IBM Security Role and Policy Modeler
Version 1 Release 1

Planning Guide

SC22-5407-03

IBM Security Role and Policy Modeler
Version 1 Release 1

Planning Guide

SC22-5407-03

October 2012

This edition applies to version 1.1.0.2 of IBM Security Role and Policy Modeler and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

About this publication

IBM Security Role and Policy Modeler Planning Guide describes how to plan for IBM® Security Role and Policy Modeler deployment, installation, configuration, and data management.

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 Product Overview Guide*, GC27-2795
- *IBM Security Role and Policy Modeler Planning Guide*, SC22-5407
- *IBM Security Role and Policy Modeler Installation and Configuration Guide*, SC27-2743
- *IBM Security Role and Policy Modeler Administration Guide*, SC27-2796
- *IBM Security Role and Policy Modeler Troubleshooting Guide*, GC27-2797
- *IBM Security Role and Policy Modeler Message Guide*, GC27-2744
- *IBM Security Role and Policy Modeler Reference Guide*, SC27-2798
- *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
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.security.modeling.doc_1.1.0.2/ic-homepage.htm site displays the information center welcome page for this product.

IBM Security Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Publications Center
The http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications you need.

IBM terminology website

The IBM Terminology website consolidates terminology from product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

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 29.

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. Planning

Planning is an activity in which you make decisions that affect one or more subsequent activities.

Preinstallation planning is covered in the "Installing" section of the IBM Security Role and Policy Modeler Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.security.modeling.doc_1.1.0.2/landing/landing-installing.htm.

Aside from the planning that precedes product installation, system administrators encounter decisions that are smaller in scale, but can have ramifications if not planned well. These decisions are outlined in this Planning section.

Planning roadmap

Using this roadmap, you can complete the planning steps for installation and configuration for IBM Security Role and Policy Modeler.

Chapter 2, “Deployment overview,” on page 3

Chapter 3, “Planning for installation,” on page 9

Chapter 4, “Planning for configuration,” on page 13

Chapter 5, “Planning for data management,” on page 15

Chapter 6, “Planning for security,” on page 17

Chapter 7, “Planning for performance,” on page 21

Chapter 8, “Planning for maintenance,” on page 23

Chapter 2. Deployment overview

Use this information to help you decide the type of deployment that you want to install. IBM Security Role and Policy Modeler is a component of and is typically used with IBM Security Identity Manager. IBM Security Role and Policy Modeler can, however, be used as a stand-alone application.

IBM Security Role and Policy Modeler is a set of WebSphere® applications running on the same WebSphere single server. These applications have a dependency on a DB2® or an Oracle database. WebSphere Application Server and a supported database are prerequisite installations.

IBM Security Role and Policy Modeler includes two Tivoli® shared components, Tivoli Integrated Portal and Tivoli Common Reporting. In most cases, the installation and configuration of IBM Security Role and Policy Modeler manages the installation, configuration, and uninstallation of these components. However, if these components are already installed on supported platform configurations, use the existing deployments.

IBM Security Role and Policy Modeler also comes with two stand-alone utilities that are installed optionally. These utilities automate extracting data from the IBM Security Identity Manager server and loading modeled roles and policies into the IBM Security Identity Manager server.

