼ To Import Resources From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Resources.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish to generate the import job.  
The import resources job runs on the scheduled date and time.
9. Verify that the resources are imported into Role Manager from Identity Manager by accessing the Role Manager Resources tab (choose Identity Warehouse > Resources).

## Use Case 4: Importing User Accounts From Identity Manager Into Role Manager

After global users are imported, you can import accounts (user entitlements) into Role Manager for different resource types. Before importing user accounts, make sure that the resource types and attributes are correctly configured in Role Manager. For more information, see [Resource Types Configuration](#) in the *Sun Role Manager 5.0.3 Business Administrator's Guide*, Role Manager Configuration chapter.

### ▼ To Import Accounts From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Accounts, and then click Next.
5. From the list of available resources for which user accounts can be imported, select the resource and the specific resource type.
6. Under Data Selection Source, select the appropriate Connection Name and click Next.
7. Complete the form by entering the Name and Description of the Job.
8. Choose one of the following:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
9. Click Finish to create the Import Job.  
The job runs on the scheduled date and time.
10. Verify that the accounts imported into Role Manager match the corresponding resource type accounts in Identity Manager.

## Use Case 5: Importing Roles From Identity Manager Into Role Manager

**Note** - This should be done only as a one time effort for initial Roles population. It is recommended that SRM kept as the Authoritative Source for roles and the toles would be overwritten if they are imported from IDM on an ongoing basis.

## ▼ To Import Role From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Roles.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish to generate the import job.  
The import resources job runs on the scheduled date and time.
9. Verify that the roles are imported into Role Manager from Identity Manager by accessing the Role Manager Roles tab (choose Identity Warehouse > Resources).

[top](#)

---

# Populating Sun Identity Manager With Roles Information From Sun Role Manager

See the use cases in this section if you have user accounts in Role Manager that you want to use to populate the Identity Manager repository.

**Note** - Exporting roles from Role Manager to Identity Manager should be a one-time event that takes place during configuration. To export roles to Identity Manager, be sure that the Role Consumer box is selected in the Sun Provisioning Server settings.

Role Manager can create roles based on either existing entitlements or business attributes (client requirements). Policy formation and role-policy association can be performed during role creation. In addition, the role-user association can also be established.

Identity Manager does not have the concept of policies. The roles in Role Manager are mapped to Business Roles in Identity Manager, whereas the policies in Role Manager are mapped to IT Roles in Identity Manager. As policies are directly assigned to resources in Role Manager, similarly IT Roles are directly assigned to resources in Identity Manager. Thus, the one-to-many relationship between role and policies is carried forward from Role Manager to Identity Manager by way of the one-to-many relationship between Business Roles and IT Roles. This allows for more efficient grouping of entitlements and easier management of user access. Thus, along with roles, policies also need to be exported from Role Manager to Identity Manager.

## Use Case 1: Exporting Roles From Role Manager to Identity Manager

**Note** - Roles in Role Manager correspond to Business Roles in Identity Manager.

### ▼ To Export Roles to Identity Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new export job, choose Schedule Job > Export> Export Roles.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by entering the Name and Description of the Job.
7. Choose one of the following:
  - To run the job immediately, select the Run the Job Now option.

- To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish to create the Import Job.  
The job runs on the scheduled date and time.
  9. Verify that the roles were properly exported to Identity Manager by opening Identity Manager and clicking the 'Business Role' Roles tab.

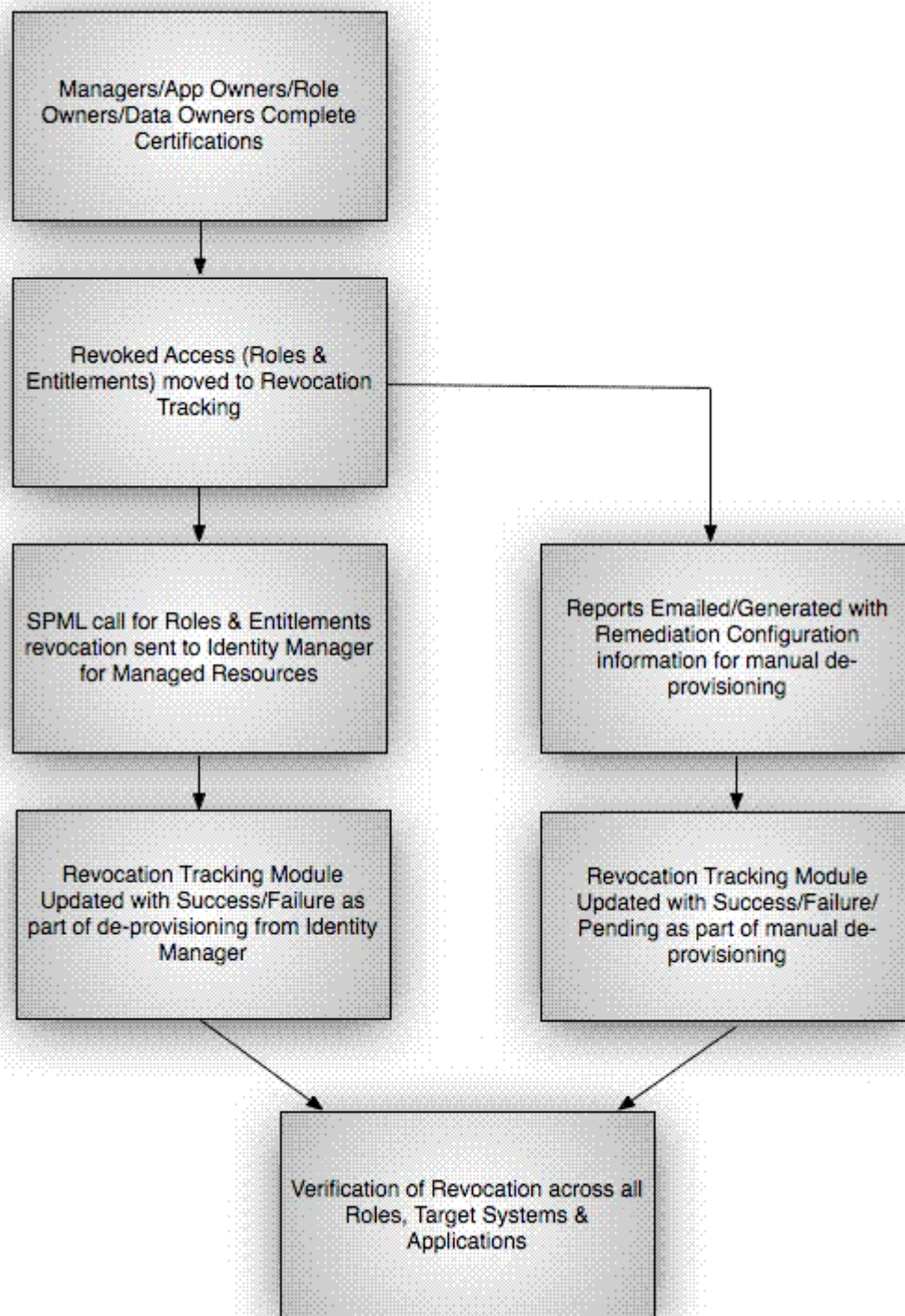
**Note:** Policies (roles content) are exported as part of roles export.

