RSA Access Manager 6.1 SP4
Planning Guide

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers**:** **www.rsa.com**

Trademarks

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to RSA, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-party licenses

This product may include software developed by parties other than RSA. To view the text of the license agreements applicable to third-party software in this product, click **Help > About** in the Administrative Console.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

RSA notice

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

Contents

Preface

About This Guide

This guide describes the high-level architecture and features of RSA Access Manager. It is intended for planners and other trusted personnel. Do not make this guide available to the general user population.

RSA Access Manager Documentation

For more information about RSA Access Manager, see the following documentation:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest version of the Release Notes is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Getting Started. Lists what the kit includes (DVD, CDs, licenses and documentation), specifies the location of documentation on the DVD, and lists RSA Customer Support web sites.

Planning Guide. Provides a general understanding of RSA Access Manager, its high-level architecture, its features, and deployment information.

Servers Installation and Configuration Guide. Provides instructions for installing and configuring the RSA Access Manager Servers and additional components. This guide also contains descriptions for different configuration options, features, and production environment considerations.

Administrator's Guide. Provides information for your security administrators about using the RSA Administrative Console to administer users, resources, and security policy in RSA Access Manager.

Developer's Guide. Provides information about developing custom programs using application programming interfaces (APIs) included with the RSA Access Manager Servers.

API Delta Document. Provides information about the differences between previous and current versions of the APIs included with the RSA Access Manager Servers.

Upgrade Guide. Provides information about how to upgrade from previous versions of the RSA Access Manager Servers, data store schema, and data to the current version.

Security Configuration Guide. Provides an overview of the settings available in the RSA Access Manager Server and compatible Agents to ensure secure operation of the product.

RSA Administrative Console Help. Provides instructions on how to perform specific administrative tasks. To view Help, click the **Help** tab on the RSA Administrative Console.

RSA Access Manager User Self- Service Console Help. Describes day-to-day user tasks performed in the User Self-Service Console. To view Help, click the **Help** tab on the RSA User Self-Service Console.

Related Documentation

For more information about products related to RSA Access Manager, see the following:

RSA Access Manager Agents documentation set. The documentation related to agents is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

RSA Adaptive Authentication documentation set. The documentation related to RSA Adaptive Authentication is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

RSA enVision documentation set. The documentation related to RSA enVision is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

Before You Call Customer Support

Make sure that you have direct access to the computer running the RSA Access Manager software.

Please have the following information available when you call:

❑ Your RSA Customer/License ID.

This is a paper license. You can find this number only on the license distribution medium. If you do not have access to the paper-based RSA Customer/License ID, contact RSA Customer Support.

❑ RSA Access Manager software version number and patch level.

- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name, version, and patch level of the operating system under which the problem occurs

1 System Overview

RSA Access Manager easily integrates with your existing IT environment to provide a dependable web access management solution. The Access Manager user authorization and privilege management features securely control access to web applications within intranets, extranets, portals, and exchange infrastructures. Access Manager is a robust solution that has been designed for efficient administration, a satisfying user experience, and adaptability to unique business needs.

System Requirements

For RSA Access Manager and RSA Access Manager Agent system requirements, see the *Servers Installation and Configuration Guide,* and your RSA Access Manager Agent documentation.

General Features

Interoperability

To provide a truly unified security management solution, Access Manager enables tight integration with existing complex, multi-vendor environments, including authentication services, a public key infrastructure, web servers, and application servers. Access Manager also provides native support for user LDAP and Active Directory data stores, which allows you to leverage your existing user data.

Scalability

As your business grows, Access Manager is able to adjust to expansion easily, not simply by accommodating heavier throughput, but also by providing for delegated administration, automated authorization policy updates, and easy integration.

Comprehensive Identity Management

Access Manager provides the key features required of an identity management solution, such as the ability to:

- Establish trust in identities through authentication.
- Integrate with user data stores.
- Manage the creation and termination of identities.

Access Manager provides the ability to manage the full life cycle of an online identity.

Web Access Management

Web access management establishes and enforces policies that control user privileges. Authorization relies on business rules that define which users can access a specific resource. When users attempt to access a particular application or area of a web site, Access Manager grants or denies access based on whether their privilege profile meets certain criteria. These criteria can be static (job responsibility or department) or dynamic (account status).

Centralized User Privilege Management

Centralized user privilege management provides rule-based and role-based access control, which relies on definable sets of business rules and user attributes. This feature offers a centralized solution that allows organizations to secure web resources through intranets, extranets, portals, and exchange infrastructures. It permits fine-grained control of user privileges while easing the administrative burden of managing a large number of users in a diverse environment.

Unique User Session

Unique user session enables the user session to be active on only one IP address. Before starting the Access Manager Servers, you can enable or disable unique user session based on your enterprise policy. Since there can be multiple instances of Authorization Servers in a deployment, the unique user session configuration must be the same across all instances of Authorization Servers.

You can also enable or disable unique user session during runtime using the Network Management System (NMS) browser. The configuration changes made using the NMS browser do not require restarting of any Access Manager Servers.

