IBM Security Role and Policy Modeler
Version 1 Release 1

Product Overview Guide
IBM Security Role and Policy Modeler
Version 1 Release 1

Product Overview Guide

IBM
Contents

Tables ........................................ V

About this publication ....................... vii
Access to publications and terminology .... viii
IBM Security Role and Policy Modeler library . vii
Online publications ........................... vii
IBM terminology website ...................... vii
Accessibility ................................. viii
Technical training ............................. viii
Support information ............................ viii

Chapter 1. IBM Security Role and Policy Modeler introduction ................................ 1
Capabilities . .................................. 1
Who uses this product ......................... 3
Security process integration .................. 3
Role and policy management cycle .......... 4

Chapter 2. Product features .................... 9
Understanding the data ........................... 9
Basic objects of the role modeling ........... 9
Groups ........................................ 18
Data management ............................. 18
Schema import ............................... 19
Data import ................................... 19
Data flow ....................................... 20
Role modeling analysis tools ................. 21
Project and role statistics .................... 21
Generating roles .............................. 21
Analysis catalog ............................... 22
Membership qualifiers ......................... 22
Report analytics ............................... 22
Integration with IBM Security Identity Manager roles . .......................... 22
Role Lifecycle Management .................. 23
Process flow for role approval ............... 24
Introduction to Business Process Manager . 24
Role approval lifecycle request ............. 25
Custom lifecycle request ..................... 26
Test and production environments .......... 26
User registries ............................... 26
User and group definitions and authorization .. 27
Reports ....................................... 28

Chapter 3. What's new .......................... 33

Chapter 4. Getting started with IBM Security Role and Policy Modeler .................. 35
Starting and stopping IBM Security Role and Policy Modeler ................................. 35
Logging on ..................................... 35
Understanding the user interface ............ 36
Home page and navigation pane ............. 36
Modeling roles and policies .................. 37
Reporting ..................................... 42
Importing Identity and Entitlement Data .... 43
Help and online documentation .............. 43

Chapter 5. Hardware and software requirements ........................................ 45
Compatibility with other software ........... 45
Operating system requirements ................ 45
Prerequisite libraries for Linux ............... 46
Hardware requirements ....................... 48
Software requirements ....................... 49
WebSphere Application Server requirements .. 49
Database server requirements ................. 50
Java Runtime Environment requirements ..... 50
Browser requirements ....................... 51
Report server requirements ................... 52
Prerequisites for Extract and Load tools .... 53

Chapter 6. Known limitations, problems, and workarounds .............................. 55

Appendix A. Conventions used in this information .......................................... 71
Typeface conventions .......................... 71
Definitions for HOME and other directory variables ........................................... 72

Appendix B. Accessibility features for IBM Security Role and Policy Modeler .......... 75

Notices ........................................ 77

Index ......................................... 81
## Tables

1. Role Lifecycle Management role approval process flow steps ........................................ 24
2. Reports for IBM Security Role and Policy Modeler .................................................. 29
3. What's new in Fix Pack 1 ......................................................................................... 33
4. What's new in Fix Pack 2 ......................................................................................... 33
5. IBM Security Role and Policy Modeler installation compatibility ............................... 45
6. Operating system requirements for IBM Security Role and Policy Modeler ............... 45
7. Prerequisite libraries for Red Hat Enterprise Linux 6.0 and later ............................. 47
8. Hardware requirements for IBM Security Role and Policy Modeler ............................. 48
9. Disk space requirements ......................................................................................... 48
10. WebSphere Application Server requirements ......................................................... 49
11. Database server requirements .............................................................................. 50
12. Browser requirements for IBM Security Role and Policy Modeler ............................ 51
13. Report server requirements ..................................................................................... 52
14. Home directory variable definitions ...................................................................... 72
About this publication


Access to publications and terminology

This section provides:

- “IBM Security Role and Policy Modeler library”
- “Online publications”
- “IBM terminology website”

**IBM Security Role and Policy Modeler library**

The following documents are available in the IBM Security Role and Policy Modeler library:

- *IBM Security Role and Policy Modeler Quick Start Guide*, GI13-2313
- *IBM Security Role and Policy Modeler Glossary*, SC27-2800

**Online publications**

IBM posts product publications when the product is released and when the publications are updated at the following locations:

**IBM Security Role and Policy Modeler Information Center**


**IBM Security Information Center**


**IBM Publications Center**


**IBM terminology website**

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see Appendix B, “Accessibility features for IBM Security Role and Policy Modeler,” on page 75.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Role and Policy Modeler Troubleshooting Guide provides details about:
• What information to collect before contacting IBM Support.
• The various methods for contacting IBM Support.
• Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.
Chapter 1. IBM Security Role and Policy Modeler introduction

IBM Security Role and Policy Modeler Version 1.1 provides a business-centric approach to planning, understanding, and modeling the security roles and separation of duty constraints for securing access to critical resources.

Using visual tools and familiar business intelligence techniques, IBM Security Role and Policy Modeler reduces the time and effort to design, manage, and approve roles and role structures for enterprise IT governance. It provides web-based modeling interfaces and reports for owners of business processes and applications so that they can use role-based access control for their employees.

This release focuses on understanding who in the organization is entitled to the access to critical resources and why. The focal point is the business role analysts who develop and maintain roles and policies. The role analysts work with the application and business owners and IT to understand the assets and build the models. These models communicate to the lines of business, corporate executive offices, and IT. They also provide deployment guidance to IT based on the business model.

The role analyst can tailor the attributes for IBM Security Role and Policy Modeler. Specifying the significant business attributes and determining appropriate access to resources optimizes the modeling and analytical tools.

The role analysts can work in parallel, creating modeling projects for specific organizational units, key application access, or a combination of both. They can review the data used for modeling, generating, creating, copying, analyzing, editing roles, and reporting on roles and policies. Completed role models can be sent to business owners for approval and then are exported for deployment.

Capabilities

IBM Security Role and Policy Modeler is a WebSphere application with a web interface. It provides the following capabilities.

Project based organization
A modeling project contains a set of roles, separation of duty constraints, and users and permission data. The role analysts scope the data to better facilitate and manage the role development process.

Role creation, editing, analysis, and interactive simulation
The role analysts can create roles, change role hierarchies, specify owners, assign user members, and attach permissions. They can provide additional custom data about the role, such as the associated business process and organizational units where the role applies. The role editing feature contains a catalog of analysis tools to evaluate and tune members or permissions assigned or attached to the roles. Changes made to the role are interactively evaluated; the results are presented to the analysts during the editing session.

Role generation through data mining
Role generation mines the user-to-permission data in a project to create an initial set of roles that optimize user access to permissions. The role analysts can adjust the role hierarchy depth and the number of roles.
generated with two mining controls. The role analysis catalog is used with role generation to name and tune the generated roles.

**Separation of duty constraints and interactive simulation**

Role level separation of duty constraints can be applied to roles and role hierarchy. Two or more roles can be assigned to the same person without warning. Changing the role membership or role structure provides role level feedback on any violations of the constraints.

**Analytics-based reporting**

IBM Cognos reporting technology provides reports that are ready for immediate use. These reports can show role details, user access, permission view of assignment, and exploration of the modeling data. The reporting component comes with a powerful custom report designer and the ability to schedule, mail, and send reports.

**Integration with IBM Security Identity Manager operational roles and separation of duty policy**

You can import modeling data, existing IBM Security Identity Manager roles, and separation of duty policy in the modeling program with comma-separated value (CSV) files. These CSV files are generated by a data extraction utility. New and updated roles and role membership can be exported in XML format and loaded into IBM Security Identity Manager using a role loading utility.

**Import of roles from business and third party sources**

You can load existing roles from sources other than IBM Security Identity Manager into the modeling program with a CSV file. Tivoli® Directory Integrator can assist with the generation of CSV files from business sources and third party applications.

**Business process automation for role approvals and certifications**

IBM Security Role and Policy Modeler contains IBM Business Process Manager to drive and track role approval and certification.

**Custom schema management**

You can add, change, and define the business attributes associating to roles, permissions, users, and separation of duty constraints through a CSV file interface.

**Data Management**

The modeling data includes user identities, permissions, roles, separation of duty constraints, user-to-permission assignments, user-to-role assignments, permission-to-role assignments, and hierarchical values. They are loaded as snapshots of data from various sources such as CSV files. A set of data from multiple CSV files can be collected by the modeling application. They can be committed as a set of modeling data for modeling roles and policies. As the data changes, new snapshot in the form of CSV files can be used to update the modeling data. An extract utility for the IBM Security Identity Manager server creates snapshots of IBM Security Identity Manager data. Tivoli Directory Integrator can assist with the generation of CSV files from other business sources and third party applications.
Who uses this product

IBM Security Role and Policy Modeler is designed for the business analyst, the sponsor of role development projects, business role owners, and security administrators. The product supports IT system owners who need to assist loading the modeling data from IT systems.

The role analysts work with many other people in the enterprise to design, refine, and verify the models. They collaborate with other corporate officers, business process owners, managers, applications owners, application administrators, and so on. The follow graphic describes people who use this product.

Security process integration

Modeling and planning are part of overall security process integration in an organization. Organizational security needs and requirements are prioritized, implemented, deployed, enforced, and monitored. As an organization or their requirements change, the security process integration cycle continues planning using the feedback from the process.

The iterative process is a collaborative effort of planning for and accommodating daily changes to the organizations and major business events like reorganizations and acquisitions. IBM Security Role and Policy Modeler is a provider of application services that help the business plan for role-based access requirements and rollout and the day-to-day maintenance of roles and separation of duty constraints.
IBM Identity and Access Governance Process Integration

Role and policy management cycle

The design and deployment of roles is a collaborative effort between the line of business and the provider of application services. The line of business needs access to business applications while the provider of application services, usually the IT organization, supports the lines of business. The role lifecycle typically starts with a request from a line of business to simplify administering access to applications. It is often guided by corporate governance policies.
The following scenario of a company that is migrating to role-based access control illustrates the role management cycle.

JKHealthcare is a healthcare provider that has grown to more than 5,000 employees over the last few years. They have over 400 applications in production. Their applications include a customer portal, B2B integration with the supplier network, and employee forums. They also have shared file systems and financial and healthcare applications governed by various regulations. Managers request access for their employees through a collection of in-house tools, help desk, and email.

Recently, Dennis Moreland, Security Compliance Manager, asked the auditor, Jeff Benson, to perform an in-house audit of access to several key healthcare applications. They found that there were more accounts than employees in some applications. A number of groups were granted access to projects that never started. In other applications, no accounts or employee access jumped out as a red flag.

Dennis is requested to work with other people to clean up the access to 18 key applications and move those applications to role-based access control. This way they can improve the compliance posture of the applications and reduce the cost of maintaining proper access. It makes it easier for managers to approve and recertify access.

Dennis considers the initial issues found by Jeff and decides to take action. He plans to drive priority items for himself and the Role and Policy Analyst, Ram Laxman, Security group leader, Mike Stevens, application owner, Wanda Liu, and managers such as Chuck Reigle.

- Dennis works with Ram to define the goals for transition to role-based access control. The goals include identifying and prioritizing the critical applications, organizational units, and metrics to measure the success of the effort. They
decide on a set of milestones, where the goal of each milestone is to model three departments for two critical applications. These milestones can show progress and success at a sustainable pace.

- Ram works with Marjorie Ramsey-Schmidt, a senior developer from the information technology team, to gather the permission entitlement data from the identified applications. They also gather the user identity information from the prioritized organizational units. Marjorie uses a command-line utility for IBM Security Identity Manager to extract the schema, permission entitlements, and user profile information for the modeling. If roles and separation of duty policies have been defined in IBM Security Identity Manager, Marjorie includes data in the modeling data.

- One application, the badge access system, is not provisioned by IBM Security Identity Manager. Dennis wants to develop roles for the badge access to secure areas. Marjorie uses the interfaces of the badge access system to extract the modeling information and prepare the CSV files of information. Marjorie imports the data into the Identity and Entitlement database.

- Ram runs reports to check the state of the initial data import and assess the completeness and quality of the data. When needed, Ram creates custom reports to meet the specific needs of the business. Ram also reviews this information with Dennis and the department managers. He catches missing data, which impacts the quality on the roles. He finds that some of the permissions for the critical application do not have a business description. Ram asks Wanda, who is responsible for the applications, and Mike, who owns the security implementation of the applications, to verify the information and fill in gaps.

- Ram also gathers interview data from Wanda and Chuck to better understand what the lines of business expect when it comes to access to the company resources. Chuck is also responsible for verifying that the right people have the right access to the application.

- With the new data that Ram collects, Marjorie works with Ram to update the CSV files and import the updates, additions, and deletions into IBM Security Role and Policy Modeler.

- Ram creates an initial role model by selecting all or a subset of users and application permissions. He uses several options and analytical tools in IBM Security Role and Policy Modeler to automatically generate roles based on the IBM Security Role and Policy Modeler data mining. He reviews and changes role generation options, creates roles based on business input, and copies existing roles. He can then view, edit, analyze, and adjusts these roles.

- Ram produces analysis reports to share with other stakeholders such as Dennis, Wanda, Mike, and so on. These reports include the roles, policies, users, permissions, and user to permissions assignments that result from the models. Where needed, Ram creates custom reports to meet the specific needs of the business. The stakeholders provide feedback to Ram, who further refines the model.

- When Ram and the stakeholders agree with the model, Ram submits the role to the role owner, Chuck, for the formal role approval. Chuck is notified of this role approval request by mail. He clicks the link in the email, reviews the final draft of the role, and approves it. Ram receives an email, indicating if Chuck approves or rejects the role.

- After the role approval, Ram exports the model in an XML file format and load it into IBM Security Identity Manager. Mike uses a command-line tool for the IBM Security Identity Manager to load and update the roles and separation of duty policies. He then uses the IBM Security Identity Manager administrative UI to complete the provisioning policies or align the imported roles with the existing provisioning policies.
• Ram also provides Mike with reports that describe the model for implementation in the IT systems, such as the secure room badge access system. Mike reviews the model and then works with the badge access coordinator to implement the model. In addition, he sets up a IBM Security Identity Manager manual service that assigns a task to the badge access coordinator to provision users to secure areas.