IBM Business Process Manager

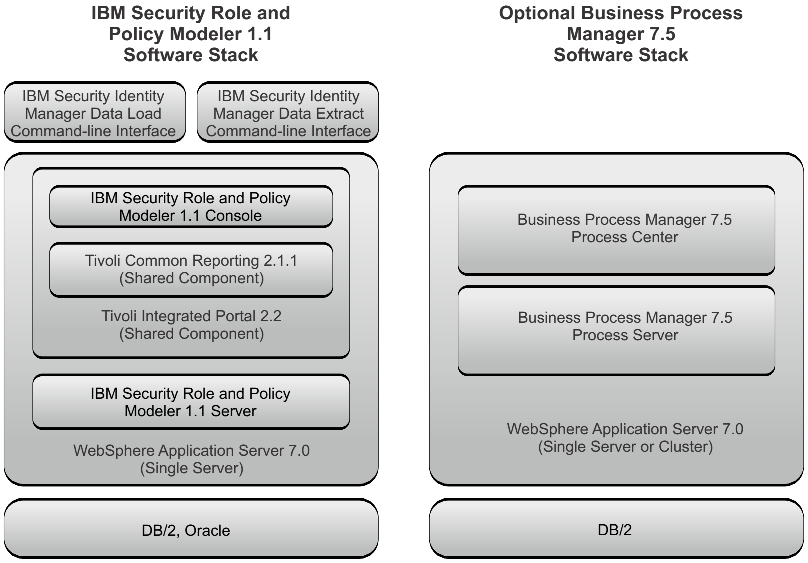
IBM Security Role and Policy Modeler includes an optional business processing component, Business Process Manager 7.5, for approving role and policy designs. Business Process Manager consists of two WebSphere applications. One application is for designing approval processes. The other application is a server for running the process.

The installation of WebSphere Application Server and a supported database are prerequisites for Business Process Manager.

For Business Process Manager planning information and installation instructions, see the Business Process Manager Information Center at http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r5m1/index.jsp.

IBM Security Role and Policy Modeler software stacks

The following illustration shows the IBM Security Role and Policy Modeler software stack and the optional IBM Business Process Manager software stack.


IBM Security Role and Policy Modeler 1.1 Software Stack
Optional Business Process Manager 7.5 Software Stack
IBM Security Identity Manager Data Load Command-line Interface
IBM Security Identity Manager Data Extract Command-line Interface
IBM Security Role and Policy Modeler 1.1 Console
Tivoli Common Reporting 2.1.1 (Shared Component)
Tivoli Integrated Portal 2.2 (Shared Component)
IBM Security Role and Policy Modeler 1.1 Server
WebSphere Application Server 7.0 (Single Server)
DB/2, Oracle
Business Process Manager 7.5 Process Center
Business Process Manager 7.5 Process Server
WebSphere Application Server 7.0 (Single Server or Cluster)
DB/2

Typical deployments

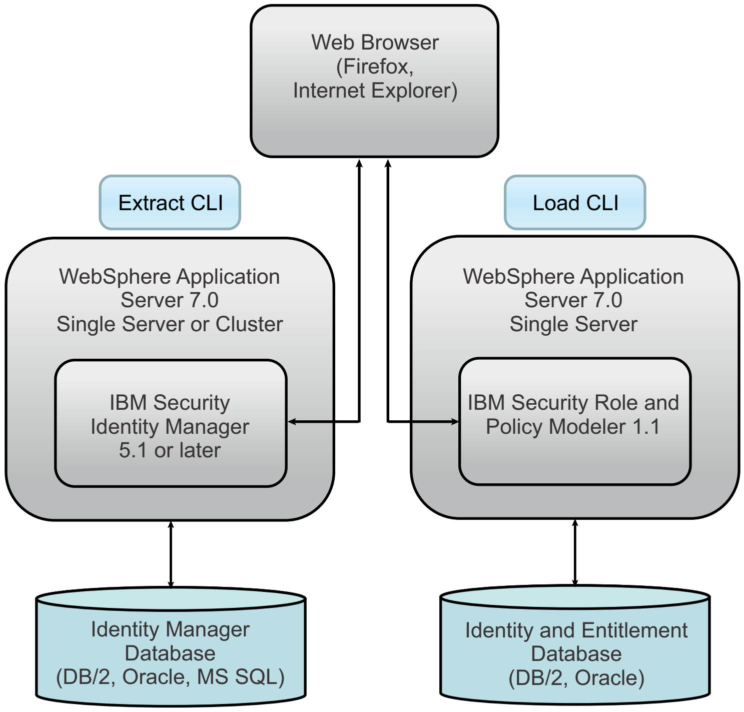
The following illustrations show the deployment architecture of IBM Security Role and Policy Modeler.

Typically, IBM Security Role and Policy Modeler is installed as a component of an existing IBM Security Identity Manager deployment. You can install the optional IBM Business Process Manager component bundled with IBM Security Role and Policy Modeler to manage role design approvals.