[top](#)

## Understanding Closed Loop Compliance

With the integration of Role Manager and Identity Manager, it is possible to directly revoke roles and entitlements from Identity Manager if the results of the certification process require it. This integration eliminates the need for manual de-provisioning of access for managed resources. In addition, the manual process of revoking roles and entitlements by leveraging the information stored in the remediation configuration module is also retained. This takes into account nonmanaged applications.

The following closed loop remediation diagram illustrates this process.



## ▼ To Configure Resources in Role Manager for Remediation

Every resource type in Role Manager can be separately configured for automatic or manual remediation.

1. Log in to Role Manager.
2. Choose Identity Warehouse> Resources.
3. Click the resource for which remediation action needs to be configured, and go to the Remediation tab.
4. Select the Select Provisioning Mode check box.

5. Choose the mode of provisioning desired for the particular resource.
  - **Auto** - Automatically send role/entitlement updates linked with this resource to Identity Manager. Select the appropriate connection name of the provisioning server and save the changes.
  - **Manual** - Use the manual steps for revocation of roles and entitlements using a text editor. List the steps to be followed for non-managed system remediation and save the changes.

## ▼ To Configure Certifications in Role Manager for Remediation

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Identity Certification.
4. Expand the Revoke and Remediation section and, under the Remediation section, choose one of the following options:
  - **Display Remediation Instructions** - Select to display instructions about how to perform manual remediation of nonmanaged resources.
  - **Perform Closed Loop Remediation on** - Select to specify that the remediation be completed by either the Certification End Date or the Certification Completion Date.

[top](#)

---

## Role Manager Web Services

With an out-of-the-box integration, web services from both Identity Manager and Role Manager can be used as needed. For information about Role Manager web services, see the [Sun Role Manager 5.0.3 API Guide](#).

[top](#)

---

## Troubleshooting

The information in this section briefly describes how to approach troubleshooting a Role Manager and Identity Manager integration.

### System Logs

Application logs are generated and stored in the application deployment folder in `rbacx.log`. The log captures various details such as import/export information, ETL processing, and any exceptions that can arise while running the application. There are different levels of logging in the `rbacx.log` file, and these can be adjusted and modified as needed. The properties file that is used to alter the logging level is found under the `$RBACX_HOME\WEB-INF` folder, and the file name is `log4j.properties`.

There are three levels of logging that are commonly used by the system integrators: `WARN`, `INFO`, and `DEBUG`.

To change logging levels, open `log4j.properties` in a text editor and modify the line under the `#Role Manager IAM logging` section as follows:

```
log4j.logger.com.vaau.Role Manager.iam=DEBUG
```

Other parameters to be aware of are Security logging and IAM logging. These logs report Security and entitlement data exceptions.

For more information about logging, see the [Sun Role Manager 5.0.3 System Administrator's Guide](#).

[top](#)

## Integrating With Oracle Identity Manager

# Overview

Sun™ Role Manager software (Role Manager) and Oracle Identity Manager (OIM) software work together seamlessly when integrated using the Thor-API connection mechanism. When integrated, Oracle Identity Manager serves as the automated provisioning and identity synchronization solution, while Role Manager defines the Role-based Access Control (RBAC) framework, the attestation process, and the approach to Segregation of Duties (SoD) policy enforcement. Rather than assigning individual access entitlements, the RBAC framework allows organizations to assign and unassign roles as a means of controlling user access on various applications.

In a fully-integrated scenario, provisioning and role management works in the following manner:

- OIM is the authoritative source for users, accounts, and entitlements. Any update made to the users or their corresponding accounts is done in OIM.
- Role Manager is the authoritative source for role management and role membership. Role Manager is also the authoritative source for policy entitlement definitions. (Roles in Role Manager correspond to "groups" in OIM, and policies in Role Manager correspond to "access policies" in OIM.)
- All roles are defined and created in Role Manager. All entitlements for policies and role-to-user relationships are managed from Role Manager.
- Roles managed by Role Manager become read-only in OIM.