• Periodically, Marjorie gathers the current data from IBM Security Identity Manager, other identified applications, and HR databases to refresh the IBM Security Role and Policy Modeler database. Ram uses the analytical tools and statistics provided by IBM Security Role and Policy Modeler to determine how the roles function. He runs reports on the model analytics to share with Dennis and other stakeholders to evaluate if changes are needed in the model. He might also ask the role owners to certify that the roles they own are still needed and accurate.

• Based on the analysis and feedback from the role certification, Ram modifies the roles and policies. He gets the changes approved and works with Mike to deploy these changes.

• A few times during the year, Jeff Benson, an auditor, gets reports from IBM Security Role and Policy Modeler on the intended model design. He compares it with the state of the IT systems to see how well the company is tracking the security model and to identify areas of concern. Jeff uses the model baseline comparison as an input in his auditing process.

As this scenario illustrates, when a business adopts role-based access control, the roles go through a process cycle of creation, update, validation, and implementation.
Chapter 2. Product features

IBM Security Role and Policy Modeler delivers the role and policy modeling capabilities that secure the control of the access to your business resources.

Understanding the data

To produce easily maintained roles, the role analysts use IBM Security Role and Policy Modeler to explore users, permissions, roles, and their attributes, and the relationships between them.

To scale up to thousands of users to even more permissions, the role analysts model the user-to-permission assignments through roles and role hierarchies.

To model effectively, the role analysts need to choose attributes for users, permissions, and roles that are meaningful to the business. They can help create security roles based on common attribute values. For example, all the employees responsible as Head Nurse at Grace Hospital need the authority to approve changes to “Patient Care Orders” in the application. To support this analysis, significant modeling attributes are needed. These attributes include the job code, their work location, the permission attributes of authority, resource, and application name.

Both data and custom schema for users, permissions, and roles are initially imported into the Identity and Entitlement database with the IBM Security Role and Policy Modeler import sessions and CSV files. Changes and deletions of the modeling schema and data in the Identity and Entitlement database are handled with subsequent imports of data from the CSV files.

Basic objects of the role modeling

The role analysts work with four object types: users, permissions, roles, and separation of duty constraints. They also work with five relationship types: user-to-permission, user-to-role, role-to-permission, role-to-role, and role-to-constraint (separation of duty constraint).

In addition to direct user-to-role relationships, membership qualifiers can simplify the process of mapping users to roles by defining membership based on the attribute values of a user.
Role analysts create efficient role designs by using the data, visual editor, analysis tools, and the automated role generation features.

**Required schema attributes and custom schema attributes**
Each of the modeling objects has a set of predefined schema that cannot be changed. However, you can extend it with custom attributes.

If the custom attributes are defined and populated, IBM Security Role and Policy Modeler provides an in-depth analysis on the data to create optimized roles for the organization. You can create, update, or remove the values for the custom schema by importing the data.

IBM Security Role and Policy Modeler uses custom schema attributes in two ways: to scope the projects and to analyze and optimize the roles. For example, the role analysts use a custom attribute on the user object to scope a project to users contained in a subset of organizational units. Later, the role analysts review a distribution of role membership by organizational unit to better understand who needs a role.

If IBM Security Identity Manager is deployed, then the IBM Security Identity Manager extract utility creates a schema file with custom schema attributes that match this deployment. The IBM Security Identity Manager extract utility also creates the CSV files from the IBM Security Identity Manager role, user, and permission (account and group assignment) data to load into IBM Security Role and Policy Modeler.
**Attribute types**
IBM Security Role and Policy Modeler objects have four attribute data types that must be specified.

**String**  Any string of less than 241 characters in length.

**Integer**  A positive or negative integer.

**Identity**  A reference to a user object in the project.

**Hierarchy**  Attributes with a name, description and identifier that can be arranged in a hierarchy, such as an organizational tree.

**Data sources**
All data imported into the Identity and Entitlement database must be associated with a source.

The source can represent all the data from a physical repository like all the user data from an LDAP directory. It also can be a logical subset of data like all the users A-J from an HR database. For roles, permission, and separation of duty constraints, all the attributes for an object must be imported as a single record associated with a source. The objects can come from multiple sources.
User identity attributes can come from multiple sources. They are joined in the identity and entitlement database with a unique user ID as the correlator. For example, the user identity data HR attributes can come from the IBM Security Identity Manager identity source with additional training certifications from a training database source.
Building Composite Identity Records

- Sources of user identity data
- CSV files for user identity attributes coming from multiple sources
- Composite user records in the Identity and Entitlement Database

The source represents a full set of the logically partitioned data. IBM Security Role and Policy Modeler compares the current data in the identity and entitlement database for a source with updated identity information from the same source. It detects the deleted identity information. To delete all data from a source, the source must be specified in an import file with no corresponding data records.

**User identities**

A user identity is the collection of attributes and values for a specific person. At minimum, a user identity includes an ID and a name.

Through importing data from the CSV files, user identities are added to the IBM Security Role and Policy Modeler identity and entitlement database. See the
“Importing data” topic in the IBM Security Role and Policy Modeler Information Center for details about importing data. User identities have a small set of required attributes defined to the schema. However, you can customize attributes to extend the data model.

Here are the required schema attributes for user identities:

**Person UID**
Uniquely identifies a user for all associated user attributes from all identity sources in the Identity and Entitlement database and modeling projects. This attribute does not display on the GUI; it is used internally to correlate and manage users in the models.

**Source Record UID**
In an identity source, a user can have multiple entries. For example, a user can own multiple accounts. Individual source records for a user are correlated by using the Person UID for records with different Source Record UIDs.

**Person Name**
The name displayed in the UI and reports. The person name is not guaranteed to be unique.

Using only Person UIDs and user-to-permission mappings, IBM Security Role and Policy Modeler can generate and optimize roles. However, adding more business attributes to the user object increases the value of the optimization and role analysis. It is a good practice that the role analysts customize the user schema to add additional data useful for modeling. Here are some helpful examples of identity data attributes:

**Job Responsibility or Job Code**
Associate people into roles based on the similar responsibilities.

**Organization**
Associate people into roles based on the area of the business.

**Department**
Associate people into roles based on the work group.

**Work Location**
Associate people into roles based on the geographic or physical location.

**Relationships**
Associate people into roles based on the common identity relationship, such as a role.

**Education Level**
Restrict access based on the level of education.

The data for custom attributes must also be included in the user source data import with the UID associated with it. At least one identity source must supply the Person Name value.

**Permissions**
For modeling, permissions are abstract representations of an action on a resource.

The permission can contain different levels of details to meet the modeling goals. The IT implementation of a modeled permission can represent a high-level permission, such as an account on a system or a membership in a group. The permission can also represent a fine grained transaction on a column or row of a database.
Through importing data from the CSV files, permissions are added to the IBM Security Role and Policy Modeler Identity and Entitlement database. Permissions have a small set of required attributes defined to the schema, but you can customize the attributes to extend the data model.

Here are the required schema attributes for permissions:

**Permission UID**
- Uniquely identifies a permission in the Identity and Entitlement database and all modeling projects. The Permission UID must be unique across all sources of permission data. This attribute does not display on the user interface, but it is used internally to correlate and manage permissions in the models.

**Permission Name**
- The display name used in the user interface and reports. The permission name is not guaranteed to be unique. It is a good practice to use a naming convention to name the permission uniquely across all permission sources.

**Permission Description**
- The optional information to describe the permission to the role analysts and the business users. A value for this description is optional.

Using only Permission UIDs and user-to-permission mappings, IBM Security Role and Policy Modeler can generate and optimize roles role models. However, the more business attributes added to the permission object, the better the optimization and role analysis are. It is a good practice that the role analysts customize the permission schema to add additional data useful for modeling. Here are some helpful examples of permission data attributes:

**Action**
- Permission action attributes such as represent, read, write, delete, and so on. The permission action is often in the permission name. However, adding some custom attributes helps with the role analysis and scoping.

**Resource**
- Data or transaction protected by this permission. The protected resource is often in the permission name and description. However, adding some custom attributes helps with the role analysis and scoping.

**Application**
- The name of the application that contains the protected resources.

**Owner**
- One or more business or IT owners of the permission.

**Risk Sensitivity**
- An assessment of the risk of assigning this permission to present to the organization. For example, writing the patient records can be a high risk, where reading the patient records is a medium risk. Business assessment data can assist the role analyst in creating roles to properly protect higher risk assets.

The data for custom attributes must also be included in the permission source data import with the UID, Name, and Description values.

**Roles**
Roles are a method of mapping users to permissions of managing resources. It is a job function that identifies the tasks that users can perform and resources to which users have access.
You can create roles with the role editor and role generation tools. Roles can also be imported into the Identity and Entitlements database and copied into modeling projects. Imported roles can be the roles extracted from IBM Security Identity Manager or other IT systems. They can be business roles developed by interviewing the lines of business or application owners.

Roles are added to the IBM Security Role and Policy Modeler Identity and Entitlement database by importing data from the CSV files. Roles have a larger set of required attributes defined to the schema, but you can customize the attributes to extend the data model.

Here are the required schema attributes for roles:

**Role UID**
Uniquely identifies a role for all roles imported into in the Identity and Entitlement database. Unlike user or permission, the Role UID might not be unique across all imported data and modeling projects. A Role UID is unique within a project and in the set of imported data. The Role UID must be unique across all sources of imported role data. This attribute does not display on the user interface, but is used internally to correlate and manage permissions in the models.

Role UIDs play a special part in associating modeled roles with the roles deployed in IBM Security Identity Manager. When roles are imported from IBM Security Identity Manager, the Role UID is set to the UID generated by IBM Security Identity Manager. When these roles are copied into a project for modeling, the analyst can keep the existing UID or generate a new UID. If the UID of the role in the project is the same as the UID from the external source of the role, you can associate the modeled role with the deployed role when you export it. For example, the existing IBM Security Identity Manager roles can be imported into IBM Security Role and Policy Modeler and then copied into a project. The analysts can change the role attributes, the structure of the roles, and the separation of duty constraints of the roles. When exporting from the project with the UID generated by IBM Security Identity Manager, the role changes can be loaded into IBM Security Identity Manager, updating the existing roles.

**Role Name**
The display name used in the user interface and reports. The role name is not guaranteed to be unique.

**Role Description**
The information to describe the role and its use to the role analysts and the business users. A value for description is optional.

**Role Type**
An optional use type for the role, such as Business role or Application role, to describe the classification of role to the business users. The types of roles are customizable to any string. After installation, IBM Security Role and Policy Modeler configures Business role and Application role as selections for type. You can remove these types and add other types to match the terminology of the enterprise role-based administration. The term *Role Classification* in the IBM Security Identity Manager user interface is equivalent in meaning as *Role Type* in IBM Security Role and Policy Modeler. A value for Role Type is optional.

**Role Owner**
The role owner is a multivalued attribute that optionally specifies the users
responsible for the role in the lifecycle of the role. The role owner attribute is used when determining who needs to approve a role.

**Note:** The role owner is limited to identities. Roles as owners are not supported.

**Role Parent**
If the role is part of a role hierarchy, the Role Parent attribute contains one or more Role UIDs of Parent Roles for imported roles.

Roles can have additional custom attributes. Custom attributes help an enterprise better identify and manage roles. Custom attribute values can be viewed in the role editor and are part of IBM Security Role and Policy Modeler reports. Here are some helpful examples of custom role attributes:

**Organization**
Name of the organization that uses this role or the name of the organization that owns this role.

**Application**
If the role is closely tied to an application, the application name can be associated with the role.

**Business Task**
The name of the business process or task that requires this role.

**Optional Reviewers**
Interested parties affected by changes in the role or people that can provide insight for the role analysts.

**Risk Classification**
An business assessment of the risk that a role represents in terms of access.

The data for custom attributes must also be included in the role source data import with the UID, Name, and Description values.

**Separation of duty constraints**
A separation of duty constraint is a business control applied to a role. The constraint specifies that a user might not be granted more than one set of roles that represent a risk to the business.

For example, a user cannot be a member of the Purchasing role and the Payments role at the same time. The role analysts use separation of duty constraint rules to create a role model that adheres to acceptable business risks. The violations can be viewed and reported from the model.

Here are the required schema attributes for separation of duty constraints:

**Rule UID**
Uniquely identifies a separation of duty constraint involving two or more roles.

**Rule Description**
The information describes the constraint.

**Cardinality**
The maximum number of roles associated with the constraint can be assigned to a user before a violation occurs.
Role UID
Two or more unique role identifiers that make the list of roles constrained by the rule.

Relationships between users, permission, roles, and constraints
The five relationship types are also specified as imported data: user-to-permission, user-to-role, role-to-permission, role-to-role, and role-to-constraint.

The relationship for the role-to-role hierarchy is set in the Role parent attribute of the role object. The role-to-constraint relationship is set in the separation of duty constrain object. The remaining relationships, user-to-permission, user-to-role, and role-to-permission, are imported in their own source definitions from the CSV files.

Here are the required attributes for importing:
- User-to-permission is a Person UID and Permission UID for each mapping
- Role-to-permission is a Role UID and Permission UID for each association
- User-to-role is a Role UID and Person UID for each association

Groups
Groups in registries can have many meanings, depending on how the groups are used by the application and by the business process.

For role and policy modeling, IBM Security Role and Policy Modeler focuses on two use patterns for groups: groups representing an assignment to a role and groups representing an assignment to permission.

Groups representing an assignment to a role
Business owners use groups in a directory to represent a business role. A group is a collection of users with a common job responsibility.

Groups representing an assignment to a permission
In an access control list (ACL), groups ease the administration of mapping users to the permissions. The group represents a user-to-permission mapping to grant the permission to a set of users. It is often called an application role. The mapping of a group to a permission is often predetermined by the application, or configured by the IT department during the application deployment.