Typical deployments with IBM Security Identity Manager

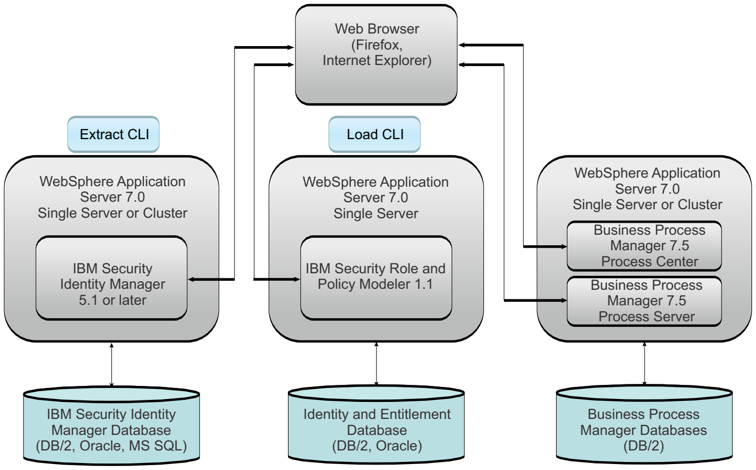
The following illustration shows IBM Security Role and Policy Modeler as part of a IBM Security Identity Manager deployment.

Typical deployment as a component of IBM Security Identity Manager


Web Browser (Firefox, Internet Explorer)
Extract CLI
Load CLI
WebSphere Application Server 7.0 Single Server or Cluster
IBM Security Identity Manager 5.1 or later
WebSphere Application Server 7.0 Single Server
IBM Security Role and Policy Modeler 1.1
Identity Manager Database (DB/2, Oracle, MS SQL)
Identity and Entitlement Database (DB/2, Oracle)

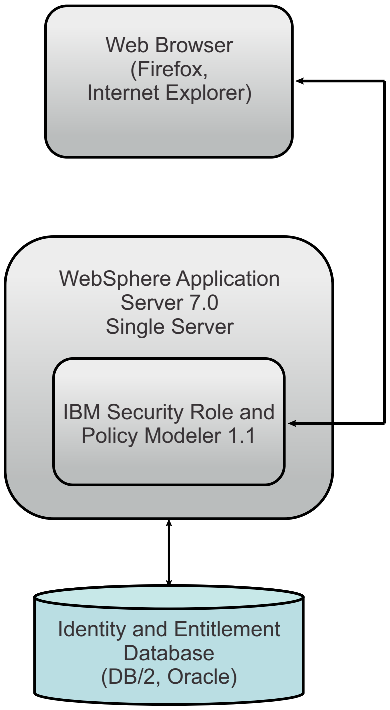
The following illustration shows IBM Security Role and Policy Modeler with the optional Business Process Manager component as part of a IBM Security Identity Manager deployment.

Deployed as a component of IBM Security Identity Manager with optional Business Process Manager 7.5


Web Browser (Firefox, Internet Explorer)
Extract CLI
Load CLI
WebSphere Application Server 7.0 Single Server or Cluster
IBM Security Identity Manager 5.1 or later
WebSphere Application Server 7.0 Single Server
IBM Security Role and Policy Modeler 1.1
WebSphere Application Server 7.0 Single Server or Cluster
Business Process Manager 7.5 Process Center
Business Process Manager 7.5 Process Server
IBM Security Identity Manager Database (DB/2, Oracle, MS SQL)
Identity and Entitlement Database (DB/2, Oracle)
Business Process Manager Databases (DB/2)