When you enable unique user session, the session information is stored in your data store. When unique user session is disabled, the cookie stored in the user's browser acts as the session identifier.

For more information, see the *Servers Installation and Configuration Guide*.

Administration Features for Security Administrators

Delegated Administration

Delegated administration lets you distribute administrative tasks to various business units, both inside and outside the organization. This feature helps balance your administrative load while preserving privacy between organizations, for example, preventing the marketing department from accessing the profiles or capabilities of users in the finance department.

Secure Delegated Impersonation

Secure delegated impersonation lets you delegate administrators to act as impersonators and access the applications used by other users and troubleshoot the issues that the users face. When you enable secure delegated impersonation, details such as user name of the impersonated user, impersonator details, and resources accessed by the impersonator are logged.

Using Access Manager APIs, you can set secure delegated impersonation policies for applications, resource URLs, and application functions. For more information, see the *Developer's Guide*.

Policy Assessment

Policy assessment lets you test the security policy prior to deployment, which helps you ensure that you have configured the security policy properly to support your organization's business policy.

Administration Features for System Administrators

Simple Network Management Protocol Support

Access Manager provides support for a third-party Network Management System (NMS) using Simple Network Management Protocol (SNMP). An NMS reveals how the Access Manager Servers are functioning in a production environment, making it easier to configure them for optimal performance.

Dynamic Debugging

Access Manager provides dynamic debugging capabilities during runtime. The debugging options are configured from an NMS browser using SNMP. You can also change the log levels for all the Access Manager servers and view the number of token errors in the last 24 hours using the NMS browser at runtime. The configuration changes made using the NMS browser do not require restarting of any Access Manager Servers. For more information, see the *Servers Installation and Configuration Guide*.

Auditing and Reporting

Access Manager lets you consolidate reports about the activities occurring in your environment. Detailed logs record the actions of users, administrators, and system processes. From Access Manager 6.1 onwards, you can use RSA enVision to interpret logs. RSA enVision can convert these log files into easily traceable reports and graphs.

User Features

Single Sign-On

As enterprises expose more applications on intranets and on the Internet, some are finding that they have multiple sites that share the same set of users. Even if the different applications share a user store, such as an LDAP directory, a user still must log on to every application separately.

Single sign-on (SSO) allows users to move seamlessly across web servers and applications without having to reauthenticate each time they click a new link.

For more information, see your RSA Access Manager Agent documentation.

Intersite Single Sign-On

Intersite single sign-on (ISSO) allows users to log on once and access resources across different divisions, partners, regions, or web domains without having to reauthenticate.

For more information, see your RSA Access Manager Agent documentation.

Form-Based Authentication

The RSA Access Manager Agent provides web forms that you can use to gather and submit a user’s logon credentials. You can customize these web forms to match the look and feel of your company’s web site. For more information, see your RSA Access Manager Agent documentation.

URL Retention

When using form-based authentication, Uniform Resource Locator (URL) retention enables the web server to retain the URL of the page the user requested. After the user has been authenticated, instead of being sent to a default location (such as the home page), the user is sent to the requested page.

For more information about URL retention, see your RSA Access Manager Agent documentation.

Customization Features

Custom Password Restrictions

In addition to the password policy in Access Manager, you can write your own listener classes to enforce any extra validation for the passwords of the users that are created or modified.

When a user is created or modified, Access Manager checks for the validity of the password before the changes are saved. For more information on configuring password restrictions, see “Configuring Password Restrictions” in the chapter “Enhanced Functionality” in the *Servers Installation and Configuration Guide*.

Authentication Support

The authentication method you choose to use is configured on the Agent. For more information about configuring authentication methods, see your RSA Access Manager Agent documentation.

Access Manager supports the following authentication methods:

Basic. This is the default authentication method. At logon, users enter their user name and password, which are authenticated with the user account information stored in the Access Manager data store.

RSA SecurID. Access Manager supports RSA SecurID two-factor authentication. At logon, a user name and passcode are authenticated against the credentials stored in the Authentication Manager.

X.509 Certificates. Access Manager supports X.509 certificates. You can configure your web server to accept browser certificates for authentication.

Windows. Access Manager can use several methods to authenticate users against the Windows environment. These include NT, NT LAN Manager (NTLM), and Integrated Windows Authentication (IWA). For more information, see the *Servers Installation and Configuration Guide*.

Custom. You can use an Access Manager Web Agent Extension (WAX) or the Access Manager Runtime API to create your own custom authentication method, with custom error messages and logging. You can also create a WAX program that integrates with existing legacy authentication methods or any number of other integrations. For more information, see the *Developer's Guide*.

RSA Adaptive Authentication. You can use RSA Adaptive Authentication, which is a flexible, layered authentication solution, to tighten security and lower transaction risk. RSA Adaptive Authentication makes use of JavaScripts to collect user-activity data from web browsers. It analyses this data to determine the risk of end-user logons. The data collected from web browsers is provided to the Adaptive Authentication Server for assessing risk and building user profiles. The Adaptive Authentication Server works with the Access Manager Server and Agent to provide customers with a first level of authentication before a second level of authentication with Access Manager.