IBM Security Identity Manager groups
The IBM Security Identity Manager extract utility allows a group in the modeling data to be configured. Groups provisioned in IBM Security Identity Manager can be configured to represent permissions and permission assignment or roles and role assignments when extracted into a CSV file.

Data management
The IBM Security Role and Policy Modeler data management includes customizing and managing the data schema and loading and maintaining the modeling data.

The schema and data are managed in a three-stage process: loading data files, validating data, and committing schema and data for modeling.

In general, the data is prepared for modeling in these steps:
1. Gather the data from IBM Security Identity Manager, IT sources, and lines of business.
2. If needed, create the comma separated formatted files.
3. Start a data import session and choose if the update is a schema update or data update.
4. Upload files into the session. Check for errors and resolve errors in the files.
5. Validate the schema or data in the session before committing the update. Correct errors by loading additional files, removing data files, or changing the data files and reloading the files. The operation report can be used to review data in an import session and the data committed in the Identity and Entitlement database.
6. Commit the schema and data update. Committing schema makes new attributes available to be loaded as data and removes values for deleted attributes. Committing the data merges the data in the import session with the data committed by the previous import session.

The schema and data management is iterative for both scale and maintenance. Only the schema and data required for modeling planned projects must be committed to the modeling database. As new projects require additional schema or additional sources of data, incrementally add the delta of new information. Add new data and data updates in planned increments with one or more data import sessions.

**Schema import**

The IBM Security Role and Policy Modeler schema can be changed by importing the schema updates.

The changes include:

- Logical sources of data used to import data. Data sources let the administrator plan and stage data committed to the modeling database.
- Attributes of permissions and users displayed on the IBM Security Role and Policy Modeler user interfaces and reports.
- Custom attributes of a role that can be associated, viewed, and managed as additional information.
- Custom attributes about imported separation of duty constraints to be displayed in the reports.
- The values of the role type attribute of a role that can be used to classify a role.

For details about the format of schema CSV file, see the “Importing schema” topic in the IBM Security Role and Policy Modeler Information Center.

**Data import**

The IBM Security Role and Policy Modeler data can be changed by importing the data updates.

The changes include:

- Create, delete, and update a role, user, permission, and separation of duty constraint.
- Create, delete, and update the user-to-permission, user-to-role, role-to-permission, role-to-role, and role-to-constraint mapping data.
- Values and hierarchy for hierarchical data.

For information about the format of data CSV file, see the “Importing data” topic in the IBM Security Role and Policy Modeler Information Center.
Data flow

The role modeling data comes into IBM Security Role and Policy Modeler by being imported as CSV format files.

The sources of data and the attribute schema for the source are defined by the CSV files. The CSV files are created by the IBM Security Identity Manager extract utility. They can be also created by editing existing CSV files, or by other tools, such as Tivoli Directory Integrator.

To produce an interactive modeling experience for the role analyst, IBM Security Role and Policy Modeler divides the modeling process into two phases: data import and security modeling. The IBM Security Role and Policy Modeler server and database support these two phases by managing two sets of data:

Staging database for collecting data to import

As data is collected, it is imported into the staging database. Data in the staging database does not affect role modeling projects.

The statistical information can be reviewed in the import session, and it can be generated as detailed reports. After passing the review, the data is committed, which moves the data to the modeling tables of the database. During the commit process, the records in the staging database are merged and resolved with data in the modeling database. These records include new, updated, and deleted records.

Identity and Entitlement database for modeling

When data is imported into the Identity and Entitlement database, the role analysts can start the security modeling process.

The data committed from the staging database must be a complete set of data from a given source per entity. For example, they must be all identity records and attributes for the users to be modeled. They must have all permissions (groups) and permission mappings (group memberships) from an LDAP directory. With a full feed from a source, IBM Security Role and Policy Modeler can detect deleted records. It compares the complete set of records from the source per entity type with the records in the modeling database and obtains the deleted records.
The IBM Security Role and Policy Modeler application administrator updates the modeling data from feeds on a periodic basis. The validating and committing processes are asynchronous and potentially long running tasks. Because the new data can change the statistics and information about a role model, committing new data affects any existing projects. When data is newly committed, no editing or viewing of the projects can be done. Editing and viewing can start when the commit process has completed and the project statistics are recalculated. When the project state is \textit{Recalculation Needed}, the role analysts can select the projects and submit the project for recalculation. After the recalculation is complete, the project is ready for editing.

\textbf{Role modeling analysis tools}

IBM Security Role and Policy Modeler provides multiple tools for the role analysts to understand, generate, and tune roles. These tools can help create and maintain optimal roles for an organization.

\textbf{Project and role statistics}

The modeling project displays a summary of statistics about the roles and role modeling project.

Project statistics include the total number of users, permissions, roles, and constraints in the project scope. It also includes the percentage of permissions assigned to the roles in the project scope.

The role statistics include the number of users and permissions assigned to each role, number of inherited users and permissions, and role hierarchy. You can review a visual overview of the role hierarchy through the Hierarchy View of the project with popup summaries of each role.

\textbf{Generating roles}

IBM Security Role and Policy Modeler can generate a set of roles based on the user-to-permission mappings imported into the Identity and Entitlement database.

Roles are created based on mining the user-to-permission mappings, creating users with like permissions into the same role. The role analysts can control the number of roles generated in two ways:

- Set the amount of hierarchy that is used by the mining process.
- Have the algorithm ignore potential roles, where the roles contain only one or two members and permissions.

Using these methods, the role analysts can generate roles that meet the project-specific criteria on both the number of roles to manage and coverage of user-to-permission assignments.

After generating the roles, the role analysts can review the information about the roles. Reviewing the attributes of the users and permissions in a role or the analytical tools in the role analysis catalog helps better understand the generated roles. They can name and describe the role and build role membership qualifiers to help identify the users who must or must not be in the role.

For more information, see the “Role administration” topic in the IBM Security Role and Policy Modeler Information Center.
**Analysis catalog**

The analysis catalog is a set of analytical summaries and drill-downs that help role analysts tune roles for efficiency.

The analysis tasks answer questions about the roles and identify potential users, permissions, and problems. Here are sample questions that the analysis catalog can answer:

- What attributes of the role members are a good predictor of role membership?
- What attributes of the role permissions are a good predictor of other permissions that can be assigned to the role?
- What attributes do members have in common?
- Are there good candidates for the role based on these attributes?
- What accesses do the members have in common?
- Are there good candidates for the role based on these similar accesses?
- How are the attributes of the permissions assigned to the similar role?
- Are there good candidate permissions to add to the role?

For more information about how to analyze roles and policies, see the “Role and policy analysis” topic in the IBM Security Role and Policy Modeler Information Center.

**Membership qualifiers**

The role analysts can create a membership qualifier to filter the membership of a role through input of the lines of business or analysis catalog.

A membership qualifier helps a role analyst identify the users that do not belong to certain roles and automatically include users who do. For example, role analytics can show that the membership of a role is made up of employees who work for the pharmacy department of a hospital. These people have been trained and certified in controlled substance processes. Therefore, a membership qualifier uses the attributes of the pharmacy department and certification to filter out the disqualified people. It includes the new members who share these attributes but were not previously members of the role.

Membership qualifiers can be multipart Boolean expressions and are built using a qualifier editor. For more information, see the “Creating a role membership qualifier” topic in the IBM Security Role and Policy Modeler Information Center.

**Report analytics**

In addition to the analytics built into the user interface, IBM Security Role and Policy Modeler provides more details on the role models through the reporting interface.

For more information about IBM Security Role and Policy Modeler reports, see the “Reports” topic in the IBM Security Role and Policy Modeler Information Center.

**Integration with IBM Security Identity Manager roles**

Roles imported from IBM Security Identity Manager can be copied into a project, then visualized and analyzed about its membership.
Using the IBM Security Role and Policy Modeler role editor, you can update the role name, description, hierarchy, and membership. The changes can be exported and loaded back into IBM Security Identity Manager. Roles imported from IBM Security Identity Manager do not have permissions attached to them. In IBM Security Identity Manager, the provisioning of attributes that equates to permissions is done through a provisioning policy object. This object contains special code and scripting to determine the final access granted by the policy. The IBM Security Identity Manager role imported into IBM Security Role and Policy Modeler has an additional information attribute that contains the identifier of any provisioning policies associated with the role.

**Role Lifecycle Management**

Role Lifecycle Management provides a process to approve role design for IBM Security Role and Policy Modeler. Using the IBM Security Role and Policy Modeler console and IBM Business Process Manager process definition template file, you can get started with the role approval process. You can also create a custom lifecycle request.

For example, when a role analyst creates a role or role hierarchy in IBM Security Role and Policy Modeler, the role owners must approve this new design. The following diagram shows the interactions and flow of this type of process.

As shown in the diagram, the role analyst selects roles for approval using the IBM Security Role and Policy Modeler console. The approval request is submitted which sends an email notification to the role owner to inform them of a role to approve. The role owner approves or rejects the new role using the Business Process Manager console. The status update is then sent back to the role analyst.

![Role Lifecycle Management process flow](image)

*Figure 1. Role Lifecycle Management process flow*

As shown in the diagram, the role analyst selects roles for approval using the IBM Security Role and Policy Modeler console. The approval request is submitted which sends an email notification to the role owner to inform them of a role to approve. The role owner approves or rejects the new role using the Business Process Manager console.
Process Manager process application. The status of this process is updated in the IBM Security Role and Policy Modeler console.

The diagram also shows how a custom process flows.

Process flow for role approval

The Role Lifecycle Management process flow for role approval requires both IBM Security Role and Policy Modeler and Business Process Manager.

The following steps show the Role Lifecycle Management role approval process flow, including the responsible party:

<table>
<thead>
<tr>
<th>Step</th>
<th>Who</th>
<th>Task</th>
<th>Information center topic name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>System Administrator</td>
<td>Install IBM Security Role and Policy Modeler version 1.1 and Fix Pack 1 or later. This process includes installing Business Process Manager version 7.5.1.</td>
<td>“Fix pack installation tasks”</td>
</tr>
<tr>
<td>2.</td>
<td>System Administrator</td>
<td>Configure and enable the Role Lifecycle Management feature. This includes setting up the user registries and defining the role analysts and role owners.</td>
<td>“Configuring and enabling Role Lifecycle Management”</td>
</tr>
<tr>
<td>3.</td>
<td>Role Analyst</td>
<td>Add or update roles and hierarchies in the IBM Security Role and Policy Modeler console.</td>
<td>“Role administration”</td>
</tr>
<tr>
<td>4.</td>
<td>Role Analyst</td>
<td>Submit a lifecycle request from the IBM Security Role and Policy Modeler console.</td>
<td>“Submitting a lifecycle request to approve roles”</td>
</tr>
<tr>
<td>5.</td>
<td>Role Owner</td>
<td>Respond to the lifecycle request.</td>
<td>“Approving or rejecting a role request”</td>
</tr>
<tr>
<td>6.</td>
<td>Role Analyst</td>
<td>Determine the status of the role request. If all role owners approve the request, the approval process is complete. If at least one role owner rejects the request, the role request is rejected. You can review the comments and you might update the roles and retry the approval process.</td>
<td>“Viewing the history of a lifecycle request”</td>
</tr>
<tr>
<td>7.</td>
<td>Role Analyst</td>
<td>Optionally, audit the process data.</td>
<td>“Auditing role approval process data”</td>
</tr>
</tbody>
</table>

Introduction to Business Process Manager

IBM Business Process Manager is an integrated platform to develop, manage, and run the Role Lifecycle Management process.

Business Process Manager contains the following components that Role Lifecycle Management uses:
• **Business Process Manager Process Center** provides the authoring and administering environment for process templates. The Role Lifecycle Management process template is imported to the Process Center for further customization and deployment.

  From the Process Designer, users connect to the Process Center. The Process Admin Console enables administrators to manage the server and process applications at run time.

• **Business Process Manager Process Designer** provides the authoring environment to create process applications. The Process Designer can be run only on a Windows operating system.

• **Business Process Manager Process Server** provides the runtime engine to support business processes. The Process Admin Console enables administrators to manage the server and process applications at run time.

• **Business Process Manager Process Portal** provides the interface for users to participate in the process.


To install Business Process Manager, see the “Installing Business Process Manager Standard” topic in the IBM Security Role and Policy Modeler Information Center.

### Role approval lifecycle request

Role approval is a type of lifecycle request that IBM Security Role and Policy Modeler provides. It requires the Business Process Manager role approval process template and toolkit provided with IBM Security Role and Policy Modeler.

The installation of IBM Security Role and Policy Modeler version 1.1 Fix Pack 1 or later copies a process template for role approval into the `lifecycle` directory of the IBM Security Role and Policy Modeler HOME installation directory. The process template includes a toolkit that enables Process Designer users to share library items across process applications. The name of the template file is `IBM_Security_Role_Lifecycle_Management_Integrated_Approval.twx`.

To import the template and toolkit into Business Process Manager, see the “Importing the process application and toolkit” topic in the IBM Security Role and Policy Modeler Information Center.

You can use the process template as is or customize it for your process. Go to the IBM Business Process Manager Information Center at [http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r5m1/topic/com.ibm.wbpm.main.doc/ic-homepage-bpm.html](http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r5m1/topic/com.ibm.wbpm.main.doc/ic-homepage-bpm.html) and search for `modeling processes`.

Another sample process template exists in the `samples` directory of the IBM Security Role and Policy Modeler HOME installation directory. The name of the template file is `IBM_Security_Role_Lifecycle_Management_Approval.twx`. This template contains a process that does not use integration with the IBM Security Role and Policy Modeler user interface. See the instructions for using this template at [https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Identity%20Manager/page/Role%20Lifecycle%20Management/attachments](https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Identity%20Manager/page/Role%20Lifecycle%20Management/attachments).
Custom lifecycle request

You can define a custom lifecycle request in IBM Security Role and Policy Modeler for a process that you require.