**Note** - Provisioning attribute definitions for Access Policies, which are required to create accounts, is managed in much the same way as the current Oracle Role Manager(ORM) - OIM integration (by OIM or external process).

## Understanding Terminology in Role Manager and Oracle Identity Manager

The following table maps Sun Role Manager terminology to Oracle Identity Manager terminology.

Role Manager Terminology	Oracle Identity Manager Terminology
Resource Type	Resource Type
Resource Type Attributes (NameSpace Attributes)	Provisioning Attributes and Entitlements
Resource	IT Resource
Global Users	Xellerate End Users
Roles	Group
Policies	Access Policies

[top](#)

---

## Integrating Sun Role Manager with Oracle Identity Manager

This section describes how to configure Sun Role Manager and Oracle Identity Manager so that the two products can be used together.

### ▼ To Configure Sun Role Manager and Oracle Identity Manager to Work Together

**Before You Begin** -

- **At least version 9.1.02 BP5 of Oracle Identity Manager and at least version 5.0.3 of Sun Role Manager are required.**
  - Oracle Identity Manager should be installed and configured.
1. In Role Manager add Oracle Identity Manager as a provisioning server option. ("Sun Identity Manager" and "File" are the default options.)  
See [Step 1: To enable Oracle Identity Manager as a Provisioning Server Option](#).
  2. In Role Manager, designate Oracle Identity Manager as the provisioning server. Establish a connection by entering authentication details.  
See [Step 2: To ensure That the Required jar Files are Present](#).
  3. In Role Manager, configure `iam-context.xml` to integrate with OIM.  
See [Step 3: To designate Oracle Identity Manager as the Provisioning Server](#).
  4. To enable real time updates from Role Manager to Oracle Identity Manager

## ▼ Step 1: To Enable Oracle Identity Manager as a Provisioning Server Option

In the Role Manager user interface, the Administration > Configuration > Provisioning Servers tab displays "file" and "sun" as the available options. To display Oracle Identity Manager as a supported provisioning server, edit `iam-context.xml` in the `RBACX_Home/WEB-INF` folder as follows.

Uncomment the oracle key entry in the `iamSolutions` property map lines in `iam-context.xml`:

```
<bean id="rbacxIAMService" parent="baseTransactionProxy">
  <property name="target">
    <bean class="com.vaau.rbacx.iam.service.impl.RbacxIAMServiceImpl" parent="baseService"
      <property name="iamSolutions">
        <map>
          <entry key="sun">
            <ref local="waveset"/>
          </entry>
          <!--entry key="ca">
            <ref local="eTrust"/>
          </entry-->
          <!--entry key="ibm">
            <ref local="tim"/>
          </entry-->
          <entry key="oracle">
            <ref local="oim"/>
          </entry>
          <entry key="file">
            <ref local="file"/>
          </entry>
        </map>
      </property>
    </bean>
  </property>
</bean>
```

and the second change to this file is to uncomment the bean definition:

```

<bean id="oim" class="com.vaau.rbacx.iam.oracle.OIMIAMSolution" parent="abstractIAMSolution">

    <property name="metadataManager" ref="metadataManager"/>

    <property name = "namespaceMap">
        <map>
            <!-- This mapping fetches the attributes from
                 the appropriate object form ( AD User). This
                 mapping clarifies that, for the "AD Server"
                 resource type, attributes are imported from
                 the "AD User" Object form in OIM -->
            <entry key = "AD Server">
                <value>AD User</value>
            </entry>
        </map>
    </property>
    <property name="resourceFieldMap">
        <map>
            <!-- This mapping identifies the field that is the
                 ITResourceLookupField for each resource type.
                 (Oracle Identity Manager "IT resources" map to
                 resources in Sun Role Manager.) From the mapping
                 for the "AD Server" resource type field, we
                 define that the "UD_ADUSER_AD" column field
                 corresponds to the ITResource Entry. -->
            <entry key="AD Server">
                <value>UD_ADUSER_AD</value>
            </entry>
        </map>
    </property>

    <property name="accountIdentifierMap">
        <map>
            <entry key="AD Server">
                <value>UD_ADUSER_UID</value>
            </entry>
        </map>
    </property>
    <property name = "secPolicyMap">
        <map>
            <entry key = "RACF Account">
                <value>Server,Group</value>
            </entry>
        </map>
    </property>
    <property name="maxStaleDays">
        <value>${com.vaau.rbacx.iam.oracle.maxStaleDays}</value>
    </property>
    <property name = "excludeFlag" >
        <value>${com.vaau.rbacx.iam.oracle.excludeFlag}</value>
    </property>

    <property name = 'roleDao'>
        <ref bean="roleDao"/>
    </property>
    <property name = "policyManager">
        <ref bean = "policyManager"/>
    </property>
    <property name="userProperties">
        <map>
            <entry key = "userName">
                <value>Users.User ID</value>
            </entry>
            <entry key = "firstName">

```



## ▼ Step 2: To Ensure That the Required .jar Files are Present

Ensure that the following `$XL_HOME/xellerate/lib/.jar` files are present in the `$RBACX_HOME/WEB-INF/lib` folder:

- `wlXLSecurityProviders.jar`
- `xlAPI.jar`
- `xlAuthentication.jar`
- `xlCache.jar`
- `xlCrypto.jar`
- `xlDataObjectBeans.jar`
- `xlLogger.jar`
- `xlUtils.xls`
- `xLVO.jar`