Access Manager can be integrated with Adaptive Authentication Server by deploying it as On Premise. On Premise is a solution that is physically implemented at your premises, independent of the centrally hosted solution.

For more information on configuring RSA Adaptive Authentication with Access Manager, see the chapter, “Integrating RSA Access Manager with RSA Adaptive Authentication” in the *Servers Installation and Configuration Guide*.

Each authentication method, except Adaptive Authentication, prompts the user to provide the appropriate identification credentials.

For example, Windows NT and Basic authentication prompt for a user name and password. RSA SecurID authentication prompts for a user name and passcode. After the authentication method accepts the user’s credentials, Access Manager checks for the user’s authorization privileges on the requested resource.

For added security, you can combine different authentication methods. For example, you can require that a user first authenticate by Basic authentication and then by Windows NT authentication.

You configure authentication on the RSA Authentication Agent. For more information, see your RSA Access Manager Agent documentation.

User Self-Service Customization

The User Self-Service Console is a web-based application that helps your users to change or reset their passwords and update attributes, such as first name, e-mail, and other custom properties. It is built on the Apache Struts 2 framework, which provides a highly customizable validation framework.

You can customize the User Self-Service Console graphical user interface to:

- Validate the inputs the users provide by extending the basic field input validation classes. You can do this by writing your own validation classes.
- Display unique messages before and after the user executes an action on the console.
- Provide internationalization support to display messages in the language of your choice.
- Display a modified help file which provides guidance to users on your implementation of the Console.

RSA Administrative Console Logon Banner

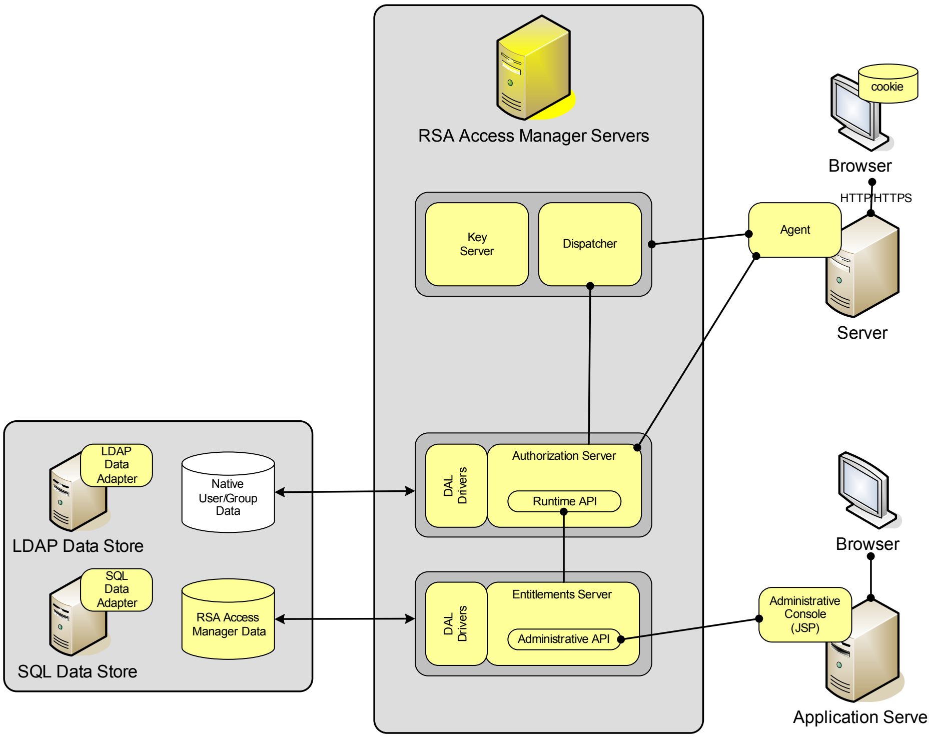
You can modify the RSA Administrative Console logon banner, which is a text that is displayed on the Administrative Console logon page. For instructions on modifying the Administrative Console logon banner, see the *Servers Installation and Configuration guide*.

2 Understanding RSA Access Manager Components

Required Components

This section describes each required Access Manager component and its purpose in the Access Manager system.

The following figure shows all of the required components and their high-level architecture.



RSA Access Manager Servers

To implement Access Manager, you must install and configure at least one instance of each of these servers.

Entitlements Server

The Entitlements Server provides Administrative API clients (including the Administrative Console) with read/write access to the Access Manager data store. This allows you to establish and revise your security policy. You can configure the Entitlements Server to selectively update the cached data on your Authorization Servers. By doing so, changes you make to the Access Manager data store, such as entitling a user to access a resource, take effect immediately. For more information, see the **eserver.conf** file.