To define a custom lifecycle request, see the “Creating a custom lifecycle request” topic in the IBM Security Role and Policy Modeler Information Center.

The installation of IBM Security Role and Policy Modeler version 1.1 Fix Pack 1 or later copies a “Review” process template for role approval into the samples directory of the IBM Security Role and Policy Modeler HOME installation directory. The name of the sample template file is IBM_Security_Role_Lifecycle_Management_Custom_Review_Example.twx. See the “Deploying the sample Review process application” topic in the IBM Security Role and Policy Modeler Information Center.

Test and production environments

With Role Lifecycle Management, you can work with a test environment and then move to a production environment.

You can use the Process Center for process application customization, testing, and deployment. You can have one or more Process Servers connected to the Process Center. Follow these steps:

1. Import the Role Lifecycle Management template into the Process Designer.
2. Optional: Customize the template based on your business requirements and test it on the Process Center.
3. Optional: Install the process application on a Process Server for testing.
4. Install the process application on a Process Server for production.

Typically, the Process Center is used for process development and testing, and the Process Server is used for testing, staging, and production.

If your production and test environments have different environment and configuration settings, correct these settings for your production Process Server before installing your process application on the production server.


User registries

Role Lifecycle Management requires proper setup of your user registries for Business Process Manager and IBM Security Role and Policy Modeler.

The role analysts and role owners that work with Role Lifecycle Management must be defined in registries using one of the following scenarios:

- File-based registries for IBM Security Role and Policy Modeler and Business Process Manager
User and group definitions and authorization

Role Lifecycle Management requires specific types of users, such as administrators, role analysts, and role owners.

In addition to the users, in Business Process Manager you can define a participant group in a process application to give a group of users the same authorities to access certain tasks or steps. Two participant groups are predefined in Role Lifecycle Management process. See “Configuring a runtime participant group” in the IBM Security Role and Policy Modeler Information Center.

Administrators

The following types of administrators are required for the Role Lifecycle Management process:

System administrator

System administrators are in the `tw_admins` group in Business Process Manager.

Authorities

System administrators have full access to Role Lifecycle Management assets.

Responsibilities

System administrators install, configure, and administer Role Lifecycle Management. They also troubleshoot system errors.

Role Lifecycle Management administrator

A Role Lifecycle Management process can be configured for a Role Lifecycle Management administrator to receive email notification of errors.

Authorities

These administrators receive error notification. If you add the administrator user ID to the `tw_admins` group, these administrators have full access to the Role Lifecycle Management assets.

Responsibilities

These administrators troubleshoot Role Lifecycle Management system errors.

Role analyst

Role analysts can optionally be defined in a group in either an LDAP registry or in the Business Process Manager file-based registry, depending on your setup.

Authorities

Role analysts have the authority to submit a lifecycle request and terminate a process.
Responsibilities
Role analysts mine roles, design role models, and submit roles for approval.

Role owner
Role owners are users with an owner identity record on a role in IBM Security Role and Policy Modeler.

Authorities
Role owners have the authority to approve role requests.

Responsibilities
Role owners review roles and decide whether to approve or reject role definition updates or additions.

Reports
IBM Security Role and Policy Modeler provides reporting capabilities for administrators and role analysts to generate reports on various data.

The reports are created by Tivoli Common Reporting, which uses IBM Cognos®. Tivoli Common Reporting provides several types of reports that are ready for IBM Security Role and Policy Modeler. You can also create custom reports using the Cognos Report Studio. A Cognos Framework Manager model accelerates creating custom reports. For more information about reports, see the “Report administration” topic in the IBM Security Role and Policy Modeler Information Center.
### Table 2. Reports for IBM Security Role and Policy Modeler

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Report Description</th>
<th>Initial Release</th>
<th>Fix Pack 1 or later</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Imported and Committed Data (formerly Operations report) | The administrator who imports data into IBM Security Role and Policy Modeler can use this report to review the data of a specific type from a specific import session. For example, the administrator can run the report for identities in a session and see the values of different attributes of those identities. Similarly, the administrator can run the report on the Identity and Entitlement database to view the details of a specific type of data committed to Identity and Entitlement database. | ✔️              | ✔️                   | • “Imported and Committed Data report” topic  
• “Generating Imported and Committed Data reports” topic |
Table 2. Reports for IBM Security Role and Policy Modeler (continued)

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Report Description</th>
<th>Initial Release</th>
<th>Fix Pack 1 or later</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td>Permissions reports give a permission-centric view of the model. For a model, the report shows if the users are entitled or directly assigned to the permission or get the permission through the role membership. The reports also provide information about the roles that have this permission.</td>
<td>✔</td>
<td>✔</td>
<td>• “Permissions report” topic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• “Generating Permissions reports” topic</td>
</tr>
<tr>
<td>Roles by Owners (formerly Roles report)</td>
<td>Roles by Owners reports provide unified details of roles in a model. They are used to get feedback from stakeholders on the modeled role grouped by the role owner. The details include the members in the role and permissions entitled by the role. Both directly assigned and inherited users and permissions are in the report. The reports also provide the membership qualifier of the role and the users who match the membership qualifier.</td>
<td>✔</td>
<td>✔</td>
<td>• “Roles by Owners report” topic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• “Generating Roles by Owners reports” topic</td>
</tr>
<tr>
<td>Report Name</td>
<td>Report Description</td>
<td>Initial Release</td>
<td>Fix Pack 1 or later</td>
<td>More Information</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| User Access                         | User Access reports provide a user-centric view of the data in IBM Security Role and Policy Modeler. For each of the selected users, the report shows the permissions that are directly assigned to the user and permissions inherited by the user. | ✓              | ✓                   | • “User Access report” topic  
• “Generating User Access reports” topic |
| All Roles in a Project by Owner     | All Roles in a Project by Owner reports show detailed information about roles. You can select roles based on project. The report shows role information based on the owner of the role. |                | ✓                   | • “All Roles in a Project by Owner report” topic  
• “Generating All Roles in a Project by Owner reports” topic |
| Role Details                        | The Role Details reports show detailed information about roles. You can select roles based on project and roles. |                | ✓                   | • “Role Details report” topic  
• “Generating Role Details reports” topic |
| Role Lifecycle History              | The Role Lifecycle History report shows lifecycle status and lifecycle history details for roles. You can select roles based on project. |                | ✓                   | • “Role Lifecycle History report” topic  
• “Generating Role Lifecycle History reports” topic |

See these additional resources about Tivoli Common Reporting:

**Tivoli Common Reporting Quick Start Service Offering**  
Meets the demand for customized Tivoli Common Reporting Cognos reports beyond the current report offering.
Tivoli Common Reporting developerWorks®
Provides the product documentation, task topics, featured videos, online
catalog of available product reports, message board and forum for
questions, and so on. See IBM Tivoli Common Reporting. You can also find
an introduction to Tivoli Common Reporting 2.1 from a link to YouTube:
http://www.youtube.com/watch?v=0zzIsZMGm-k

Information Center
You can find the Tivoli Common Reporting documentation from its
information center at http://publib.boulder.ibm.com/infocenter/tivihelp/
v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html.

Tivoli Common Reporting support
Find the support from http://www.ibm.com/support/entry/portal/
Overview/Software/Tivoli/Tivoli_Common_Reporting. It includes
downloads, troubleshooting, documentation, technical notes, fixes, and so
on.
Chapter 3. What's new

Fix Pack 1 and Fix Pack 2 provide updates to IBM Security Role and Policy Modeler Version 1.1.

Fix Pack 1 updates

IBM Security Role and Policy Modeler Version 1.1 Fix Pack 1 provides the following updates:

Table 3. What's new in Fix Pack 1

<table>
<thead>
<tr>
<th>Update</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Lifecycle Management integration with IBM Security Role and Policy Modeler</td>
<td>“Role Lifecycle Management” on page 23</td>
</tr>
<tr>
<td>Operating system requirements</td>
<td>“Operating system requirements” on page 45</td>
</tr>
<tr>
<td>Linux library requirements</td>
<td>“Prerequisite libraries for Linux” on page 46</td>
</tr>
<tr>
<td>Support for Microsoft Internet Explorer, Version 9.0</td>
<td>“Browser requirements” on page 51</td>
</tr>
<tr>
<td>Known issues</td>
<td>Chapter 6, “Known limitations, problems, and workarounds,” on page 55</td>
</tr>
<tr>
<td>Installing IBM Security Role and Policy Modeler Version 1.1 fix packs</td>
<td>“Fix pack installation tasks” topic</td>
</tr>
<tr>
<td>Troubleshooting the installation of IBM Security Role and Policy Modeler Version 1.1 fix packs</td>
<td>“Troubleshooting fix pack installation errors” topic</td>
</tr>
<tr>
<td>Enabling Role Lifecycle Management</td>
<td>“Configuring and enabling Role Lifecycle Management” topic</td>
</tr>
<tr>
<td>Performing administrative tasks for Role Lifecycle Management</td>
<td>“Role Lifecycle Management administration” topic</td>
</tr>
<tr>
<td>Troubleshooting problems in Role Lifecycle Management</td>
<td>“Troubleshooting Role Lifecycle Management” topic</td>
</tr>
<tr>
<td>New and updated reports</td>
<td>“Reports” topic</td>
</tr>
<tr>
<td>New messages for Role Lifecycle Management</td>
<td>“Role Lifecycle Management messages” topic</td>
</tr>
</tbody>
</table>

Fix Pack 2 updates

IBM Security Role and Policy Modeler Version 1.1 Fix Pack 2 provides the following updates:

Table 4. What's new in Fix Pack 2

<table>
<thead>
<tr>
<th>Update</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract and Load tools updates, including custom role attributes and URI information</td>
<td>“Extract and Load tools” topic</td>
</tr>
<tr>
<td>Known issues</td>
<td>Chapter 6, “Known limitations, problems, and workarounds,” on page 55</td>
</tr>
</tbody>
</table>
Table 4. What's new in Fix Pack 2 (continued)

<table>
<thead>
<tr>
<th>Update</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation of the full IBM Security Role and Policy Modeler Version 1.1.0.2 packaged with IBM Security Identity Manager 6.0</td>
<td>“Installing” topic</td>
</tr>
<tr>
<td>Installation instruction improvements</td>
<td></td>
</tr>
<tr>
<td>Support for Mozilla Firefox Version 10 ESR</td>
<td>“Browser requirements” on page 51</td>
</tr>
<tr>
<td>New messages</td>
<td>“Log messages” topic</td>
</tr>
</tbody>
</table>
Chapter 4. Getting started with IBM Security Role and Policy Modeler

This section describes some key concepts and gets you started with the initial tasks you must perform to work with IBM Security Role and Policy Modeler.

Starting and stopping IBM Security Role and Policy Modeler

When you start WebSphere® Application Server, IBM Security Role and Policy Modeler is automatically started.

Before you begin

Ensure that you meet all software requirements. See “Software requirements” on page 49 for detailed instructions.

Procedure

1. Start WebSphere Application Server with this command: WAS_PROFILE_HOME\bin\startServer.bat servername. Or, use this command: WAS_PROFILE_HOME/bin/startServer.sh servername.
2. To stop WebSphere Application Server, use this command: WAS_PROFILE_HOME\bin\stopServer.bat servername.

Logging on

To open the IBM Security Role and Policy Modeler home page, you must open a web browser, navigate to the correct address, and log on to the Tivoli Integrated Portal. You can establish either a secure (HTTPS) or unsecure (HTTP) connection to the Tivoli Integrated Portal.

Procedure

1. In the address bar, enter one of these addresses to display the Tivoli Integrated Portal logon.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a secure connection,</td>
<td>https://host_name:port/ibm/console where default HTTPS transport port: 16311, WebSphere administrative console secure port: 16316</td>
</tr>
</tbody>
</table>

where host_name is the name or IP address of the system where IBM Security Role and Policy Modeler is installed.

2. In the User ID field, enter your user ID.
3. In the Password field, enter your password.
4. Click Log in. The IBM Security Role and Policy Modeler home page is displayed.
What to do next

After you have logged on to the Tivoli Integrated Portal, you can start working with IBM Security Role and Policy Modeler. See “Understanding the user interface.”

Understanding the user interface

This section describes major tasks you can perform with IBM Security Role and Policy Modeler.

Modeling Roles and Policies
Use the modeler to create, visualize, and analyze roles, role hierarchies, and separation of duty constraints.

Reporting
Use reports to view details of roles and identify permissions assigned to users.

Importing Identity and Entitlement Data
The modeling and analytical tools use the imported data to provide optimized roles and policies.

Home page and navigation pane
Use the home page and navigation pane to launch IBM Security Role and Policy Modeler tasks.

You can open or close the navigation pane by clicking the Show Navigation arrow or Hide Navigation arrow in the middle of the pane borders.

Note: The home page and navigation pane display only those nodes to which you have access. Depending on the roles in which you are defined in Tivoli Integrated Portal, you might not have access to certain tasks. If you do not have access to a task, it does not display in the navigation. To gain access to a particular task, contact your system administrator. See the “User administration” topic in the IBM Security Role and Policy Modeler Information Center.
Modeling roles and policies

The user interface for role modeling consists of these windows: Projects, Role and Policies, and Role Properties.

Projects window
Use this window to search and manage current projects.

Roles and Policies window
Use this window as the main role editing interface that provides both table and graphical views of the roles in the opened project. An analysis pane is available on this window for detailed role analysis.

Role Properties window
Use this window to edit the properties of a role. You can select a role from the Roles and Policies window and edit it.

Projects window
Use this window to create, edit, delete, export, and recalculate projects. The table on this window lists the names of the projects and shows their status, roles, and policies. Clicking the status link gives you more details about the status of the project.
Roles and Policies window

Use this window to plan and develop roles and policies. The window is divided into three sections:

Summary pane

This pane provides basic information about the project you are currently modeling. From the summary pane, you can open other windows to:

- Edit the project name and description
- View and update the project scope
- View additional statistics about the project

Roles pane

This pane provides a searchable view of roles in the project. The Roles pane has two views. You can switch between the views by clicking the appropriate icon:

- Click the icon to display the hierarchical view.
- Click the icon to display the table view.