### IMPORTANT

For Jboss server copy `* jbossall-client.jar`

For WebLogic server copy `* oim_design_console\xlclient\ext\wlfullclient.jar`

## ▼ Step 3: To Designate Oracle Identity Manager as the Provisioning Server

1. Log in to Sun Role Manager.
2. Choose Administration > Configuration.
3. Click Provisioning Servers.
4. Click New Provisioning Server Connection.  
The New Provisioning Server Connection wizard asks you to choose the type of provisioning server connection that you want to create.
5. From the Type of Provisioning Server Connection drop-down menu, select Oracle and click Next.
6. Complete the form:
  - **Server Name** - Type the connection object name.
  - **Xellerate Home** - Type the path to the `config` file in OIM. (example: `C:\oracle\xellerate`)
  - **Login Config** - Type the path to the authentication configuration ( `auth.config` ) file. (example: `C:\oracle\xellerate\config\auth.conf`)
  - **Provider URL** - Type the provider URL. The format for this field is as follows:
    - **WebLogic** - `t3://host:7001`
    - **JBoss** - `jnp://host:1099` (The default port number in a clustered environment is 1100.)
    - **WebSphere** - `corbaloc:iiop:host:2809`
  - **Initial Context Factory** - Enter the name of the environment property for specifying the initial context factory. The default values are as follows:
    - **WebLogic** - `weblogic.jndi.WLInitialContextFactory`
    - **JBoss** - `org.jnp.interfaces.NamingContextFactory`
    - **WebSphere** - `com.ibm.websphere.naming.WsnInitialContextFactory`
  - **User Name** - Enter the OIM user name. (example: `xelsysadm`)
  - **Password** - Enter the OIM password.

## ▼ Step 4: To Enable Real-Time Updates from Role Manager to Oracle Identity Manager

To send real-time changes from Role Manager to Oracle Identity Manager, change the configuration files related to workflows.

For example, the following code snippet has to be enabled in `role-creation-workflow.xml` during the "Finish" step ( step 6):

```
<\!--<function name="exportIAMRoleFunction" type="spring">
  <arg name="bean.name">exportIAMRoleFunction</arg>
  <arg name="iamConnectionName"/>
</function-->
```

This becomes the following:

```
<function name="exportIAMRoleFunction" type="spring">
  <arg name="bean.name">exportIAMRoleFunction</arg>
  <arg name="iamConnectionName">OIMConnectionObjectName</arg>
</function>
```

Note: The OIM ConnectionObjectName is the name of the connection object you define in Step 2. Similar changes have to be made for all role related workflows.

( role-modification-workflow.xml, role-user-membership-workflow.xml, role-user-membership-activation-workflow.xml )

## Populating Sun Role Manager With User Information From Oracle Identity Manager

Refer to the use cases in this section if you have user entitlements in Oracle Identity Manager that you want to use to populate the Sun Role Manager Identity Warehouse. Importing users and roles from Identity Manager into Role Manager should be a one-time event that takes place when first configuring the systems.

### Use Case 1: Importing Global Users From Oracle Identity Manager Into Role Manager

The users existing in Oracle Identity Manager (Xellerate End Users) are imported as global users in Role Manager on a scheduled basis. The attributes of the users in OIM are mapped to global user properties in Role Manager by way of a map. Extended attributes in OIM can be imported as custom properties in Role Manager.

The following table contains the default mapping of user attributes between Role Manager and Oracle Identity Manager.

Role Manager User Attribute Name	Oracle Identity Manager (OIM) User Attribute Name
username	Users.UserID
firstname	Users.First Name
lastname	Users.Last Name
middlename	Users.Middle Name
manager	Users.Manager Login
primaryemail	Users.Email
startdate	Users.Start Date
enddate	Users.End Date
createdate	Users.Provisioned Date

### ▼ To Import Users From Oracle Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Users.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by entering the Name and Description of the Job.
7. Choose one of the following tasks:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish.  
The import users job runs on the scheduled date and time.
9. Verify that the users are imported into Role Manager from Identity Manager by accessing the Users View in Role Manager (choose Identity Warehouse > User).

[top](#)

## Use Case 2: Importing Resource Metadata From Oracle Identity Manager Into Role Manager

In the Role Manager integration with Identity Manager, information on resource metadata can be imported from Identity Manager to Role Manager. This eliminates the need to manually recreate resource metadata in Role Manager.

### ▼ To Import Resource Metadata From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Resource Metadata.  
The next page will prompt you to choose the resource from the list of available resources for which metadata on attributes needs to be imported.
5. Select the specific resource type.
6. Under Data Selection Source, select the appropriate Connection Name and click Next.
7. Complete the form by entering the Name and Description of the Job.
8. Choose one of the following:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
9. Click Finish to generate the Import Job.  
The import resource metadata job runs on the scheduled date and time.
10. Verify that the resource metadata was properly imported into Role Manager by accessing the Role Manager Resources Types tab (choose Configuration > Resources Types).

## Use Case 3: Importing Resources From Identity Manager Into Role Manager

With out-of-the-box integration capabilities, Role Manager can import resources from Oracle Identity Manager to Role Manager. This eliminates the need to manually create the resources in Role Manager. ITRResource in OIM corresponds to a resource in Role Manager.

### ▼ To Import Resources From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Resources.

5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish to generate the import job.  
The import resources job runs on the scheduled date and time.
9. Verify that the resources are imported into Role Manager from Identity Manager by accessing the Role Manager Resources tab (choose Identity Warehouse > Resources).