Authorization Server

The Authorization Server performs the authentication and authorization checks for users at runtime. When a user tries to access a resource, the Authorization Server determines whether the authentication method validated the user and whether the user is allowed to access the resource.

The Authorization Server reads the user and policy information directly from the data store. To improve runtime performance, the Authorization Server can be configured to cache a variety of data. When properly configured, the Authorization Server does not have to go to the data store to check access privileges for users who have already been allowed or denied access to a resource. For more information, see the **aserver.conf** file.

Dispatcher/Key Server

The Dispatcher/Key Server has two functions.

The Dispatcher keeps track of all available Authorization Servers. By default, Agents are configured to query the Dispatcher at startup for available Authorization Servers. Agents then connect to the Authorization Servers that are available.

The Key Server generates single sign-on (SSO) token encryption keys (or secret keys), which carry a limited lifetime. When a user authenticates to the Access Manager system, the Authorization Server issues a token, encrypted with one of these keys, that encapsulates the user's session state. The Agent returns this token to the user's browser in the form of a cookie. On subsequent requests, the token is sent back to the Authorization Server for decryption as needed. For more information, see your Agent *Installation and Configuration Guide*.

RSA Access Manager Data Adapters

Access Manager uses the Data Abstraction Layer (DAL) to access user data in data stores, such as an LDAP directory or an SQL database. The user data store contains all information about your users and their access privileges. Access Manager adds additional policy, resource, and administration data schemas to your directory server or database, which you can manage separately from your user data store. This allows you to consolidate your users and security policies into one central location, and makes administering your enterprise security less time-consuming.

Access Manager policy, resource, and administrative data can also be kept in separate data stores from your user and group data. You can configure the Data Adapter to control the location and setup of your user and policy data stores.

Keep in mind that your data stores must all be of the same type. For example, you cannot store some users in an LDAP directory, and other users in an SQL database.

You make changes to the Access Manager data stores through the Administrative Console (or through the Administrative API, which has larger capabilities than those provided by the Administrative Console).

Both the Entitlements Server and Authorization Server use the Data Abstraction Layer (DAL) drivers to connect directly to your data servers.

Install one Data Adapter for each of your data stores. For a list of supported data store servers, see the *Servers Installation and Configuration Guide*.

RSA Access Manager Administrative Console

You use the Access Manager Administrative Console to administer your Access Manager system. The Administrative Console is a web-based, Java Server Page (JSP) application that you install on any supported application server or servlet engine. For a list of supported application servers and servlet engines, see the *Servers Installation and Configuration Guide*.

You can access the Administrative Console from any computer with a web browser. From the Administrative Console, you can set up administrative groups and roles, add resources, and define your security policies. You can also use the Administrative Console to add and edit your users and groups, and store them in its data store.

For users and groups created outside of Access Manager in an LDAP data store, RSA recommends that you continue to use your existing data management tool to create and update users, and set up Access Manager in the **ldap.conf** configuration file to treat this data as read-only. If you use the Administrative Console to edit data created outside of RSA Access Manager, you can overwrite or corrupt existing entries.

Web Server and Application Server Agents

You must install an Agent on each of the servers you want to protect. For instructions, see your RSA Access Manager Agent documentation.

RSA Access Manager Agents are not provided on the RSA Access Manager 6.1 DVD. If your company has an Access Manager maintenance contract, you can download the Agents from RSA SecurCare Online at **https://knowledge.rsasecurity.com**

If your company does not have an RSA Security maintenance contract, call your RSA Security account representative or qualified reseller to obtain the Agent software.

Web Server Agents

RSA Access Manager Web Server Agents supplement the native security mechanisms of a web server. RSA Access Manager Web Server Agents run in the same process as the web server itself and are invoked whenever the web server needs to determine access rights for a particular Uniform Resource Locator (URL). RSA Access Manager Web Server Agents forward access requests to an Authorization Server, which passes the answers it receives back to the web server.

Application Server Agents

RSA Access Manager Application Server Agents supplement the native security on your application servers with Access Manager, and extend single sign-on to your web application environment. This allows you to protect web resources, such as servlets, Enterprise Java Beans (EJBs), and Java Server Pages (JSPs) with Access Manager.

Optional Components

You can implement the following optional components, depending on your security needs, system load, existing network architecture, and logging plans.

User Self-Service Console

The User Self-Service Console is deployed as a Web Archive (WAR) file and requires a third-party servlet engine or application server. Once you deploy the User Self-Service Console, users can access it from any computer using a supported web browser. To deploy and configure the User Self-Service Console, see the *Servers Installation and Configuration Guide*.

For more information on customizing the User Self-Service Console, see the *Developer's guide*.

You can also customize the User Self-Service Console Help to reflect how your company uses it. For more information on customizing the User Self-Service Console Help, see the *Servers Installation and Configuration Guide*.

Redundant RSA Access Manager Servers and LDAP Directories

You can deploy additional Access Manager Servers and LDAP directories to increase runtime performance and stability, and to eliminate single points of failure in your Access Manager system.