From this pane, you can create, edit, copy, and delete roles. Use the Actions menu to perform these actions:

- Generate Roles
- Project Export
- Copy Roles into Project

A menu is available when you right-click on a role for performing actions on a specific role and selecting a role for analysis.
Use the **Undo** icon to roll back changes that were recently made to the model.

**Analysis pane**

The analysis pane provides a catalog of analysis tasks and a tab for the current analysis activity that you are performing.

---

**Roles hierarchical (graphical) view**

The role hierarchy view provides a graphical alternative to the table view. The same features are available as in the table view with additional features to help explore the role hierarchy graph. This view includes a collapsible outline section to show you where you are when zoomed into a large roll graph. It has **Zoom In** and **Zoom Out** icons, **Fit Contents** icon, and a search feature for highlighting roles in the graph. To switch to the table view click the **icon.**
Analysis pane

The Analysis pane contains the catalog and tab for current analysis task. The catalog provides a list of available analysis tasks. When you click an item in the analysis catalog, it switches to the analysis tab and displays the result.

A menu of recently viewed analysis tasks is also available in case you want to switch back to a previous analysis item. The analysis pane automatically opens when you select Analyze Role from the Roles and Policies window. You can use the arrows on the separator bar to toggle between a minimized, maximized, and split views of the analysis pane.

Note: To select a role to analyze, use the Analyze Role menu item in the menu in the Roles and Policies window. A role is also automatically selected for analysis when you open its properties in the Role Properties window.
Chapter 4. Getting started with IBM Security Role and Policy Modeler

Figure 6. Analysis catalog

Figure 7. Example analysis task
Note: The task What do members of this role have in common? supports drilling down through the graph and table links for additional analysis.

**Role Properties window**

Use this window to edit the properties of a role. Navigate the window by using the tabs to edit specific properties of the role. These properties include general information, hierarchy, membership, permissions, separation of duty policy, and additional information about the role.

As you edit the properties of the roles, changes are saved immediately. A saving indicator is displayed while the saving operation is in process. You can use the **Undo** icon on both the table and graphical views to roll back a change made while editing the role. As you update the role, the related properties are also updated. For example, if you add a new parent role, the content in the **Permissions** tab is updated to reflect any permissions inherited from the newly added parent.

Use the breadcrumbs at the top of the window to navigate back to the Roles and Policies window for further editing.

![Figure 8. Role Properties window](image)

**Note:** The analysis pane is available in the Role Properties window. Use the arrows on the separator bar to toggle between a minimized, maximized, and split view of the analysis pane.

**Reporting**

IBM Security Role and Policy Modeler provides reports for the system activities and resources.
IBM Security Role and Policy Modeler uses IBM Tivoli Common Reporting to create reports. To start this report tool, click **Report** from the IBM Security Role and Policy Modeler home page. For more information about this tool and instructions about how to use this tool, see the **Tivoli Common Reporting Information Center**.

**Importing Identity and Entitlement Data**

Use this window to manage import sessions, including creating, deleting, validating, and committing import sessions.

Click the link in the **Status** column to see status messages associated with the session and actions taken on the data session. The link in the **Messages** column provides detailed messages about the data in the selected session. Click the link in the **Session** column, or select a session and click the **Edit** icon to view and manage files uploaded to the session.

![Import Identity and Entitlement Data window](image)

**Figure 9. Import Identity and Entitlement Data window**

**Help and online documentation**

From the administrative console, you can access the online help for IBM Security Role and Policy Modeler and its related products.

You can use two methods to access the help and online documentation:

- Click **Help** in the upper right corner of the console window. A new window contains the IBM Security Role and Policy Modeler online help information.
- You can also access the following information in this Help window:
  - Tivoli Integrated Portal help
  - IBM electronic support website links
- Tivoli Common Reporting information center
  Click the titles in the left navigation pane to expand these areas.
- Click the ? icon in the upper right corner of an individual panel. A new window contains the help information for that specific panel.
Chapter 5. Hardware and software requirements

IBM Security Role and Policy Modeler has several hardware and software requirements.

Compatibility with other software

This section describes IBM Security Role and Policy Modeler compatibility with other software products.

If any of the following software is already installed on your computer, you can continue to use it, but be aware of the restrictions.

Table 5. IBM Security Role and Policy Modeler installation compatibility

<table>
<thead>
<tr>
<th>Installed software</th>
<th>Usage restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Integrated Portal version 2.2 installed</td>
<td>You can use an existing Tivoli Integrated Portal administrative user name and password during IBM Security Role and Policy Modeler installation. <strong>Restriction:</strong> If you have Tivoli Integrated Portal 2.2 installed with embedded WebSphere Application Server, you cannot use the existing software.</td>
</tr>
<tr>
<td>with WebSphere Application Server</td>
<td></td>
</tr>
<tr>
<td>Tivoli Common Reporting version 2.1.1 installed</td>
<td>You can use Tivoli Common Reporting to generate IBM Security Role and Policy Modeler reports. <strong>Restriction:</strong> If you have Tivoli Common Reporting 2.1.1 installed with embedded WebSphere Application Server, you cannot use the existing software.</td>
</tr>
<tr>
<td>with WebSphere Application Server</td>
<td></td>
</tr>
<tr>
<td>WebSphere Application Server version 7.0</td>
<td>You can use an existing WebSphere Application Server. <strong>Restriction:</strong> IBM Security Role and Policy Modeler does not support:</td>
</tr>
<tr>
<td></td>
<td>• Embedded WebSphere Application Server</td>
</tr>
<tr>
<td></td>
<td>• WebSphere Application Server Network Deployment Cluster environment</td>
</tr>
<tr>
<td></td>
<td>• 32-bit WebSphere Application Server on a 64-bit operating system</td>
</tr>
</tbody>
</table>

Operating system requirements

The IBM Security Role and Policy Modeler installation program checks for specific operating systems and levels before starting the installation process.

Table 6. Operating system requirements for IBM Security Role and Policy Modeler

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Patch or maintenance level requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX® 6.1 POWER® System 64-bit</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 6. Operating system requirements for IBM Security Role and Policy Modeler (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Patch or maintenance level requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 7.1 POWER System 64-bit</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2008 (Release 1) Standard Edition x86-32</td>
<td>None</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 (Release 1) Standard Edition x86-64</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2008 (Release 1) Enterprise Edition x86-32</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2008 (Release 1) Enterprise Edition x86-64</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2008 Release 2 Standard Edition x86-64</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2008 Release 2 Enterprise Edition x86-64</td>
<td>None</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0 x86-64</td>
<td>None</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.0 x86-64 *</td>
<td>None</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10.0 x86-64</td>
<td>None</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 11.0 x86-64</td>
<td>None</td>
</tr>
</tbody>
</table>

* Oracle on Red Hat Enterprise Linux version 6.0 is not supported.

**Prerequisite libraries for Linux**

The IBM Security Role and Policy Modeler installation program checks for specific operating systems and versions before starting the installation process. You must install the 32-bit and 64-bit versions of the libraries for Linux.

Tivoli Common Reporting installs 32-bit binary files. You must install both the 32-bit and 64-bit versions of the prerequisite libraries, even on the supported 64-bit Linux operating system.

The levels that are listed below are the latest available. You can use these versions or newer versions.

**Tip:** Run the prerequisite scanner to check for all the necessary libraries for Tivoli Common Reporting. The prerequisite scanner checks the configuration of your environment and detects missing prerequisites. You can download it from the IBM Support Site.

**Red Hat Enterprise Linux 6.0 and later**

IBM Installation Manager needs a set of 32-bit and 64-bit libraries to install on Red Hat Enterprise Linux 6.0 x86-64.

IBM Installation Manager is a 32-bit application and requires 32-bit versions of operating system libraries. These libraries are not installed on Red Hat Enterprise Linux 6.0 x86-64 by default.

Before you run IBM Installation Manager on Red Hat Enterprise Linux 6.0 x86-64, download and install these libraries:
Table 7. Prerequisite libraries for Red Hat Enterprise Linux 6.0 and later

<table>
<thead>
<tr>
<th>32-bit libraries</th>
<th>64-bit libraries</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtk2-2.18.9-6.el6.i686.rpm</td>
<td>gtk2-2.18.9-6.el6.x86_64.rpm</td>
</tr>
<tr>
<td>glib2-2.22.5-6.el6.i686.rpm</td>
<td>glib2-2.22.5-6.el6.x86_64.rpm</td>
</tr>
<tr>
<td>libXtst-1.0.99.2-3.el6.i686.rpm</td>
<td>libXtst-1.0.99.2-3.el6.x86_64.rpm</td>
</tr>
<tr>
<td>compat-libstdc++-33-3.2.3-69.el6.i686.rpm</td>
<td>compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm</td>
</tr>
<tr>
<td>pam-1.1.1-10.el6.i686.rpm</td>
<td>pam-1.1.1-10.el6.x86_64.rpm</td>
</tr>
<tr>
<td>openmotif22-2.2.3-19.el6.i686.rpm</td>
<td>openmotif22-2.2.3-19.el6.x86_64.rpm</td>
</tr>
<tr>
<td>libXp-1.0.0-15.1.el6.i686.rpm</td>
<td>libXp-1.0.0-15.1.el6.x86_64.rpm</td>
</tr>
<tr>
<td>libXmu-1.0.5-1.el6.i686.rpm</td>
<td>libXmu-1.0.5-1.el6.x86_64.rpm</td>
</tr>
</tbody>
</table>

SUSE Linux Enterprise Server 10 and SUSE Linux Enterprise Server 11

Download and install the following required libraries:
- compat-32bit
- compat-libstdc++
- openmotif-libs-32bit-2.2.4 or newer

Requirement for Tivoli Common Reporting and JDBC drivers

Cognos has some issues with JDBC drivers. In Red Hat Enterprise Linux, the /home/db2inst1/sqllib/java directory contains a file named db2java.zip.

Make a copy of the db2java.zip file, and rename the copied file to db2java.jar.

Requirement for Red Hat Enterprise Linux 6.1 and 6.2

After you unpack the IBM Security Role and Policy Modeler code into disk1/, the following directory structures exist:
- disk1/IBMTIP/cdimage/COI/PackageSteps/TCRCore_Upgrade/TCR.cognos.xml
- disk1/IBMTIP/cdimage/COI/PackageSteps/TCRCore/TCR.cognos.xml

Edit the cognos.xml file in both directories as follows:

For Red Hat Enterprise Linux 6.1
Change substring="6.0" to substring="6.1"

For Red Hat Enterprise Linux 6.2
Change substring="6.0" to substring="6.2"

Increase ulimit for open files

Before you install IBM Security Role and Policy Modeler, you must increase the ulimit to 2048 or higher for open files. For more information, see "Report server requirements" on page 52.

Error while loading shared libraries

You might get this error message related to shared libraries:
An error occurs because Cognos is linked to the openmotif library 2.2.X that contains a symbolic link to libXm.so.3. When libXm.so.3 library is upgraded, the openmotif library is upgraded as well. Newer versions of openmotif do not have the symbolic link to libXm.so.3, but rather to libXm.so.4, while Cognos requires libXm.so.3.

To resolve this error, create a new symbolic link. Run this command from the /usr/lib directory:

\[ \text{ln -s libXm.so.4 libXm.so.3} \]

For more information

For more information, see the following topics:


### Hardware requirements

IBM Security Role and Policy Modeler has these hardware requirements.

**Table 8. Hardware requirements for IBM Security Role and Policy Modeler**

<table>
<thead>
<tr>
<th>System components</th>
<th>Minimum values</th>
<th>Suggested values</th>
</tr>
</thead>
<tbody>
<tr>
<td>System memory (RAM)</td>
<td>4 gigabytes (see <a href="#">Note</a>)</td>
<td>8 gigabytes</td>
</tr>
<tr>
<td>Available system memory</td>
<td>500 MB</td>
<td>500 MB</td>
</tr>
<tr>
<td>Processor speed</td>
<td>Single 3.0 gigahertz Intel or pSeries® processor</td>
<td>Dual 4 gigahertz Intel or pSeries processors</td>
</tr>
<tr>
<td>Disk space for product and prerequisite products</td>
<td>30 gigabytes</td>
<td>40 gigabytes</td>
</tr>
</tbody>
</table>

**Note:**

- If you are using an AIX or Linux operating system, a minimum of 8 gigabytes of space is required. This requirement includes the combined RAM and swap space. For example, if the system has 4 gigabytes of RAM, a swap space of 4 gigabytes must be available to install the product.
- A computer that is running a client side browser must have one of the following minimum requirements:
  - 3.0 gigahertz Intel with a fast graphics controller
  - pSeries processor and 4 gigabytes of RAM

**Disk space requirements for installing IBM Security Role and Policy Modeler and its components**

The following table details the required disk space for installing IBM Security Role and Policy Modeler and its components.

**Table 9. Disk space requirements**

<table>
<thead>
<tr>
<th>Components</th>
<th>Disk space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>To install Tivoli Integrated Portal 1</td>
<td>4.5 GB</td>
</tr>
</tbody>
</table>
Table 9. Disk space requirements (continued)

<table>
<thead>
<tr>
<th>Components</th>
<th>Disk space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>To install Tivoli Common Reporting 1</td>
<td>2.5 GB 3</td>
</tr>
<tr>
<td>To install IBM Security Role and Policy Modeler 1</td>
<td>1.0 GB</td>
</tr>
<tr>
<td>For the IBM Security Role and Policy Modeler installation location</td>
<td>350 MB</td>
</tr>
<tr>
<td>For the system temporary directory 4</td>
<td>300 MB</td>
</tr>
</tbody>
</table>

1 Indicates that the space is required in the directory where WebSphere Application Server is installed.

2 Includes the disk space required for installations of these components: Tivoli Integrated Portal, Tivoli Common Reporting and IBM Security Role and Policy Modeler.