## Use Case 4: Importing Roles From Identity Manager Into Role Manager

Groups defined in OIM are imported as Roles within Role Manager. This import also pulls in the relationship between the Group to Access Policy within OIM as Roles-Policy relationship within Role Manager. This requires a successful policy import.

In addition, this step also imports the group-user relationship from OIM and recreates it as a role-user relationship in Role Manager. To establish role-user relationship, ensure that users are imported.

### ▼ To Import Role From Identity Manager Into Role Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new import job, choose Schedule Job > Import > Import Roles.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish to generate the import job.  
The import resources job runs on the scheduled date and time.
9. Verify that the roles are imported into Role Manager from Identity Manager by accessing the Role Manager Roles tab (choose Identity Warehouse > Resources).

[top](#)

---

## Populating Oracle Identity Manager With Roles Information From Sun Role Manager

See the use cases in this section if you have user accounts in Role Manager that you want to use to populate the Identity Manager repository.

Roles defined in Role Manager can be exported to OIM on a scheduled basis, once role definition/management is completed. This use case will perform the following exports into OIM:

1. Export Role Manager roles to OIM groups.
2. Export the Role Manager policy definition and its entitlements from Role Manager into OIM Access Policies. If the policy does not exist it would create the new policy as Access Policies within OIM.
3. Export the Role Manager Policy-Resource relationship as OIM Access Policy- ITResource relationship.
4. Export the Role Manager Role-Policy relationship as OIM Group-Access Policy relationship.
5. Export the Role Manager Role-User relationship to OIM Group-User relationship.

Note : During initial integration this is done on a scheduled basis. A recommended long-term solution is to update OIM as definitions are changed in Role Manager on a real-time basis.

# Use Case 1: Exporting Roles From Role Manager to Identity Manager

**Note** - Roles in Role Manager correspond to Groups in Identity Manager.

## ▼ To Export Roles to Identity Manager

1. Log in to Role Manager.
2. Choose Administration > Configuration.
3. Click Import/Export.
4. To start a new export job, choose Schedule Job > Export> Export Roles.
5. Under Data Selection Source, select the appropriate Connection Name and click Next.
6. Complete the form by entering the Name and Description of the Job.
7. Choose one of the following:
  - To run the job immediately, select the Run the Job Now option.
  - To schedule the job for later, clear the Run the Job Now option and enter the details of the scheduled job.
8. Click Finish to create the Import Job.  
The job runs on the scheduled date and time.
9. Verify that the roles were properly exported to Identity Manager by opening Identity Manager and clicking the User Group --> Manage link on the left pane.

[top](#)

# Integrating With Other Provisioning Servers

In addition to [Sun Identity Manager](#) and [Oracle Identity Manager](#), Sun Role Manager has the ability to integrate with the following provisioning servers:

- IBM Tivoli Identity Manager
- CA eTrust Identity Access Management

In the user interface, the Administration > Configuration > Provisioning Servers tab displays 'file' and 'sun' as the available options. To display other supported provisioning servers, edit `iam-context.xml` in the `RBACX_Home/WEB-INF` folder.

## ▼ To Set Up IBM Tivoli Identity Manager

Uncomment the following lines in `iam-context.xml`

```
<!--entry key="ibm">
<ref local="tim"/>
</entry-->
<!--bean id="tim" class="com.vaau.rbacx.iam.ibm.TIMIAMSolution"
parent="abstractIAMSolution"/-->
```

## ▼ To Set Up CA eTrust Identity Access Management

Uncomment the following lines in `iam-context.xml`

```
<!--entry key="ca">
<ref local="eTrust" />
</entry-->
<!--bean id="eTrust" class="com.vaau.rbacx.iam.ca.ETrustIAMSolution"
parent="abstractIAMSolution">
<property name="extensions">
<value>${com.ca.iam.extensions}</value>
</property>
    <property name="userSearchFilter">
        <value>*</value>
    </property>
</bean-->
```

[top](#)

## Authenticating With LDAP

The page Integrating With LDAP does not exist.

## Integrating With Intellitactics Security Manager

Intellitactics Security Manager (ISM) is a Security and Information Event Management (SIEM) solution that enables real-time event monitoring and reporting, and makes it possible to quickly investigate alerts and incidents. By integrating Sun Role Manager with Intellitactics, a certifier can view important user activity information during the certification process.

The inclusion of event and alert information in the certification process allows the certifier to make better, more informed decisions about whether a user should have certain system or application privileges. This information provides Role Manager with a view of *what the user did* (actions), which complements and expands on the default Role Manager view of *what the user is allowed to do* (permissions). This correlation is critical for many compliance standards, including Sarbanes-Oxley (SOX).

## Understanding the Intellitactics Data Structure and Information Flow

Two components of Intellitactics are captured in Role Manager: events and alerts.

### Understanding Events

Event information is collected directly from monitored devices or resources. Intellitactics' out-of-the-box behavior is to perform minimal aggregation. For example, if an identical event occurs 850 times in 2 seconds, ISM will record one event with a counter value of 850.

Because this method can still generate too many events for a certifier to use to get an accurate picture of user activity, an additional optimization has been included that summarizes events into hourly and daily tables.

Role Manager captures only the daily tables, as that is the optimum granularity that can be achieved in the current certification process.

The following tables are used by Role Manager.

sdw.event_daily_summary	Contains the summary of events
sdw.event_id	Contains the event classification
sdw.supported_devices	Contains a list of devices that ISM supports

**Note** - Queries on the `event_daily_summary` table must include a `summarization_id = 60` statement in the `WHERE` clause.