For more information, see Chapter 3, "Planning Your Physical Deployment."

RSA Access Manager Log Server

The Access Manager Log Server allows you to configure your system so that all servers write to a single log file, regardless of where the servers are physically located.

For information about the individual log files generated by the log server, see "Planning Your System Logs" on page 35.

RSA Access Manager Instrumentation Server

The Instrumentation Server provides Simple Network Management Protocol (SNMP) support for a third-party Network Management System (NMS). Using an NMS, a system administrator can query the Instrumentation Server for information about the Access Manager Servers that are running in a production environment. This allows for real-time monitoring of Server activity and performance.

For more information, see the *Servers Installation and Configuration Guide*.

RSA Certificate Manager

The RSA Certificate Manager creates keystores that can be used by Access Manager for intercomponent security.

RSA Access Manager Software Development Kit

Access Manager is a highly customizable solution. You can use the following Access Manager Application Programming Interfaces (APIs) and Service Provider Interfaces (SPIs) to create custom applications that work with the Access Manager components.

Administrative APIs

The Java web service versions of the Administrative API allow you to develop applications that interact with the Entitlements Server to create user accounts and the security policies that protect resources. A security policy identifies protected resources, defines the entitlements and Smart Rules that control access to these resources, and identifies the administrative groups and administrative roles in these groups that manage the security policy itself. In addition, if Access Manager is configured for write access to the user data store, your Administrative API applications can create and update users and user groups. This allows you to write custom programs to perform various administrative functions.

For example:

- Load a large quantity of data from another source directly into the Access Manager data store.
- Develop custom web applications to perform self-registration and self-service account management for Access Manager.
- Develop custom policy administration applications that enhance the functionality provided by the Administrative Console.

Runtime APIs

The Java, C, and web service versions of the Runtime API allow you to develop custom programs that use or extend the runtime functionality of the Authorization Server. The Runtime API provides efficient and scalable read-only access to certain Access Manager objects and security policy settings. You can use the Runtime API to:

- Authenticate users.
- Control user access to protected resources.
- Personalize a user’s online experience.
- Allow SSO tokens created by the Runtime API to be passed to application servers and web servers.
- Impersonate users and access resources they have access to.

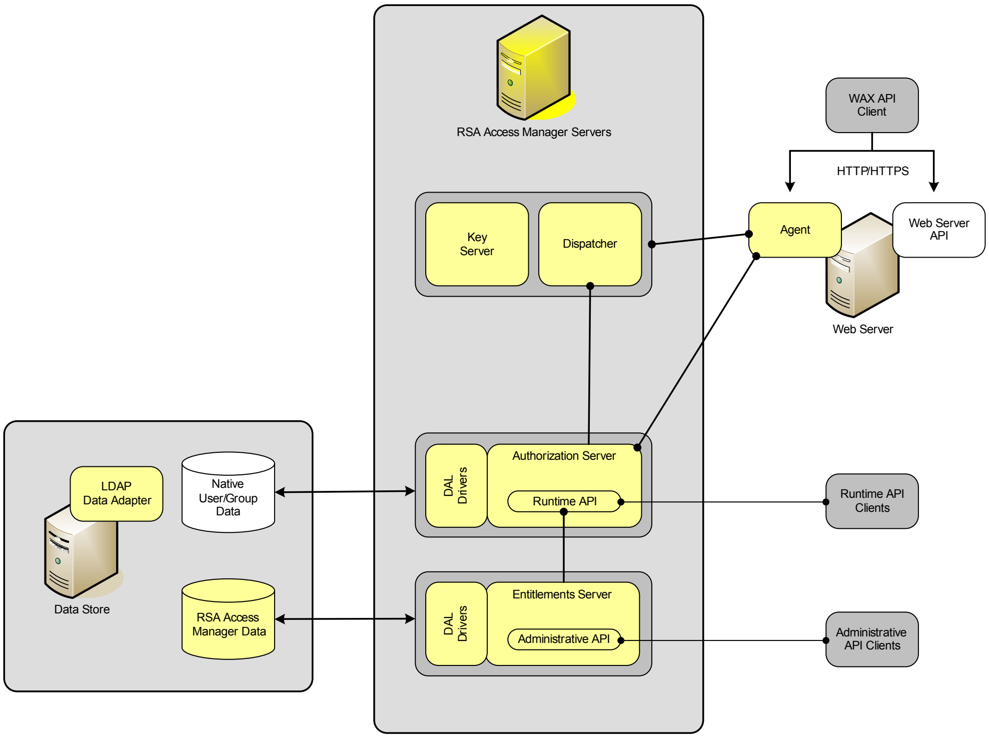
Web Agent Extension (WAX) API

The WAX API, implemented in C, allows you to extend the functionality of the RSA Access Manager Web Server Agents. This allows you to customize or control the behavior of the Agent during the authentication and authorization processing. For example, you can:

- Create an extension to do custom logging.
- Create an extension to do custom authentication of users without connecting to an Access Manager Authorization Server.
- Create an extension to direct the web server to custom HTML pages based on the return codes returned from the Authorization Server.