3 Includes the disk space required for installations of these components: Tivoli Common Reporting and IBM Security Role and Policy Modeler.

4 If temporary directory does not have enough space, you can change your system temporary directory to point to a drive that has enough space.
   - Microsoft Windows operating system: Reset TMP and TEMP system variable to point to the drive with enough space. For example, D:/temp.
   - AIX:
     mv /tmp /mnt/new/location/tmp
     ln -s /mnt/new/location/tmp /tmp

Important:
- You must have root user authority to run these commands.
- None of the files in temporary directory can be in use at the time you run these commands.
- If you create a folder to redirect tmp, the folder must have universal Read, Write, and Execute privileges (777).

Software requirements

IBM Security Role and Policy Modeler has software requirements that are described in the following topics.

WebSphere Application Server requirements

The following table lists the WebSphere Application Server requirements:

Table 10. WebSphere Application Server requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must install WebSphere Application Server version 7.0.</td>
<td>See the “Install WebSphere Application Server” topic in the IBM Security Role and Policy Modeler Information Center.</td>
</tr>
<tr>
<td>Note: If you are going to install the Load tool on a different computer than IBM Security Identity Manager, you must install the 32-bit WebSphere Application Server 7.0 Application Client. This applies to both 32-bit and 64-bit operating systems.</td>
<td></td>
</tr>
</tbody>
</table>
Table 10. WebSphere Application Server requirements (continued)

<table>
<thead>
<tr>
<th>Requirements</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must install WebSphere Application Server</td>
<td>You can either install the required Fix Pack from the product DVD or download from</td>
</tr>
<tr>
<td>Version 7.0 with Fix Pack 19 or later, including</td>
<td>the official IBM support website. See <a href="http://www.ibm.com/support">http://www.ibm.com/support</a>.</td>
</tr>
<tr>
<td>the WebSphere Java SDK updates.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** IBM Security Role and Policy Modeler does not support a 32-bit WebSphere Application Server on a 64-bit Windows operating system.

**Database server requirements**

IBM Security Role and Policy Modeler requires either DB2® or Oracle database.

You must install a database on a local computer or use remote database server.

Table 11. Database server requirements.

<table>
<thead>
<tr>
<th>Database server</th>
<th>Fix pack, and other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2 Enterprise Server Edition, Version 9.7</td>
<td>• Install fix pack 4 or later. If you need to work with IBM Security Role and Policy Modeler reports, you must:</td>
</tr>
<tr>
<td></td>
<td>• Install either the 32-bit or 64-bit DB2 client on the local system if you use a remote database server.</td>
</tr>
<tr>
<td>Oracle Database Enterprise Edition 11g Release 2 Fix Pack 2</td>
<td>• Minimum amount of memory (RAM) for IBM Security Role and Policy Modeler database on the Oracle database is 1.5 GB. The suggested amount is 2.0 GB or more.</td>
</tr>
<tr>
<td></td>
<td>• Minimum amount of disk space for IBM Security Role and Policy Modeler database on the Oracle database is 10 GB. The suggested amount is 20 GB.</td>
</tr>
<tr>
<td></td>
<td>If you need to work with IBM Security Role and Policy Modeler reports, you must:</td>
</tr>
<tr>
<td></td>
<td>• Install 32-bit Oracle client.</td>
</tr>
</tbody>
</table>

**Note:** IBM Security Role and Policy Modeler does not support a 32-bit database server on a 64-bit operating system. A 32-bit database server is only supported on a 32-bit operating system. Similarly, a 64-bit database server is only supported on a 64-bit operating system.

See the “Installing the database” topic in the IBM Security Role and Policy Modeler Information Center.

**Java Runtime Environment requirements**

The IBM Security Role and Policy Modeler server application runs in the WebSphere Application Server Java™ Runtime Environment. The WebSphere Application Server Fix Pack includes the required Java Runtime Environment version.

For more information about the required WebSphere Application Server version and Fix Pack, see “WebSphere Application Server requirements” on page 49.
IBM Security Role and Policy Modeler bundles Java Runtime Environment version 6.0.9.2 and is only used for the purpose of installing Tivoli Integrated Portal, Tivoli Common Reporting, and associated Fix Packs.

**Browser requirements**

The following table lists the supported browsers and browser versions. The supported browsers are not included with the product.

*Table 12. Browser requirements for IBM Security Role and Policy Modeler*

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Mozilla Firefox Version 10 ESR²,³</th>
<th>Microsoft Internet Explorer, Version 7.0</th>
<th>Microsoft Internet Explorer, Version 8.0</th>
<th>Microsoft Internet Explorer, Version 9.0¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 Intel x86, 32-bit</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Microsoft Windows 7 Intel x86, 64-bit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Vista Intel x86, 32-bit</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Windows Vista Intel x86, 64-bit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows XP Intel x86, 32-bit</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0 for Intel x86, 64-bit</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.0 for Intel x86, 64-bit</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.0 Desktop</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6.0 Desktop</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10.0 for Intel x86, 64-bit</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 11.0 for Intel x86, 64-bit</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 12. Browser requirements for IBM Security Role and Policy Modeler (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Mozilla Firefox Version 10 ESR</th>
<th>Microsoft Internet Explorer, Version 7.0</th>
<th>Microsoft Internet Explorer, Version 8.0</th>
<th>Microsoft Internet Explorer, Version 9.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUSE Linux Enterprise 10 Desktop</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE Linux Enterprise 11 Desktop</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes:
1. Microsoft Internet Explorer, Version 9.0 is supported on IBM Security Role and Policy Modeler version 1.1.0.1 (Fix Pack 1) or later.
2. Mozilla Firefox Version 3.6 is supported in IBM Security Role and Policy Modeler version 1.1.0.1 and 1.1.0.0. Mozilla Firefox Version 10 ESR is supported in IBM Security Role and Policy Modeler version 1.1.0.2.
3. If you plan to use Mozilla Firefox Version 10 ESR and view reports, ensure you install Tivoli Integrated Portal 2.2.0.7 and Tivoli Common Reporting 2.2.1 with interim fix 6.
4. Verify that your browser supports Adobe Flash Player. At the time of this publication, Windows 2008 64-bit does not support Adobe Flash Player.

Report server requirements

This topic describes the Tivoli Common Reporting and IBM Security Role and Policy Modeler report requirements.

Table 13. Report server requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Common Reporting server version 2.1.1</td>
<td>The installation process does one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Installs Tivoli Common Reporting version 2.1.1</td>
</tr>
<tr>
<td></td>
<td>• Provides an option for you to configure Tivoli Common Reporting if it is already installed</td>
</tr>
<tr>
<td></td>
<td>This interim fix is required if you use Mozilla Firefox Version 10 ESR to view reports.</td>
</tr>
<tr>
<td>32-bit database client</td>
<td>You must install the 32-bit database client to work with IBM Security Role and Policy Modeler reports.</td>
</tr>
<tr>
<td>32-bit and 64-bit versions of the prerequisite libraries for Linux</td>
<td>See <a href="#">Prerequisite libraries for Linux</a> or page 46.</td>
</tr>
<tr>
<td>Set open files to greater than 2048 for Tivoli Common Reporting installed on operating systems other than Windows.</td>
<td>To increase this value, run this command: <code>ulimit -n nnnn</code></td>
</tr>
<tr>
<td></td>
<td>where nnnn is the number of open files that you want. For example, <code>ulimit -n 2048</code></td>
</tr>
</tbody>
</table>
Prerequisites for Extract and Load tools

You can optionally install the Extract and Load tools by selecting Extract and Load Utilities for IBM Security Identity Manager during the installation.

You must install IBM Security Identity Manager version 6.0 to work with the Extract and Load utilities.
Chapter 6. Known limitations, problems, and workarounds

The following known limitations, problems, and workarounds apply to IBM Security Role and Policy Modeler Version 1.1.

- “Product installation”
- “Reports” on page 56
- “Attributes” on page 59
- “Import” on page 59
- “Copying roles” on page 60
- “Browsers” on page 60
- “User interface” on page 63
- “Extract and Load tool” on page 63
- “Performance” on page 64
- “Role Lifecycle Management” on page 64

Product installation

Product installation hangs if an unsupported special character is included in the Shared Resources Directory or Installation Directory names. If you include unsupported special characters in the names of Shared Resources Directory or Installation Directory, the product installation hangs. Apart from alphanumeric characters, the only supported special characters for Shared Resources Directory or Installation Directory are:

- "." (dot)
- "-" (hyphen)
- "_" (underscore)

Workaround

Use the supported special characters for Shared Resources Directory or Installation Directory.

You cannot assign the IBM Security Role and Policy Modeler roles to a user through installer. The installer fails to assign the IBM Security Role and Policy Modeler roles to a user under these conditions:

- Multiple users exist across different federated repositories of either Tivoli Integrated Portal or WebSphere Application Server with the same user ID.
- That user ID is provided as a IBM Security Role and Policy Modeler user.

Workaround

You can manually assign the IBM Security Role and Policy Modeler roles to a user. For information about assigning roles to a user, see the “Administering” topic in the IBM Security Role and Policy Modeler Information Center.

An insufficient disk space error occurs during the product installation even after you make the required space available.

When you specify the WebSphere Application Server location during the product installation, a warning message is displayed in the installer if:
There is not enough required space in the location to install IBM Security Role and Policy Modeler components.

The message does not disappear. The installer does not continue even after you make the required free space available in the WebSphere Application Server directory. The message is displayed even after you return to the previous panel and then navigate back to the current panel.

**Workaround**

You must enter the WebSphere Application Server path again. You can choose to either browse again or manually enter the path again.

The test connection operation for the specified database details might take a long time to respond.

While entering the database details in the database panel for IBM Security Role and Policy Modeler, the Test Connection operation might take a long time. One cause might be an incorrect DB2 port number at an input at Database Port Number. The amount of time for the response is also related to the TCP/IP timeout settings defined by the operating system.

**Workaround**

Wait for the Test Connection result. Provide the correct DB2 port number and then click Test Connection icon to validate credentials.

Disk space requirements vary between the Features and Summary panels.

Disk space requirements for IBM Security Role and Policy Modeler are inconsistent between the Features and Summary panels. The space requirements listed in the Features panel are not as accurate as the space requirements in the Summary panel. It appears as though there is enough space at the beginning of the installation process. However, at the end of the process, the installer reports that there is not enough space.

**Workaround**

Ensure that there is 100 MB more space available than the specified space in the Features panel.

IBM Security Role and Policy Modeler installation fails on a system with a Turkish locale.

The installation of IBM Security Role and Policy Modeler fails on a system with a Turkish locale.

**Workaround**

Change your system locale to English for the installation. When the installation completes, change the locale back to Turkish.

Reports

The Identity and Entitlement database operations report on user-to-permissions assignments fails on an Oracle database.

An error when attempting to run the report, with a message similar to:

UDA-SQL-0114 The cursor supplied to the operation "sqlOpenResult" is inactive.
UDA-SQL-0107 A general exception has occurred during the operation "open result".
ORA-06000: internal error code, arguments: [weirw: check ret val], [l], [l], [l], [l], [l], [l], [l], [l], [l]

**Solution:**

This error is a known problem when using Oracle Database 11gR2.0.2.0. This problem is fixed in Oracle Database 11gR2.0.3. The temporary workaround is to add a database trigger to the IBM Security Role and Policy Modeler Oracle database to set the Oracle
parameter ".replace_virtual_columns=false". Run the following from a SQL*Plus session connected to the IBM Security Role and Policy Modeler Oracle database with administrative privilege (that is, as SYSTEM or SYS):

```sql
-- BEGIN
CREATE OR REPLACE TRIGGER WORKAROUNDORA9965278 AFTER
LOGON ON DATABASE BEGIN
EXECUTE IMMEDIATE 'ALTER SESSION SET ".replace_virtual_columns=false";'
END;
/
-- END
```

This command adds the trigger named WORKAROUNDORA9965278 to the SYS schema. It implements the required workaround for every session that connects to the IBM Security Role and Policy Modeler Oracle database.

When you run the roles report with an Oracle database, the user information is missing.

Roles reports that are run with an Oracle database are missing role membership identities. The Tivoli Common Reporting and Cognos team is investigating this issue.

Solution:
Use PMR 87260 004 to track the solution for this issue.

Attempting to run two or more reports concurrently causes intermittent errors on Internet Explorer.


Increase asynchronous timeout in high user load environments.
This known limitation is documented in the following link. See [http://publib.boulder.ibm.com/infocenter/c8bi/v8r4m0/index.jsp](http://publib.boulder.ibm.com/infocenter/c8bi/v8r4m0/index.jsp) To locate the topic:
1. Enter Increase asynchronous timeout in high user load environments at Search.
2. Click Go.

Corrupted attribute names are displayed in reports in Chinese and Japanese languages.
Double-byte character set (DBCS) characters appear to be corrupted in reports.

Workaround
Configure reporting so that the data flow is in Unicode format.
1. On the Work with Reports page, click the Launch menu and click Administration.
2. Click Configuration to open the data source connection.
3. Click Security Modeling DataSource.
4. Under the Action column, click Set properties-Security Modeling DataSource.
5. On the Set properties-Security Modeling DataSource window, click Configuration.
6. In the Connection String field, click the pencil symbol to edit the connection string.
7. In the Collation Sequence field, type @UNICODE.
8. Click **OK**.
9. Run the report to verify that the text is no longer corrupted.

A Cognos error **QE-DEF-0285 The logon failed** occurs while testing the DB2 data source connection on Linux.


Edit the file `/etc/ld.so.conf` as described in the preceding link, and then run the `ldconfig` command from the `/sbin` directory.

**Prompt for values is restricted or unexpected when selecting the Save the Report option.**

The issue occurs in the following conditions:

- **Permissions report and Roles report**
  When you try to run the Permissions report, you click **Run with Options** in the **Action** column. Then you select the format, **Save the report Delivery**, and click **Run**. You can select only the project, and nothing else is visible for selection.