## Understanding Alerts

Alert information is generated by way of ISM's standard, predefined processes. During processing, events are collected from participating systems by way of Intellitactic's data collectors. When predefined thresholds are met, ISM raises alerts. This means that appropriate entries will be entered into the alert-related tables.

The relevant tables are as follows:

<code>sdw.alerts</code>	Contains basic alert information
<code>sdw.alert_events</code>	Contains additional information on the events that triggered the alert
<code>sdw.nsmaudit_fact</code>	Contains the status of the alert

The 10 highest risk alerts are displayed to the user during the certification process. (Risk level is determined by ISM.)

**Note** - If the alert status field is empty, it signifies that the alert is open.

[top](#)

---

## ▼ To Integrate Intellitactics With Role Manager

### **Before You Begin** -

Intellitactics Security Manager (ISM) should be installed according to the standard deployment instructions distributed with the software.

You will have to make the following modifications for integration with Role Manager.

1. Copy the `jdbc.properties` file to the `$RBACX_HOME/conf` folder.
2. Add the `siem.properties` file to the `$RBACX_HOME/conf` folder.

The file should look like this:

```
siem.jdbc.username=<user_id>
siem.jdbc.password=<password>
siem.jdbc.url=jdbc:mysql://<ip>:<port>/sdw
siem.jdbc.driverClassName=com.mysql.jdbc.Driver
```

This is an example of a completed file:

```
# SIEM connection properties
siem.jdbc.username=siemuser
siem.jdbc.password=siemuserpassword
siem.jdbc.url=jdbc:mysql://127.0.0.1:3306/sdw
siem.jdbc.driverClassName=com.mysql.jdbc.Driver
```

3. Modify the `siem-sql-map-config.xml` file as follows:

- Comment out `<ref bean="dummyDataSource"/>` by changing the line to read as follows:  
`<!-- ref bean="dummyDataSource" / - -->`.
- Uncomment `<!-- ref bean="siemDataSourceTarget"/-->` by changing the line to read as follows:  
`<ref bean="siemDataSourceTarget"/>`.

For example:

```
<bean name="swappableDataSource
class="org.springframework.aop.target.HotSwappableTargetSource">
  <constructor-arg>
    <!--ref bean="dummyDataSource"/-->
    <ref bean="siemDataSourceTarget"/>
  </constructor-arg>
</bean>
```

4. Make the following changes in the user interface:

- a. Log in to Role Manager.
- b. Choose Identity Warehouse > Resources.
- c. Click the appropriate resource.
- d. Add the device ID in the comments field.

These values are maintained in `com.vaau.rbacx.siem.SiemConstants`.

Usually, the values are as follows:

AD - 136; AS400 - 500; RACF - 424; Oracle - 4; Solaris - 30.

5. Click Save.

**Note** - The previous examples are for a MySQL™ database installation.

## ▼ To View User Activity Information During the Certification Process

To enable certifiers to see user activity information during the user entitlement certification process, do the following:

1. Log in to Role Manager
2. Choose Administration > Configuration.
3. Click Identity Certification.
4. In the General section, click and open the User Entitlement option.
5. Select the box next to View User Activity Information.
6. Click Save.

The certifier can now view the user activity information during the certification process. For instructions on how to complete a user entitlement certification, see [To Complete a User Entitlement Certification](#).

[top](#)

# Configuring Role Manager For Web Access Control

This chapter describes how to authenticate with Sun Role Manager using Web Access Components.

## Overview

Sun Role Manager can be integrated with Web Access Control solutions such as Sun Access Manager, CA's eTrust SiteMinder, Novell's ICHAIN, and so on. This enables Role Manager to follow enterprise standards for web application security.

## Configuring Role Manager For Web Access Control

The following two configuration changes need to be made in Role Manager:

1. Setting up the correct HTTP header variable name in `security-context.xml`
2. Setting up the logout URL



## To Set Up the http Reader

Web Access Control Solutions send user information as part of the http header variable. This header variable, which is the user name, holds a unique identity for the user being authenticated. This user name should be the same as the Role Manager user.

As shown in the following snippet from the `security-context.xml` configuration file (under the `WEB-INF` folder in Role Manager), Role Manager is configured to use the value of the "sm-user" http header variable to authorize a user. Change the property of "`preAuthEnabled`" to "`true`" and also change "`sm-user`" for "`preAuthUsernameHeaderKey`" and "`preAuthPasswordHeaderKey`" to the header variable sent by the Web Access Control Solution.

```
<bean id="preAuthAwareAuthenticationProcessingFilter"
      class="com.vaau.commons.springframework.security.filter.PreAuthAwareAuthenticationProce
<property name="authenticationManager">
  <ref bean="authenticationManager"/>
</property>
<property name="authenticationFailureUrl" value="/welcome.action?login_error=true"/>
<property name="defaultTargetUrl" value="/secure/checkExpiredCredentials.action"/>
<property name="filterProcessesUrl" value="/j_acegi_security_check"/>
<property name="formUsernameParameterKey" value="j_username"/>
<property name="formPasswordParameterKey" value="j_password"/>
<property name="preAuthEnabled" value="true"/>
<property name="preAuthUsernameHeaderKey" value="sm-user"/>
<property name="preAuthPasswordHeaderKey" value="sm-user"/>
<!--SM_USER -->
<property name="exceptionMappings">
  <props>
    <prop key="org.springframework.security.BadCredentialsException">/welcome.action?
    <prop key="org.springframework.security.CredentialsExpiredException">/passwordExp
  </props>
</property>
</bean>
```

## To Set Up the Logout URL

For a user to completely log out from the session, the Role Manager default logout URL needs to be modified with the logout URL for the Web Access Control Solution.