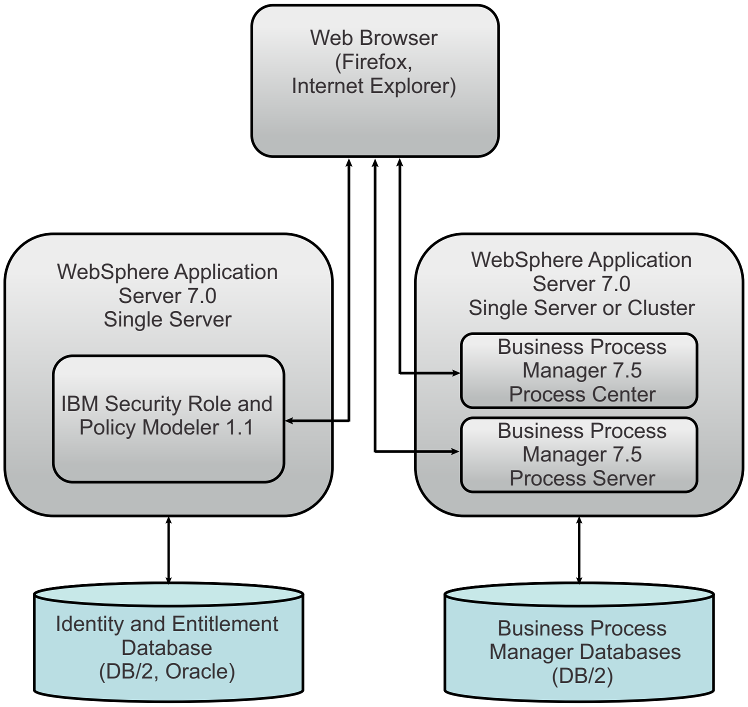
The following illustration shows IBM Security Role and Policy Modeler as a stand-alone deployment.

Standalone deployment


Web Browser (Firefox, Internet Explorer)
WebSphere Application Server 7.0 Single Server
IBM Security Role and Policy Modeler 1.1
Identity and Entitlement Database (DB/2, Oracle)

The following illustration shows IBM Security Role and Policy Modeler with the optional Business Process Manager component as a stand-alone deployment.

Standalone deployment with optional Business Process Manager 7.5



Chapter 3. Planning for installation

Before installing IBM Security Role and Policy Modeler, you must make certain decisions. For example, you must decide which supported database you want to use in your environment. You must also understand what additional steps you must perform if you use existing components.

For detailed information about planning for your installation, see "Installation overview and scenarios" in the IBM Security Role and Policy Modeler Information Center.

Interoperability considerations

Ensure that you understand the hardware and software requirements for IBM Security Role and Policy Modeler. You must also understand the compatibility of IBM Security Role and Policy Modeler with the existing software on your system.

For hardware and software requirements, see "Hardware and software requirements" in the IBM Security Role and Policy Modeler Information Center.

For compatibility with existing software on your system, see "Compatibility with other software" in the IBM Security Role and Policy Modeler Information Center.

J2EE application specifications

The only supported application server is WebSphere Application Server 7.0 deployed as a single server.

You can install the single server from the IBM Security Identity Manager bundled copy of WebSphere Application Server Network Deployment Manager.

Installation considerations

The IBM Security Role and Policy Modeler installation wizard collects data and presents some choices before beginning the product installation.

You must have specific information ready before beginning the installation for IBM Security Role and Policy Modeler. Review the information in the following sections to ensure that you gathered the appropriate information.

Installing as an administrator or a non-administrator

A user who has an ID with or without administrative authority can install IBM Security Role and Policy Modeler.

If you install IBM Security Role and Policy Modeler using a non-administrative ID, the ID for the installation process must have the necessary permissions. These permissions are required by the file systems and operating system services to make the system changes needed to install IBM Security Role and Policy Modeler.

See "Installing as a non-administrator" in the IBM Security Role and Policy Modeler Information Center.

Installation packages

Using the IBM Installation Manager, select the IBM Security Role and Policy Modeler package and the subpackage of version 1.1 or later.

Choosing an installation directory

You can use the default installation directory for the IBM Security Role and Policy Modeler installed image, or you can choose your own installation directory.

On Windows systems with User Access Control enabled, the default directory is a virtualized directory associated to the user ID performing the installation. If a virtualized directory is used, the user ID must perform the installation program with the **Run as Administrator** option. Alternatively, User Access Control can be deactivated before installation.

See "Installing as a non-administrator" in the IBM Security Role and Policy Modeler Information Center.