For more information about using the APIs to develop your own custom security applications, see the *Developer's Guide*.

The following figure shows the relationships between the Administrative, Runtime, and Web Agent Extension APIs and Access Manager.



Server Provider Interfaces

The Service Provider Interfaces (SPIs) allow you to extend the Access Manager Servers in various ways by implementing code that is run in-process as part of the Servers. This code is registered with the Servers to be invoked at certain points during client request processing. This allows you to:

- Alter or override default Administrative and Runtime API call behavior, or to perform arbitrary operations (for example, sending notifications to remote systems) when such calls are executed.
- Retrieve user properties from third-party data sources for use in Smart Rule evaluation and by RSA Access Manager Agents.

- Make additional Runtime API calls within the context of a client call execution within the Authorization Server. This makes it possible to have more complex combinations of authentication and authorization logic.

System Configuration Files

You must configure Access Manager components so that they can communicate with each other and securely pass information over the network. You can also take advantage of features available with Access Manager, such as single sign-on (SSO). All system configuration parameters are controlled in text files that are read by the Access Manager components.

There is a configuration file for each of the Access Manager components:

- Authorization Server (**aserver.conf**)
- Entitlements Server (**eserver.conf**)
- Dispatcher/Key Server (**dispatcher.conf** and **keyserver.conf**)
- Log Server (**lserver.conf**)
- Instrumentation Server (**iserver.conf**)
- LDAP Data Adapter **(ldap.conf**)
- SQL Data Adapter (**sql.conf**)
- Web Server Agent/Application Server Agent (**webagent.conf** and **cleartrust.properties)**
- Administrative Console (**admingui.cfg**)
- Unique User Session (**uus.conf**)
- User Self-Service (**selfservice.conf**)

RSA Access Manager Server Configuration Files

These are the configuration files for the Access Manager Servers:

Authorization Server configuration file. There is one configuration file for each Authorization Server you install. You must configure the Authorization Server to find the Dispatcher/Key Server and your data stores.

This configuration file lets you control the information that is cached on the Authorization Server, controlling the level of performance (and memory usage) for the runtime operations of the Access Manager system. You can also configure the level of information that is written to the log files for user and runtime activity.

Entitlements Server configuration file. This file contains all of the information that the Entitlements Server needs to connect to your data store and the Administrative Console. You can also configure the level of information that is written to the log files for administrator and API activity.

Dispatcher/Key Server configuration files. There are two configuration files for each Dispatcher/Key Server you install. You must configure the Dispatcher to listen for connections from the Authorization Servers and the Web Server Agents. The Key Server file has parameters that control the distribution of the secret keys used for single sign-on.

Log Server configuration file. This file contains all of the information that the Log Server needs to consolidate log messages from the Access Manger Servers. This file has parameters for setting the port where the Log Server listens for incoming client connections, setting log file size, and setting the number of log backups to retain before the oldest is deleted.

Instrumentation Server configuration file. This file contains settings for making information about Access Manager Servers available through Simple Network Management Protocol (SNMP). This file has parameters for connecting a third-party Network Management System (NMS) to the Access Manager Servers.

Adaptive Authentication configuration files. These files contain configuration parameters and descriptions for configuring Access Manager with Adaptive Authentication. For each parameter, the files contain information, such as descriptions, allowed values, the default values, dependencies, and examples.

Data Adapter Configuration Files

LDAP Data Adapter configuration file. This file contains settings to connect the Entitlements Server and Authorization Server to the Access Manager Data Adapter for your LDAP directory, where both user data and Access Manager policy data are stored. A copy of the LDAP Data Adapter configuration file must reside on each machine running an Entitlements Server or Authorization Server.

This file allows for flexible integration with your directory server environment. For example, to leverage your existing directory structure, you can map your directory server attributes to Access Manager attributes. You can also specify different directory servers for backup and for storing your user data separate from your Access Manager policy data.

SQL Data Adapter configuration file. This file contains settings to connect the Entitlements Server and Authorization Server to the Access Manager Data Adapter for your SQL database, where both user data and Access Manager policy data are stored. If you are using an SQL data store, a copy of this file must reside on each machine that is running an Entitlements Server or Authorization Server.

Web Server and Application Server Agent Configuration Files

A relevant configuration file must reside on each web server or application server protected by Access Manager. The RSA Access Manager Agent uses this configuration file to obtain information about:

- The Access Manager Dispatcher/Key Server and Authorization Servers to find and connect to.
- The maximum lifetime and idle time for a user's session.
- The types of authentication that are used to verify a user's access to particular resources on that server.

- What and how additional features of Access Manager are implemented, such as single sign-on, URL retention, form-based authentication, and so on.
- The location of any custom HTML forms or Web Agent Extensions (WAX) you are using.

RSA Administrative Console Configuration File

The Administrative Console finds and connects to the Entitlements Server using this file.