To configure the logout URL in Role Manager, change the following entry in the `header.jspf` file under the `WEB-INF/jspf` folder.

Current information in line 111-122 in the `header.jspf` file:

```
<tr>
  <td height="22">
    <div align="center" style="font-size:10px;">
      <a href="<%=ctx%>/secure/home/home.action" class="hoverUnderline"
      style="color:#000000">Home</a>
      <a href="<%=ctx%>/logout.action" class="hoverUnderline"
      style="color:#000000">Logout</a>
      <a href="<%=ctx%>/docs/userguide/index.html" target="_blank"
      class="hoverUnderline" style="color:#000000">Help</a>
    </div>
  </td>
</tr>
```

Line 111-122 in the `header.jspf` file after the modification:

```
<tr>
  <td height="22">
    <div align="center" style="font-size:10px;">
  <a href="<%=ctx%>/secure/home/home.action" class="hoverUnderline"
    style="color:#000000">Home</a> |
    <a href="www.vaau.com/logout.jsp" class="hoverUnderline"
    style="color:#000000">Logout</a> |
    <a href="<%=ctx%>/docs/userguide/index.html" target="_blank"
class="hoverUnderline" style="color:#000000">Help</a>
    </div>
  </td>
</tr>
```

## To Access Sun Role Manager When Using Web Access Control

End-users should use the following URL to access Sun Role Manager:

`http://SrmHost:Port/rbacx/j_acegi_security_check`

**Note** - If the SSO solution allows for setting up a specific redirect URL for each application, then the SSO solution should be configured to redirect to the URL provided above.

Because this URL is protected by the SSO solution, the end-user is redirected to the SSO login screen, and, once successfully authenticated, re-directed to the URL provided. At this point, Sun Role Manager can verify the HTTP header and allow the end-user to access the application.

[top](#)

## Customizing The Role Manager User Interface

This chapter describes how to customize the Sun Role Manager user interface (UI).

Role Manager features an AJAX-rich, Web 2.0 user interface for an enhanced, user-friendly experience. Menu items and logos can be customized so that your organization can adhere to its internal style guidelines.

### Before You Begin

To customize the user interface, you need the following access privileges:

- Access to the Role Manager application server with rights to modify and add files to the Role Manager deployed `war` folder
- Administrative credentials to log in to the Role Manager application

[top](#)

---

## Configuring Logos

The Role Manager home screen displays the default logo.

If Role Manager is hosted on the Apache Tomcat application server, the directory where the `.war` file is expanded is usually set to the following location:

## On UNIX

`/usr/local/Vaau/rbacx-4.0/tomcat55/webapps/rbacx/`

## On Windows

`C:\Program Files\Vaau\RBACx2008\tomcat55\webapps\rbacx`

This path is referred to as `$RBACX_WAR` in this chapter.

**Note** - If you are using an application server other than Tomcat, contact a system administrator to determine the location of the deployed Role Manager WAR file.

## ▼ To Configure a Custom Logo

1. Open the `$RBACX_WAR/images` directory and replace the `logo.gif` file with your company logo. Ensure that the company logo follows the same naming convention, which is `logo.gif`.
2. Open Role Manager to view the new logo. The new logo is displayed throughout the application.
3. If the new logo is not displayed immediately, restart the application server.

[top](#)

---

## Configuring Labels

All labels in Role Manager can be modified or renamed as desired.

To make changes to labels, it is important to understand the structure of two files: `rbacxmessages.properties` and `rbacxaudit-messages.properties`. These two files contain the dynamic links to configure labels for the Role Manager user interface.

These files are located in `$RBACX_WAR/WEB-INF/classes`.

- The `rbacxmessages.properties` file contains labels that are separated by modules such as Identity Warehouse, Role Management, Identity Certification, and so on.
- The `rbacxaudit-messages.properties` file allows modifications to labels only within the Identity Audit module.

The following procedures describe how to modify the labels of various modules and menu items.

## ▼ To Modify Menu Labels

1. Open the `rbacxmessages.properties` file located in `$RBACX_WAR/WEB-INF/classes`.
2. Scroll down to the `# Menu` section of the file.
3. As needed, modify the existing menu definitions, which are located to the right of the `'='` sign, and save the file.
4. Restart the Role Manager application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```