Windows 32-bit versus 64-bit installations

You can install WebSphere Application Server for Windows operating systems as a 32-bit or 64-bit application.

Decide which version you want to use before installing IBM Security Role and Policy Modeler. The 64-bit version is preferred because role analysis and data mining operations are more efficient with the larger memory space.

Note: The 64-bit version of IBM Security Role and Policy Modeler is required on 64-bit Windows systems. The 32-bit version of WebSphere is not supported on 64-bit Windows systems.

Features to install

The installation wizard prompts you to select the program features to install. You can install any or all of the features.

IBM Security Role and Policy Modeler console
The J2EE application for the web-based user interface component.

IBM Security Role and Policy Modeler server
The J2EE application for the server component.

Extract and Load Utilities for IBM Security Role and Policy Modeler
The command-line component for managing transfer of modeling data between the modeling database and the IBM Security Identity Manager operational database.

You must install the console and server components on the same system and into the same installation of WebSphere Application Server. You can install the Extract and Load utilities on the same system as the server and console or on one or more different systems.

WebSphere Application Server location and component deployment

You must choose the location of WebSphere Application Server that hosts the application.

IBM Security Role and Policy Modeler uses Tivoli Integrated Portal. Tivoli Integrated Portal is a shared Tivoli component for user interface consoles across multiple products.

The installation process:

- Creates a profile for the program based on the Tivoli Integrated Portal component.
- Deploys the console and server application into the Tivoli Integrated Portal profile.
- Installs IBM Tivoli Common Reporting, which is a Tivoli shared component for reporting and report design. Tivoli Common Reporting is installed as a component of the WebSphere Application Server installation.

If another product is installed that also uses the Tivoli Integrated Portal and Tivoli Common Reporting:

- IBM Security Role and Policy Modeler does not install these shared components into the WebSphere Application Server.
- IBM Security Role and Policy Modeler is installed into the existing deployment and reuses the shared component. If you do not want to reuse the shared components, choose another location for WebSphere Application Server.

Required user IDs and passwords

IBM Security Role and Policy Modeler needs two sets of credentials for the installation, configuration, and initial login.

Tivoli Integrated Portal administrator ID and password

This user ID is required for the system management of:

- The Tivoli Integrated Portal console
- The Tivoli Common Reporting settings
- User management
- Management of the WebSphere Application Server settings

If this ID exists in the WebSphere user registry, then the credentials are verified. If this ID does not exist in the WebSphere user registry, then a credential is created for the Tivoli Integrated Portal administrator.

The Tivoli Integrated Portal administrator ID:

- Administers the Tivoli Integrated Portal
- Manages and views the IBM Security Role and Policy Modeler reports

By default, the Tivoli Integrated Portal administrator does not have access to the Modeling and Import portlets.

IBM Security Role and Policy Modeler user ID and password

The IBM Security Role and Policy Modeler user ID:

- Is the primary and first user ID that can log in to the IBM Security Role and Policy Modeler console
- Can be created in the WebSphere user registry, or an existing user ID can be used
- Has the authority to use the console for modeling roles and for importing identity and entitlement data
- Can use the Tivoli Common Reporting console
- Cannot change the application or system settings

After installation, the authority of this user ID can be changed in the Tivoli Integrated Portal console for managing roles. You can add users with the ability to scope the authority to any combination of consoles.

- Modeling portlet
- Import portlet
- Reporting portlet
- System Settings portlet

For more information, see "User administration" IBM Security Role and Policy Modeler in the Information Center.

Configuring the database and database connections

You can configure the database connection information during the IBM Security Role and Policy Modeler installation or after it is completed.

You cannot log on to IBM Security Role and Policy Modeler until you configure the database. You must create and configure the database and the database tables before configuring the database connection.

You can choose either IBM DB2 or Oracle for the database provider. For information about configuring the databases during installation, see "Installing the database" in the IBM Security Role and Policy Modeler Information Center.

Configuring Tivoli Common Reporting

You can configure Tivoli Common Reporting during the installation or afterward. You can choose to configure Tivoli Common Reporting after installation if either of these conditions are met:

- Tivoli Common Reporting is installed on a different WebSphere Application Server.
- Tivoli Common Reporting is administered by a different person.