- **Operations report**
  When you try to run the Operations report, you click **Run with Options** in the **Action** column. Then you select the format, **Save the report Delivery**, and click **Run**. The prompt page is rendered to enter the input values for report. After you select the database option and report operation, a new page is displayed. You are prompted to enter different IDs, such as a file ID or session ID.

**Solution**


**An exception is logged when you open Tivoli Common Reporting as a non-administrator user.**

Opening Tivoli Common Reporting as a non-administrator user results in an exception being logged in the log file. The exception occurs even if the user has the necessary roles to work with the reports. For example, the following exception message might be logged in the log file for a user `rapmuser`:

```
CWWIM2008E The principal 'user:defaultWIMFileBasedRealm/uid=rapmuser, o=defaultWIMFileBasedRealm' is not authorized to perform the operation
```

It is a known problem and does not have an impact on the report generation functions. You can ignore this exception message.

**Operations reports have problems using an Oracle database with double-byte, Greek, or Russian locales.**

If you are using an Oracle database, do not select double-byte, Greek, or Russian locales for running operations reports. Use the English locale instead. This restriction applies to operations reports only.

**Using localhost in the Tivoli Integrated Portal console URL address causes a problem loading the Reports window.**

If `localhost` is used in the URL to connect to the server when accessing Tivoli Common Reporting for the first time after starting the server, any attempt to access the **Reports** window from a different computer with the correct host name or IP address fails.
Solution
Restarting WebSphere Application Server might resolve this problem. Alternatively, install Tivoli Common Reporting interim fix 2.1.1.0-TIV-TCR-IF0002. Or, go to [http://www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral) and search for the IBM Tivoli Common Reporting 2.1.1 fixes.

The User Access report does not show permissions assigned to the users.
The User Access report shows permissions that are assigned to the users directly or inherited through roles. This report shows only those permissions which are part of a project. This report does not show the permissions that are not part of a project.

On AIX, stopping the server for the Tivoli Integrated Portal profile might result in a Java memory dump.
Stopping the server for the Tivoli Integrated Portal profile might produce Java cores under the $TIP_HOME directory.

Solution

Attributes
Multivalued display attributes return only the first one found.
An attribute configured as a display attribute for an identity or a permission in schema CSV can contain multiple values for a user or permission. For example, if one of the user display attributes is a telephone number, and if John Smith has two telephone numbers, the table showing users contains only one of the telephone numbers. You can click the hyperlink on the user name to see all the values of such multivalued display attributes. A good practice is to choose attributes that have a single value for the custom display attributes.

Import
There are limitations while importing a CSV file that contains delimiter and escape sequence characters.
These two limitations are applicable for the data and schema import operation. In the following examples, the delimiter is a colon (:), and the escape sequence character is double quotation marks (").
- The space after the delimiter is invalid in any record. For example:
  - Space after the delimiter in the section definition:
    #Define Hierarchical Attributes: "hrdirectory://locationName"
  - Space after the delimiter in the attribute definition:
    "Source Record UID": "Person UID": "Person Name"
  - Space after the delimiter in the data record:
    "source://source1": "Source Name 1": "Source Description 1"
- The escape sequence in a string enclosed by same escape sequence is invalid. For example:
  'O'BRIEN: MIKE'
  or
  "3 feet 6" "

Chapter 6. Known limitations, problems, and workarounds 59
Uploading large data files before import operation might take an extended amount of time.

The process of uploading large files might take an extended amount of time depending upon these factors:

- The speed of the network.
- The speed of the client browser computer.
- The location of the application server.

Do not logout during the file upload process. An error occurs if you try to logout before the file upload process is complete.

Copying roles

An error occurs while copying a role with quotation marks in the role name.

An internal error occurs and copying a role operation fails when you perform these actions:

1. Selecting an existing role in the model containing quotation marks in the role name. For example, "Emergency Room" Nurse.
2. Clicking Copy Role.

Workaround

Remove the quotation marks from the role name that you want to copy.

There is a limitation on copying roles into the project.

Copying roles into the project operation might fail if the number of roles associated with separation of duty constraints directly or through hierarchy exceeds 100. On the IBM Security Role and Policy Modeler user interface, the status of the role copying operation changes to Role copy failed (Recalculation required). You can perform the Recalculate Project operation. After you perform the Recalculate Project operation, the project state changes back to Ready for editing to copy other roles in the project.

This issue does not occur if you installed IBM Security Role and Policy Modeler version 1.1 Fix Pack 1 or later. See the “Fix pack installation tasks” topic in the IBM Security Role and Policy Modeler Information Center.

Browsers

Internet Explorer 8 upload control shows C:\fakepath.

Internet Explorer 8 security feature hides the path of the selected file from the upload widget. The Internet Explorer security setting Include local directory path when uploading files to a server controls if the browser discloses the local path to the file upload widget. By default, this option is selected as Disabled, therefore the C:\fakepath string is shown in the file path name.

Workaround

If you do not want browser to hide the local path of the selected file, complete these steps:

1. Start Internet Explorer.
2. Click Tools > Internet Options.
3. On the Security tab, click the Internet icon, and then click Custom Level.
4. In the Include local directory path when uploading files to a server area, select Enable.
You cannot view the IBM Security Role and Policy Modeler home, project, and import windows on Internet Explorer running on a Windows remote system.

If you encounter this problem on Internet Explorer running on remote Windows system, add the IBM Security Role and Policy Modeler website to the Trusted sites list.

Workaround
To add a website to the Trusted sites list, complete these steps:
1. Start Internet Explorer.
2. Navigate to the website that you want to add to a specific security zone.
3. Click Tools > Internet Options.
4. On the Security tab, click the Trusted sites icon.
5. Click Sites.
6. At Add this website to the zone: review the website address.
7. Click Add.

Note: If the site is not a secure site (HTTPS), clear the Require server verification (https:) for all sites in this zone check box.
8. Click Close.

Using the Back button in the browser or Backspace key with the console can produce unexpected results.

Do not use the Back button in a browser or Backspace key to return to a previous page. Doing so might display a blank white page with a spinner. To reach a prior panel, you can follow the breadcrumb navigation available for some panels.

Workaround
To resolve this problem, close the page and relaunch it either from the home page or from the navigation area.

The Report window starts in minimized page size in some Internet Explorer browsers.

You might get this problem intermittently in some Internet Explorer browsers.

Workaround
Maximize the panel by clicking the arrow icon in the upper right corner and selecting maximize.

The users and permissions views in the Selected Users and Selected Permissions windows are not keyboard accessible.

After you create a project and add new users and permissions to the project, you can view the project details. You can also edit the project scope by adding more users and permissions. When you click View All to open the Selected Users or Selected Permissions windows, you can view all users and permissions entered. However, when you try to view a specific user or permission by pressing the Enter or Space key, you cannot open the user or permission view. Instead, you must use a mouse click to open the user or permission view and see the details of that user or permission.

Using the Tab key to select items on the home page is not clearly indicated by the dotted line of the focus indicator.
When you use the Tab key to navigate through the home page in Internet Explorer 8, the dotted line of the focus indicator does not clearly indicate which item or area you are selecting.
Workaround
Use Mozilla Firefox 3.6.22 and later as your browser option.

The page listing links are not keyboard accessible using Internet Explorer version 8.
When you work with the roles with the Tivoli Integrated Portal console, the links to display items on each page and the page number are not accessible in Internet Explorer 8.

Workaround
Use Mozilla Firefox 3.6.22 as your browser option.

The default setup for HTTP server with Secure Sockets Layer (SSL) does not work with IBM Security Role and Policy Modeler topology items.
When you use IBM HTTP Server in front of IBM Security Role and Policy Modeler, the communication between IBM HTTP Server and WebSphere Application Server must use the SSL protocol. You must configure the web server plug-in for SSL. If this configuration is not done correctly, role hierarchy and other topology views might fail with the following error:

Web Browser:
ATKRST100E An unexpected error occurred. The error message is as follows: 'java.lang.RuntimeException: javax.net.ssl.SSLException: Unrecognized SSL message, plaintext connection?'.

Workaround
Set up the SSL communications between the HTTP Server plug-in and WebSphere Application Server. For information about this configuration, see [http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_httpserv2.html](http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_httpserv2.html).

Using localhost on a system with Internet Protocol version 6 (IPv6) addresses causes issue in loading the hierarchical view.
While accessing IBM Security Role and Policy Modeler using IPv6, loading of a hierarchical or topology view fails. The graphical representation of user and permission hierarchical attribute values is not displayed while:
• Creating a modeling project
• Modifying the scope of an existing modeling project
• Creating or modifying a membership qualifier for a role

An IllegalArgumentException is recorded in the WebSphere Application Server System.out file.

Workaround
Either access Tivoli Integrated Portal by using the fully qualified host name or with the IPv4 loopback address 127.0.0.1.
This issue does not occur if you installed IBM Security Role and Policy Modeler version 1.1 Fix Pack 1 or later. See the “Fix pack installation tasks” topic in the IBM Security Role and Policy Modeler Information Center.

The hierarchical view does not work on Internet Explorer 9 on Windows 2008 64-bit.

Workaround
A browser that supports Adobe Flash Player is required for the hierarchical view to be displayed.
The help window is empty on Internet Explorer 9.
When you click on the help icon for IBM Security Role and Policy Modeler, the help window is empty. This problem occurs only in Internet Explorer 9.

Workaround
Enable the META REFRESH option in Internet Explorer 9. To enable the option, complete these steps:
1. Click Tools > Internet Options.
2. In the Internet Options window, click the Security tab.
3. Click the Custom level button.
4. In the Security Settings window, scroll to the Allow META REFRESH option in the Miscellaneous section.
5. Click Enable for the Allow META REFRESH option.
6. Click OK, and then click Apply.

User interface
Attempting to access the console produces Unable to connect to the server error. The following scenario might produce the Unable to connect to the server error when trying to access the IBM Security Role and Policy Modeler console:

- Installed IBM Security Role and Policy Modeler Version 1.1 Fix Pack 1 or later.
- Rolled back Fix Pack 1 or a later fix pack.
- Uninstalled Tivoli Integrated Portal 2.2 Fix Pack 5.
- Started the IBM Security Role and Policy Modeler console.

Also, in the TIP_PROFILE_HOME/logs/server_name/SystemOut.log you might find the following error:

WSWS7011E: The configuration for the com.ibm.security.modeling.rest.war application module cannot load correctly.

This means that there is a problem with the file that runs the IBM Security Role and Policy Modeler server.

Workaround
Install the IBM Security Role and Policy Modeler server. See the “Installing IBM Security Role and Policy Modeler server” topic in the IBM Security Role and Policy Modeler Information Center.

Extract and Load tool
An exception message is logged multiple times on the command prompt when the Extract tool starts.

When the Extract tool starts, the following exception message is logged multiple times on the command prompt:

NMSV0307E: A java: URL name was used, but Naming was not configured to handle java: URL names. The likely cause is a user in error attempting to specify a java: URL name in a non-J2EE client or server environment. Throwing ConfigurationException.

Ignore this exception because it does not have an impact on the Extract tool functions.

Multiple values assigned to a single value custom role attribute produces a schema error.
IBM Security Identity Manager supports single and multiple value custom
role attributes. However, IBM Security Role and Policy Modeler considers all attributes to be multiple value custom role attributes. Therefore, if you define multiple values for a single value custom role attribute, then the Load tool fails with a schema violation error for that role.

Ensure that you assign only one value for a single value custom role attribute in IBM Security Role and Policy Modeler.

**Performance**

At times, stopping Tivoli Integrated Portal using the `stopTCRserver.sh` script can result in core files being produced.

To locate the core and trace files, look in the `$TCR_HOME/cognos/bin64` directory.

**Workaround**

Clean up the Java core dump to prevent the hard drive from filling up.

**Role Lifecycle Management**

Use unique users and groups across Business Process Manager federated repositories.

If you set `ldapEnabled` to true, and have both an internal role analyst group and an LDAP user group assigned as the members of the RoleAnalyst participant group, only users in the LDAP user group can successfully submit the role approval request.

Users in the internal role analyst group can start the role approval request, but the request will not be submitted successfully and the following message exception will be logged in the `System.out` file:

```
CWLLG2041E: TeamWorksJavaScriptException created non-nested.
Error: [TeamworksException name='TypeError',
message='TypeError: Cannot read property "fullName" from null',
line=0, pos=0 nested=<none>]
```

Also, if the same user ID exists in both the Business Process Manager internal registry and LDAP registry, you will have a problem adding the user to the Role Analyst role.

**Workaround**

Configure either an internal registry or an LDAP user registry for Business Process Manager users, but not both. Specify the type of configuration by setting the environment variable `ldapEnabled` to `true` or `false`.

Even if you have enabled one type of registry, if another type of registry exists, ensure that you do not have any user IDs or group names that are the same in both registries. The names must be unique across both registries.

This limitation exists only for Business Process Manager registries and not IBM Security Role and Policy Modeler registries.

**Reinstallation of Business Process Manager might cause a database error.**

If you uninstall Business Process Manager and attempt to reinstall it without first creating a new database, you will receive the following error:

```
The database is already in use. Choose an empty database.
```

This error displays while reinstalling Business Process Manager when you are on the panel for setting up the existing database.
**Workaround**

Create a new database when you reinstall Business Process Manager. Do not re-use the same database you used for the initial installation.

**Business Process Manager user interface content does not display properly.**

Under certain circumstances in Business Process Manager, the browser does not display the user interface content correctly. For example, in the Process Portal some icons do not display properly. This problem can happen independent of the type of browser you are using. The issue is the result of not specifying a fully-qualified host name during Business Process Manager installation or if the etc/hosts file does not correctly resolve the host name to the fully-qualified host name.