Unique User Session Configuration File

The unique user session configuration file lets you to configure the connection parameters for Authorization Servers to use the SQL database for session management.

User Self-Service Console Configuration File

The User Self-Service configuration file contains the configuration parameters for User Self-Service Console and description for each of those parameters.

RSA Access Manager Component Security

Creating a truly secure Access Manager system requires more than just protecting servers. The communication between the different components must be secure, and sensitive information stored in the file system must also be protected. This section describes the different areas that need protection and the steps necessary to shield the system from attack. It also provides information about password storage and transmission across the network.

User Passwords

The default authentication mode, Basic authentication, requires a user name and password, which the Authorization Server validates against the Access Manager data store. Each user in Access Manager has a password. Whenever a password passes over the network or is stored on disk, the password may be stolen. To reduce the risk of password theft, all passwords stored in Access Manager are hashed.

Hashing converts a password into a unique numeric value. The same password always converts into the same characters, and you cannot run the process in reverse, so that there is no way to retrieve the password.

Operating System Security

You must tightly control file permissions on the directory where Access Manager is installed. Only grant access to the individuals or groups that absolutely need it, and only grant administrators access to the configuration files.

Single Sign-On Cookie Security

You can protect the Access Manager cookie on the client in the following ways:

- Configure RSA Access Manager Web Server Agents to treat the cookie as a session cookie, rather than as a persistent cookie. When configured in this way, the cookie is stored on the browser rather than on the hard drive, which prevents a malicious user from retrieving the cookie from the computer for later use.
- Configure RSA Access Manager Web Server Agents to check the source of each incoming cookie. To permit this, the cookie is labeled with the IP address of the machine (where the user's browser is running) for which the cookie was created. Each time the user cookie is used to request another resource, the Agent checks that the request originated at the IP address for which that cookie is valid. This means that only the requesting client machine can use the cookie created for that client. This prevents a malicious user from stealing the cookie and using it from another computer.
- Set Access Manager to enforce validity periods for cookies. With this feature turned on, each cookie becomes unusable after a determined period of inactivity. For example, if a user logs on to a resource protected by Access Manager and then leaves his or her desk, a short expiration period narrows the window of time that another person can sit down at the unattended workstation and assume the existing session.
- Set the maximum lifetime for a user's session. The cookie has a maximum lifetime that forces a reauthentication when the cookie's lifetime expires. You set the timeout settings, both for maximum lifetime and inactivity, individually for each server.

In addition, you can configure your web servers to run with SSL encryption turned on, which encrypts cookies along with all other communications between the web browser and web server.

Intercomponent Security

Intercomponent security protects information as it passes between components. Access Manager supports different types of intercomponent security, such as:

- No encryption
- Shared secret encryption
- Anonymous SSL (default)
- Mutually Authenticated SSL
- Server Authenticated SSL

No Encryption

This means that communications between components are not encrypted when they pass over the network. Such unencrypted information is often called clear text or plain text.

Shared Secret Encryption

You can use shared secret (or symmetric) encryption to protect sensitive information in the Access Manager single sign-on (SSO) cookie. Shared secret encryption is required if you are using single sign-on or form-based authentication. It is always enabled, regardless of whether or not you pass the SSO cookie over an SSL connection. The SSO cookie is never passed over the network without being encrypted.

Every Authorization Server and any Web Server Agent that participates in intersite single sign-on (ISSO), a method that allows a user to go from one protected site to another without having to reauthenticate, must have a valid key generated by the Access Manager Key Server (the Access Manager internal cryptography server). This ensures that the SSO cookie is only encodable and decodable by trusted Access Manager components. The client must present the key to the Key Server before the client can obtain the current cookie encryption/decryption key, thus authenticating the client to the Key Server.

You can use shared secret encryption between the following Access Manager components:

- Authorization Servers and Key Server
- Web Server Agents and Key Server

Anonymous SSL

This is the default mode for intercomponent communications. When you install Access Manager, by default, all data exchanged between Access Manager components is encrypted with Secure Sockets Layer (SSL) encryption technology. Before transmission over the network, the data is encrypted using anonymous SSL. Anonymous SSL means that neither the client nor the server is required to present a certificate to authenticate itself.

The particular SSL modes vary from one component to another, but in all cases, Access Manager uses 128-bit encryption for all messages sent across the network.

Anonymous SSL can be used by all interfaces between Access Manager components to secure connections.

Mutually Authenticated SSL

Communications between the Access Manager components can be secured using mutually authenticated SSL. In this mode, each Access Manager component must present its digital certificate when contacting another component, allowing that component to verify its identity.

To activate SSL communications, you must configure the Access Manager Servers and Agents to use mutually authenticated SSL, and you must make sure each component has access to the keystore containing its certificate and the trusted CA certificate.

When setting up mutually authenticated SSL, you can use a single keystore format, either PKCS #12 or JKS (Java Keystore). Your choice may be guided by the limitation of the Agents, which are not compatible with JKS format.