Reporting is not enabled until the database connections for Tivoli Common Reporting are configured. See "Creating a data source for reporting" in the IBM Security Role and Policy Modeler Information Center.

Completing installation after database configuration

After the installation wizard collects the database information, review the installation parameters on the summary page and continue with the installation. Success or failure is indicated at the end of the installation process. You can review the log files before exiting IBM Installation Manager. The completion summary page also indicates the login URL for IBM Security Role and Policy Modeler.

Chapter 4. Planning for configuration

You can configure components either during or after the installation. If you configure IBM Security Role and Policy Modeler components and related software later, you must perform additional tasks.

For help in deciding which configuration option you want to use, see "Determining database and report configuration actions" in the IBM Security Role and Policy Modeler Information Center.

The major component of IBM Security Role and Policy Modeler that requires configuration is the database component. Other WebSphere and system configurations are built into the installation process.

For information about configuring the IBM Security Role and Policy Modeler database, see "Supported configurations after installing" in the IBM Security Role and Policy Modeler Information Center.

Product customization considerations

You can customize certain aspects of the product based on how you intend to use it. There are a number of things that you must consider before you customize the product to ensure that the results meet your needs.

IBM Security Role and Policy Modeler supports these types of customization:

Custom attributes on users, permissions, roles, and separation of duty constraints

You can extend each of the four major objects with custom schema for attributes.

See "Attributes" in the IBM Security Role and Policy Modeler Information Center.

Custom attributes displayed on the user interface for users and permissions

The table views of users and permissions can display up to five additional attributes that provide easy access to additional data about users and permissions.

Role Type

After installation, these default role types exist:

- Business role
- Application role

Through schema customization, you can add new role types and delete default role types. An enterprise can have as many role types as required by the organization.

For details about customization, see the "Understanding the data" and "Import schema" topics in the IBM Security Role and Policy Modeler Information Center.

In addition to the customization that can be done through schema management, you can perform the task **How do member attributes compare to membership in the role?**. You can specify up to five attributes of users and permissions for analytics and analytical displays from the role analysis catalog. Set the unique identifiers and priorities for the five attributes in the `securityModeling.properties` file. The default location of this file is *WAS_HOME*`\profiles\TIPProfile\installedApps\TIPCell\isc.ear\com.ibm.security.modeling.rest.war\WEB-INF`. If not otherwise specified, IBM Security Role and Policy Modeler uses the first five analysis attributes specified in the schema committed by the import process.

For more information about the analysis catalog attributes, "Attributes" in the IBM Security Role and Policy Modeler Information Center.

Chapter 5. Planning for data management

There are some considerations for planning data management.

For an overview of data management, see "Understanding the data" in the IBM Security Role and Policy Modeler Information Center.

If IBM Security Role and Policy Modeler is not the exclusive source of modeling data, then the enterprise must plan a custom schema. Considerations for the custom schema are:

- Data to be imported
- Sources of the data
- Number of users
- Permissions
- Roles
- Constraints and mappings to be imported
- How to manage the data into CSV files for import

You can put all data from all sources into a single file and upload that file into an import session. However, that option might not be practical because the data needed for modeling increases over time. Dividing the data by data type and by sources is one way to manage loading large amounts of data. For sources with large data sets, such as a human resources directory, you can logically divide the source into multiple sources. For example, a human resources source can be logically divided into all users with family names A through L as one source. Another source can be all users with family names M through Z.

Committing the data that was loaded from the import staging database into the Identity and Entitlement database locks out role analysts from working with projects. The lockout continues until the commit process is completed. Consider when and how often to commit the data. Committing large amounts of data, such as committing all data from all sources in a single import session, can take a long time. Committing an import session containing a subset of sources or data from logical sources might be faster. Consider committing data as part of an agreed-upon maintenance schedule to avoid conflicts with the availability of the Identity and Entitlement database for modeling.

Chapter 6. Planning for security

There are different aspects of security planning. For example, there is physical security and system security.