**Workaround**

To fix this problem, use one of the following methods:

- In Network Properties, add the server domain to the list of search domains, specifying the IP address and fully-qualified host name.
- In the system hosts file, include the IP address and fully-qualified host name. On a Windows operating system, the hosts file is located in Windows\system32\drivers\hosts.
- In the Process Portal URL, use the IP address instead of the host name.
- In the Process Portal URL, specify the host name that matches the value you entered during the installation for the URL. For example:
  - If you used the fully-qualified domain name, use that domain name value in the browser URL. For example, specify http://host9.example.com:9080/portal.
  - If you used the host name, use just the host name in the browser URL. For example, specify http://host9:9080/portal.


**Business Process Manager user interface content displays mixed content warning in Microsoft Internet Explorer 8.**

If you are using Internet Explorer 8, the user interface of Business Process Manager might display a warning message that says This page contains both secure and nonsecure items. Do you want to display the nonsecure items? This happens if the web pages come from the Business Process Manager server and you are accessing the HTTPS protocol.

**Workaround**

Enable viewing of the mixed content without a warning message by adjusting the Internet Explorer settings:

1. Click **Tools > Internet Options > Security**.
2. Select a zone of either **Local intranet** or **Trusted sites**, depending on your setup.
3. Click **Custom level**.
4. In the Security Settings pop-up window, locate the **Miscellaneous** section of the settings and then the **Display mixed content** setting.

5. Click **Enabled** to display mixed content.

6. Click **OK** to save the setting.

7. Click **OK** to save the internet options.

**Cannot select approvers from the list in Business Process Manager.**

Under certain circumstances in Business Process Manager, the approver select widget on the role approval request form does not work properly. That is, you cannot select an approver from the list. This problem can happen independent of the type of browser you are using.

**Workaround**

To fix this problem, specify the host name that matches the value you entered during the installation for the Process Portal URL. For example:

- If you used the fully-qualified domain name, use that domain name value in the URL. For example, specify `http://host9.example.com:9080/portal`.
- If you used the host name, use just the host name in the URL. For example, specify `http://host9:9080/portal`.

**Test Connection button on the AIX Business Process Manager installation panel does not work.**

During the AIX installation of IBM Business Process Manager Standard, if you click the **Test Connection** button, it does not work. This button is on the panel titled “Install a Process Server”.

**Workaround**

You will not be able to test the connection during this installation process. Click **Next** to proceed with the installation.

**Unspecified error after submitting a lifecycle request in IBM Security Role and Policy Modeler.**

You might receive the following errors if you submit a Role Lifecycle Management request within the IBM Security Role and Policy Modeler console:

**Unspecified error occurred**

This error displays in the email message sent to the `tw_admin` user ID and it also displays in the Business Process Manager Process Inspector.

```
[1/27/12 13:16:33:559 EST] 0000002e exception
E com.ibm.websphere.wim.security.authz.AccessException
CWWIM2008E The principal 'user:defaultWIMFileBasedRealm/uid=rapmuser,
o=defaultWIMFileBasedRealm' is not authorized to perform the operation
'GET PersonAccount' on 'uid=rapmuser,o=defaultWIMFileBasedRealm'
```

This error displays in the IBM Security Role and Policy Modeler `systemOut.log` file.

```
<ns1:messageString xsi:type="xs:string"> Unable to load the driver manager library ( libdb2.so ).</ns1:messageString>
<ns1:messageString xsi:type="xs:string"> The operating system returned an error message ( libdb2.so: cannot open shared object file: No such file or directory ).</ns1:messageString>
```

These errors display in the Business Process Manager `systemOut.log` file.
Workaround

To resolve this problem, export the LD_LIBRARY_PATH before starting WebSphere Application Server. See “Setting up a user environment for working with reports” in the IBM Security Role and Policy Modeler Information Center.

Unable to log in to Process Designer or console after starting the Business Process Manager server.

If you are using the Role Lifecycle Management feature, you might not be able to log in to the Business Process Manager Process Designer or console with the LDAP server administrator user ID. This problem occurs if LDAP is set as the user repository and the password for the LDAP server administrator account has expired.

Following is an excerpt from the exception in the Business Process Manager SystemOut.log file:

```java
com.ibm.wsspi.sib.core.exception.SIAuthenticationException:
CWSIP0301E: Unable to authenticate user admin when creating a connection to secure messaging engine
IBM-NGTI0X1U8NSNode01.server1-PROCSVR.IBM-NGTI0X1U8NSNode01Cell.Bus on bus
PROCSVR.IBM-NGTI0X1U8NSNode01Cell.Bus.
at com.ibm.ws.sib.processor.impl.MessageProcessor
    .createConnection(MessageProcessor.java:766)
at com.ibm.ws.sib.ra.inbound.impl.SibRaMessagingEngineConnection
    .createConnection(SibRaMessagingEngineConnection.java:1187)
at com.ibm.ws.sib.ra.inbound.impl.SibRaMessagingEngineConnection
    .<init>(SibRaMessagingEngineConnection.java:262)
```

Workaround

To resolve this problem, change the setting on the LDAP server administrator account to **Password never expires** and restart the LDAP server.

Business Process Manager file-based registry user IDs are case sensitive.

If you are using the Business Process Manager file-based registry for Role Lifecycle Management, you will get the following log in error if you do not specify the correct case of the user ID:

```text
Cannot login. Please check your user name and password.
```

The message in the SystemOut.log file is:

```
The password match failed for the 'name' principal name.
```

For example, if the Business Process Manager registry contains the user ID roleAnalyzer, entering roleAnalyzer will not be found in the registry when you attempt to log in.

Workaround

Enter the exact Business Process Manager log in ID specified in the registry, including the proper case.

Having IBM Security Role and Policy Modeler and Business Process Manager servers on the same system without single sign-on might cause a user to get logged out of the IBM Security Role and Policy Modeler console

The following scenario causes a user to get logged out of the IBM Security Role and Policy Modeler console:

- Both IBM Security Role and Policy Modeler and Business Process Manager servers are installed on the same computer.
- Single sign-on is not configured between the two servers.
- You have logged into the IBM Security Role and Policy Modeler console.
You have logged into the Business Process Manager Portal as a different user, and then logged out.

You get logged out of the IBM Security Role and Policy Modeler console.

**Workaround**

Follow these steps to avoid this problem:

1. Create a DNS alias for the system.
2. Access the IBM Security Role and Policy Modeler console using the alias you defined in step 1. For example, specify:
   
   `http://DNS_alias:16311/ibm/console`

**In the console, the Roles and Policies window does not list the Submit Request action in the menu.**

If you have installed IBM Security Role and Policy Modeler Fix Pack 1, or later, and configured and enabled the Role Lifecycle Management feature, you might have a problem accessing the Submit Request action. Specifically, if you are on the Roles and Policies window, select one or more roles, and click the Actions menu, the Submit Request action might not show up in the list.

**Workaround**

In your browser, clear the cookies and cache and start the IBM Security Role and Policy Modeler console again.

**"Cannot calculate next primary key" error in role analyst email after submitting roles for approval.**

After a role analyst submits roles for approval, a return email might list an error for one or more of the submissions that says “Cannot calculate next primary key”.

**Workaround**

See the information in the following topic to fix the problem:


**Cannot call method "isInParticipantGroup" of null error after submitting roles for approval.**

After a role analyst submits roles for approval, the approval process might fail with the following message in the IBM Security Role and Policy Modeler SystemOut.log file:

CTJR6923E Failed to submit the Business Process Manager lifecycle request for request type: APPROVAL, process short name: IBMRLP2, and process name: Role Approval Request

Business Process Manager logs the following type of exception in the SystemOut.log file:

CWLLG2229E: An exception occurred in an EJB call. Error:

"TypeError: Cannot call method "isInParticipantGroup" of null"

Script (line 0):

1 : // Initialize objects
2 : tw.local.roleRequest = new tw.object.RoleRequest();

```
Step (Initialize)]
com.lombardisoftware.core.TeamWorksDecoratingException:
Runtime error in script ("TypeError" 0:0).TypeError:
Cannot call method "isInParticipantGroup" of null
Script (line 0):
1 : // Initialize objects
2 : tw.local.roleRequest = new tw.object.RoleRequest();
```
**Workaround**

Ensure that the user with the submitter user ID exists in the Business Process Manager registry.
Appendix A. Conventions used in this information

This information uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface conventions

This information uses the following typeface conventions.

**Bold**
- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicoloumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations:**)
- Keywords and parameters in text

**Italic**
- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a **point-to-point line**)
- Emphasis of words and letters (words as words example: "Use the word that to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter L.")
- New terms in text (except in a definition list): a **view** is a frame in a workspace that contains data.
- Variables and values you must provide: ... where **myname** represents....

**Monospace**
- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

**Bold monospace**
- Command names, and names of macros and utilities that you can type as commands
- Environment variable names in text
- Keywords
- Parameter names in text: API structure parameters, command parameters and arguments, and configuration parameters
- Process names
- Registry variable names in text
- Script names
Definitions for HOME and other directory variables

The table contains default definitions that are used in IBM Security Role and Policy Modeler information center and guides. These definitions represent the HOME directory level for different product installation paths.

You can customize the HOME directory for your specific requirement. The default directory installation locations in the following table are provided for either administrator or root users.

For non-administrator or nonroot users, replace the following paths with `user_home`:
- Windows operating system: `drive:\Program Files`
- Linux: `/opt`
- UNIX, or AIX: `/usr`

Table 14. Home directory variable definitions

<table>
<thead>
<tr>
<th>Path variable</th>
<th>Default definitions</th>
<th>Description</th>
</tr>
</thead>
</table>
| SM_HOME              | • Windows operating system: `C:\Program Files\IBM\SecurityModeler`
                       | • Linux, UNIX or AIX: `/opt/IBM/SecurityModeler`                              | The base directory that contains IBM Security Role and Policy Modeler and documentation. |
| DB_HOME              | • Windows operating system: `C:\Program Files\IBM\SQLLIB`
                       | • Linux: `/opt/ibm/db2/V9.7`
                       | • UNIX or AIX: `/opt/IBM/db2/V9.7`                              | The default DB2 home directory. |
| WAS_HOME             | • Windows operating system: `C:\Program Files\IBM\WebSphere\AppServer`
                       | • Linux: `/opt/IBM/WebSphere/AppServer`
                       | • UNIX or AIX: `/usr/IBM/WebSphere/AppServer`                              | The default WebSphere Application Server home directory. |
| TIP_PROFILE_HOME     | • Windows operating system: `WAS_HOME\profiles\TIPProfile`
                       | • Linux, UNIX, or AIX: `WAS_HOME\profiles\TIPProfile`                              | The default Tivoli Integrated Portal home directory. |
Table 14. Home directory variable definitions (continued)

<table>
<thead>
<tr>
<th>Path variable</th>
<th>Default definitions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCR_COMPONENT_HOME</td>
<td>• Windows operating system: C:\Program Files\IBM\WebSphere\AppServerComponents\TCRComponent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux: /opt/IBM/WebSphere/AppServerComponents/TCRComponent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UNIX or AIX: /usr/IBM/WebSphere/AppServerComponents/TCRComponent</td>
<td>The Tivoli Common Reporting home directory.</td>
</tr>
</tbody>
</table>
Appendix B. Accessibility features for IBM Security Role and Policy Modeler

Accessibility features help users who have a disability, such as restricted mobility, use information technology products successfully.

**Accessibility features**

The following list includes the major accessibility features in IBM Security Role and Policy Modeler:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but not activated by touch
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Role and Policy Modeler information center and its related publications are accessibility-enabled.

**Keyboard navigation**

This product allows operation with a keyboard.

**Interface information**

**Hierarchical view is not keyboard accessible**

The hierarchical view of the role and policy model is not keyboard accessible. However, the table view of the role and policy model is keyboard accessible. Customers who require a keyboard-accessible role and policy model can use the table view on the Roles and Policies window.

**Analysis graphs are not keyboard accessible**

There is an alternative representation of the same data in the form of in and out tables in the analysis windows.

**Supported browsers for accessibility**

Mozilla FireFox 3.6.22.

Microsoft Internet Explorer 8. For information about known accessibility issues for this browser, see the "Known limitations, problems, and workarounds" topic in the IBM Security Role and Policy Modeler information center.

**Reports are accessible**

Reports are accessible in HTML and PDF format. For more information, see the "Assistive technologies for reports" topic in the IBM Security Role and Policy Modeler information center.

**Opening online help within IBM Security Role and Policy Modeler**

For Microsoft Internet Explorer, press Alt+6+Enter.

For Mozilla FireFox, press Shift+Alt+6.
IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features contained in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing, or distributing application programs that conform to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample
programs are provided "AS IS", without warranty of any kind. IBM shall not be
liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must
include a copyright notice as follows: © (your company name) (year). Portions of
this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp.
2004, 2012. All rights reserved.

If you are viewing this information softcopy, the photographs and color
illustrations might not appear.

**Trademarks**

The following terms are trademarks of the International Business Machines
Corporation in the United States, other countries, or both: [http://www.ibm.com/

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of
Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems,
Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered
trademarks or trademarks of Adobe Systems Incorporated in the United States,
and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other
countries.

The Oracle Outside In Technology included herein is subject to a restricted use
license and can only be used in conjunction with this application.
requirements (continued)
WebSphere Application Server requirements 49
role management cycle 5
role analyst description 27
role approval request description 25
role generation 1
Role Lifecycle Management
description 23
process diagram 23
process flow 24
role modeling analysis tools 21
role owner description 27
Role Properties window 37
role statistics 21
role UID 17
roles
role description 16
role name 16
role owner 16
role parent 16
role type 16
role UID 16
Roles and Policies window 37
rule description 17
rule UID 17

S
schema attributes 10, 13
schema import 19
Security Identity Manager roles 23
security process integration 3
security roles 1
separation of duty constraint 1
separation of duty constraints 1, 19
cardinality 17
role UID 17
rule description 17
rule UID 17
software compatibility 45
source record UID 13
staging database 20
supported operating systems 45

T
technical training viii
terminology vii
terminology web site vii
test environment 26
Tivoli Integrated Portal
logging on 35
training viii
troubleshooting viii
known limitations 55
typeface conventions 71

U
ulimit 52
user identities 13