# Menus
menu.welcome=<span>Welcome</span>
menu.register=Register
menu.info=My info
menu.administration=<span Title='Administration'>Administration
  </span>
menu.monitoring=Monitoring
menu.logout=Log out
menu.tools=Tools
menu.reports=Reports
menu.dashboard=<span Title='My Reports'> My Reports</span>
menu.security=Security
menu.help=Help
menu.certifications=<span Title='Identity Certification'>Identity
  Certification</span>
menu.provisioning=Access Control
menu.audit=<span Title='Identity Audit'>Identity Audit</span> menu.home=Home
menu.configuration=Configuration
menu.settings=<span Title='My Settings'>My Settings</span>
menu.requests=<span Title='My Requests'>My Requests</span>
menu.system=System
menu.identityWarehouse=<span Title='Identity Warehouse'>Identity Warehouse</span>
menu.users= Users
menu.roles= Roles
menu.businessUnit=Business Unit
menu.reporting=<span Title='Reports'>Reports</span>
menu.roleManagement=<span Title='Role Management'>Role Management</span>
menu.roleEngineering=<span Title='Role Engineering'>Role Engineering</span>
menu.roleEntitlementDiscovery=Role Entitlement Discovery
menu.roleConsolidation=Role Consolidation
menu.myRequest=<span Title='My Request'>My Request</span>
menu.rme=<span Title='Role Engineering'>Role Engineering</span>

```

## ▼ To Modify User Labels

1. Open the `rbacxmessages.properties` file located in `$RBACX_WAR/WEB-INF/classes`.
2. Scroll down to the # Identity Warehouse section of the file.
3. As needed, modify any of the existing user labels, which are located to the right of the "=" sign, and save the file.
4. Restart the Role Manager application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```
#####Identity Warehouse #####

user.username= User Name
user.employeeid= Employee Id
user.employeetype= Employee Type
user.firstname= First Name
user.middlename= Middle Name
user.lastname= Last Name
user.allNameRequired=All name's required. user.fullname= Full Name
user.title= Title
user.officename= Office Name
user.street= Street
user.city= City
user.state= State/Province
user.zip= Zip/Postal Code
user.country= Country/Region
user.phone= Phone
user.extension= Extension
user.mobile= Mobile
user.fax= Fax
user.filter.pagesize=Page Size user.pager= Pager
user.pemail= Primary Email
user.semail= Secondary Email
user.comments= Comments
user.suspension= Suspension
user.gustatus= Global User Status user.startdate= Start Date
user.enddate= End Date
user.servicedesk= Service Desk user.status= Status
user.servicedeskticket= Service Desk Ticket
user.serverDeskTicket=Server Desk Ticket
user.customProperty1=Custom Property 1
user.customProperty2=Custom Property 2
user.customProperty3=Custom Property 3
user.customProperty4=Custom Property 4
user.customProperty5=Custom Property 5
user.customProperty6=Custom Property 6
user.customProperty7=Custom Property 7
user.customProperty8=Custom Property 8
user.customProperty9=Custom Property 9
user.customProperty10=Custom Property 10
user.customProperty11=Custom Property 11
user.customProperty12=Custom Property 12
user.customProperty13=Custom Property 13
user.customProperty14=Custom Property 14
user.customProperty15=Custom Property 15
user.customProperty16=Custom Property 16
user.customProperty17=Custom Property 17
user.customProperty18=Custom Property 18
user.customProperty19=Custom Property 19
user.customProperty20=Custom Property 20
user.addBusinessUnit=Add Business Unit
user.address=Address
```

[top](#)

---

## Configuring Error Messages

Configuring error messages in Role Manager is similar to configuring labels.

The `rbacxmessages.properties` and `rbacxaudit-messages.properties` files contain the dynamic links to configure error messages for the Role Manager user interface.

- The `rbacxmessages.properties` file contains error messages that are separated by modules (such as Identity Warehouse, Role Management, Identity Certification, and so on).
- The `rbacxaudit-messages.properties` file allows modifications to error messages only within the Role Manager Identity Audit Module.

These files are located at `$RBACX_WAR/WEB-INF/classes`.

The following procedures describe how to modify the error messages generated from various Role Manager modules.

## ▼ To Modify My Requests Error Messages

1. Open the `rbacxmessages.properties` file located in `$RBACX_WAR/WEB-INF/classes`.
2. Scroll down to the `#My Requests` section of the file.
3. As needed, modify the existing error message labels, which are located to the right side of the '=' sign, and save the file.
4. Restart the Role Manager application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```
#####  
#       My Requests  
#####  
request.error.selectRequest=Please choose a request first!  
request.error.approveFailed=Unable to approve the request!  
request.error.rejectFailed=Unable to reject the request!
```

## ▼ To Modify Identity Certification Error Messages

1. Open the `rbacxmessages.properties` file located in `$RBACX_WAR/WEB-INF/classes`.
2. Scroll to the `#Identity Certification` section of the file.
3. As needed, modify the existing error message labels, which are located to the right of the '=' sign, and save the file.
4. Restart the Role Manager application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```
#####  
# Identity Certification  
#####  
  
idc.error.errorUsersRequired = No Users found in this certification...  
idc.error.errorRolesRequired = No Roles found in this certification...  
idc.error.updateCommentsFailed = Unable to update the comments!  
idc.error.noEndPointsFound = No EndPoints found in this certification!  
idc.error.selectCertification = Please select at least one certification  
first!  
idc.error.selectReport = Please select a report first!  
idc.error.reportError = This report has no pages!  
idc.error.selectDate = Please select date values!  
idc.error.selectMonths = Please select months values!  
idc.error.selectYear = Please select year values!  
idc.error.selectSeconds = Please select seconds values!  
idc.error.selectMinutes = Please select minute values!  
idc.error.selectHours = Please select hour values!  
idc.error.errorAlphanumericCharactersRequired = Certification name must contain alphanumeric characters!  
idc.error.deleteFailed = Unable to delete certification job!  
idc.error.unableToAdd = Unable to add certification job!  
idc.error.checkHighlightedFields = Please check the highlighted fields!  
idc.error.selectBusinessUnit = Please select a business unit!
```

[top](#)

The individuals who post here are part of the extended Oracle Corporation community and they might not be employed or in any way formally affiliated with Oracle Corporation. The opinions expressed here are their own, are not necessarily reviewed in advance by anyone but the individual authors, and neither Oracle Corporation nor any other party necessarily agrees with them.

[Oracle Social Media Participation Policy](#) | [Privacy Policy](#) | [Terms of Use](#) | [Trademarks](#) | [Site Map](#) | [Employment](#) | [Investor Relations](#) | [Contact](#) © 2010, Oracle Corporation and/or its affiliates  
Powered by Atlassian Confluence