Identifying the security policy

A security policy is a set of rules that apply to activities for the resources that belong to an organization. This policy serves as the basis for security planning when you use IBM Security Role and Policy Modeler.

Planning for physical security

Ensure that you understand the requirements of a physically secure environment.

When you prepare to install IBM Security Role and Policy Modeler, you can create a physical security plan by asking these questions:

- Where is this software going to fit in my environment?
- Are the locations for the hardware or systems running IBM Security Role and Policy Modeler physically secure?
- What additional equipment is necessary to secure the systems?
- What type of protection is necessary to ensure that IBM Security Role and Policy Modeler can be quickly recovered after a fire or power interruption?

Planning for system security

Controlling user access and permissions and maintaining information integrity are the items to consider when planning for system security.

Security design overview

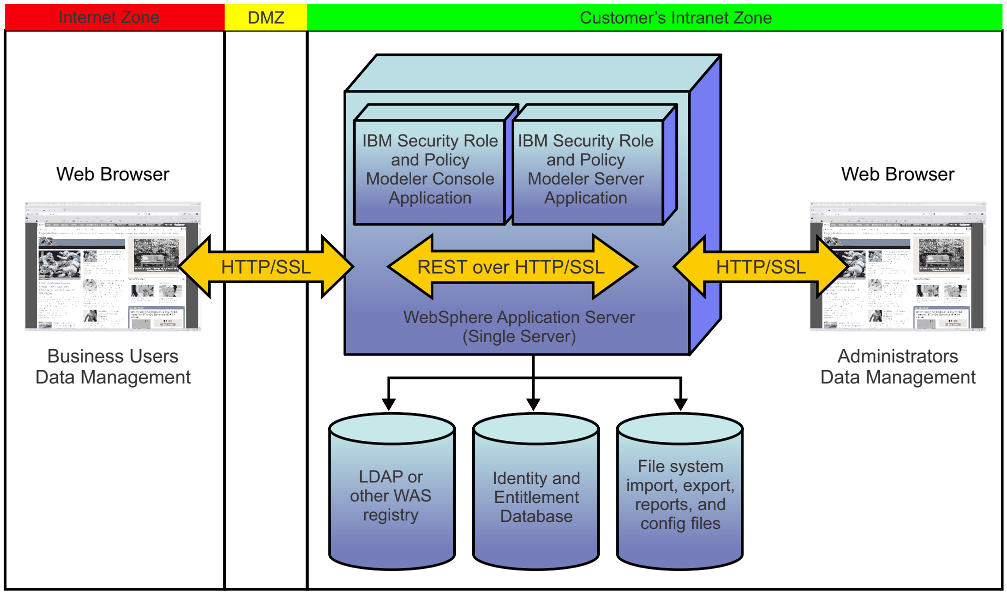
IBM Security Role and Policy Modeler security uses the security features of WebSphere and managed resources.

IBM Security Role and Policy Modeler is a WebSphere application that relies on WebSphere security for:

- Transport security
- Authentication
- Role-based authorization
- Single signon (SSO) by using lightweight third-party authentication (LTPA)

IBM Security Role and Policy Modeler relies on the security of the database and file systems for securing the data in their respective repositories. Appropriate transport layer security is used for accessing data in the middleware repositories, such as LDAP over SSL.

Security design


Internet Zone
DMZ
Customer's Intranet Zone
Web Browser
Business Users
Data Management
HTTP/SSL
IBM Security Role and Policy Modeler Console Application
IBM Security Role and Policy Modeler Server Application
REST over HTTP/SSL
WebSphere Application Server
(Single Server)
HTTP/SSL
Web Browser
Administrators
Data Management
LDAP or other WAS registry
Identity and Entitlement Database
File system import, export, reports, and config files

Use of existing user registries

IBM Security Role and Policy Modeler uses the WebSphere user registry configuration (WebSphere UserRegistry and Virtual Member Manager) to integrate your existing user registries.

Such registries might include:

- LDAP
- Operating system registries
- File registries
- Federated registries
- Custom registries

Authorization and access management

The IBM Security Role and Policy Modeler `.war` deployment files define roles as part of the deployment descriptors.

These defined roles are:

- `Application Administrator`
- `Role Analyst`

Additionally, Tivoli Common Reporting defines a role, `tcrPortalOperator`, for controlling access to reporting features.

You can use the Tivoli Integrated Portal console to map these roles directly to users or to groups in your registry.

Table 1. Defined roles

Role name	Description	Authorized actions
`Application Administrator`	Manages the IBM Security Role and Policy Modeler server and data.	• Change the modeling data schema and customization • Import data into the staging area • Commit data into the Identity and Entitlement database
`Role Analyst`	Manages and exports models.	• Browse catalog of models • View models and statistics • Create and delete models • Change roles and policies in the models
`tcrPortalOperator`	Runs, views, and manages reports.	• Run reports • View reports • Save reports and report templates • Customize reports

The default IBM Security Role and Policy Modeler user created during the installation of IBM Security Role and Policy Modeler is assigned all three of these roles.

Ready-to-use security configuration

IBM Security Role and Policy Modeler is deployed into an existing WebSphere deployment.

Tivoli Integrated Portal creates a profile with global security enabled.

Chapter 7. Planning for performance

The IBM Security Role and Policy Modeler database is designed to process complex queries. These queries analyze and mine the role model data.

IBM Security Role and Policy Modeler analytics and data mining can discover relationships between users, permissions, and roles. IBM Security Role and Policy Modeler includes some database indexing for tuning the initial installation. As the amount of data encapsulated in tables increases and custom attributes are introduced, you might want to further tune the system. Re-evaluating and retuning the system based upon updated profile data might improve overall system performance.

For information about planning and maintaining the system related to scale and performance, see the *IBM Security Role and Policy Modeler 1.1 Performance Tuning Guide* in developerWorks® at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Identity%20Manager/page/Related%20Resources.

Chapter 8. Planning for maintenance

As you plan for the hardware and software installations, plan for their eventual maintenance. For example, plan to back up information in case you need to restore data.

Planning a fix management strategy

When you plan for using the hardware and software product, also plan for the eventual installation and use of fix packs. For example, develop a plan for how to determine which fix packs are available for your product. Plan for how to obtain, install, and use the required fix packs.

IBM Security Role and Policy Modeler provides fix packs on a periodic basis to update product code for a number of reasons.

Check Fix Central for information about available fix packs for IBM Security Role and Policy Modeler: http://www.ibm.com/support/fixcentral/.

Fix packs for IBM Security Role and Policy Modeler are installed through the Update feature of IBM Installation Manager. Fix packs can be installed from local copies of the fix pack files.

Planning for service and support

Preventive service planning can save you time when working with support.

If a problem occurs, you might be asked to start traces and supply the IBM support team with log and trace files.

For information about starting tracing and locating log and trace files, see "Troubleshooting and support" in the IBM Security Role and Policy Modeler Information Center.

Planning for backup and recovery

A maintenance plan involves developing a backup and recovery plan for any configuration data or user data for the product. Having a thorough backup and recovery plan for IBM Security Role and Policy Modeler ensures that you can maintain high availability. For example, you need to develop a backup and recovery plan for IBM Security Role and Policy Modeler as part of your overall disaster recovery planning.

Ensure that you back up the database that contains the IBM Security Role and Policy Modeler import session data and all the project and modeling data. Depending on the type of database installed with IBM Security Role and Policy Modeler, consult the DB2 or Oracle documentation for information about backup and restore operations.

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, multicolumn 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 2. Home directory variable definitions

Path variable	Default definitions	Description
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 2. Home directory variable definitions (continued)

Path variable	Default definitions	Description
TCR_COMPONENT_HOME	• Windows operating system: `C:\Program Files\IBM\WebSphere\AppServerComponents\TCRComponent` • Linux: `/opt/IBM/WebSphere/AppServerComponents/TCRComponent` • UNIX or AIX: `/usr/IBM/WebSphere/AppServerComponents/TCRComponent`	The Tivoli Common Reporting home directory.

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/legal/copytrade.shtml

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.

Index

Printed in USA

SC22-5407-03