Server Authenticated SSL

Communications between the LDAP directory server and the Entitlements and Authorization Servers can be secured using server authenticated SSL. In this mode, the LDAP directory server presents its digital certificate when responding to client requests from the Authorization and Entitlements Servers.

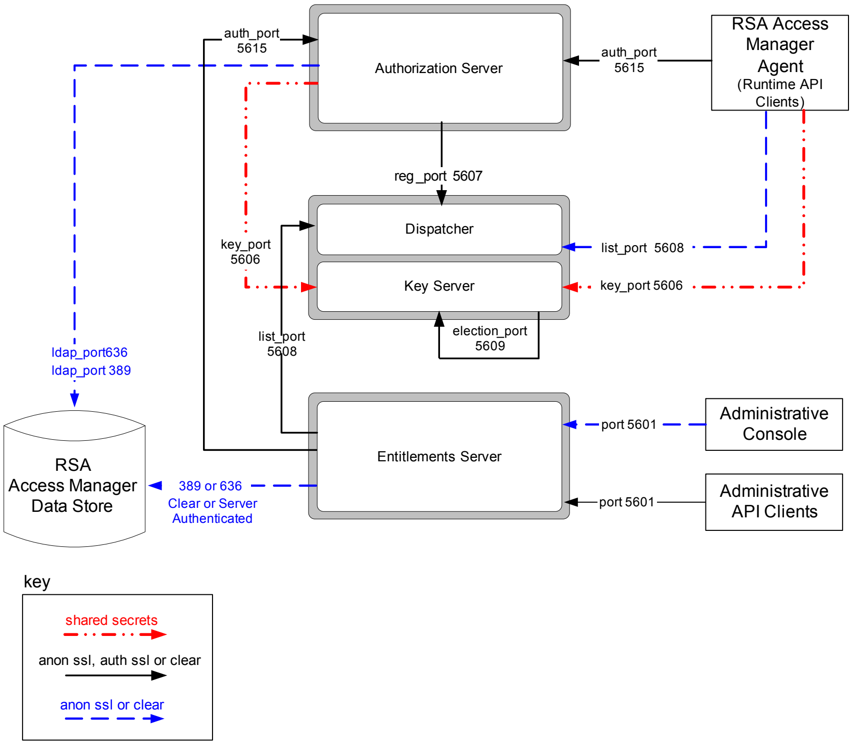
To activate server authenticated SSL, you must configure the LDAP directory server for SSL communications and then ensure that the keystore of each Access Manager Server includes the CA certificate of the authority that signed the LDAP server certificate.

The following components support server authenticated SSL:

- Entitlements Server and LDAP Directory Server
- Authorization Server and LDAP Directory Server

Mutually authenticated SSL is available for all components except SQL data stores.

The following figure shows the intercomponent security options for the various connections between components.



3 Planning Your Physical Deployment

Before You Begin

Before you install RSA Access Manager components and configure the system, plan how you want to deploy Access Manager in your organization. This chapter describes the different architectures you can deploy, depending on your security needs and planned system capacity.

Before you get started, take inventory of your current environment, and find answers to these questions:

- How many servers do you want to protect?

  This helps you determine the number of Access Manager components you need to deploy:

  – You must have one Web Server Agent for each web server you want to protect.

  – You must have one Application Server Agent for each application server you want to protect.

  – Determine the appropriate ratio of Authorization Servers to servers protected by Access Manager. The appropriate ratio for your installation depends on the load your system must support.

- Which data servers do you want Access Manager to access?

  You must install and configure the appropriate Data Adapter for your data store:

  – For SQL and directory server data stores, you must have administrator credentials for servers that contain your user and group data needed to perform authentication and access control. This includes servers used as replicas, backups, and partitions.

  – For directory server data stores, decide where to install the Access Manager policy data store. The Access Manager policy, resource, and administration can be stored in a separate data store from your user and group data.

  - For directory server data stores, identify backup directory servers, if any, that are required for failover of the primary user and group data store, and the Access Manager policy data store.
  - For directory server data stores, you must map attributes in your existing user and group data to Access Manager attributes. For more information, see Chapter 4, "Planning Your Logical Deployment."

- What is your security policy?

  This helps you determine how to set up your logical architecture and business rules in the Administrative Console. For more information, see Chapter 4, "Planning Your Logical Deployment."

- What additional features of Access Manager do you want to deploy?

  Determine which additional features you want to deploy:

  - Single sign-on
  - Customized logon forms
  - Custom programs using the Access Manager APIs to meet unique requirements
  - Access Manager developer tools
  - Additional distributed Authorization Servers
  - A redundant Entitlements Server
  - A redundant Dispatcher/Key Server
  - Redundant LDAP directory hosts for sites that use an LDAP/X.500 directory server
  - RSA Certificate Manager
  - Access Manager intercomponent security
  - Access Manager Log Server
  - Access Manager Instrumentation Server
  - Secure Delegated Impersonation
  - User Self-Service Console

For more information about optional components, see the chapter "Installation Requirements" in the *Servers Installation and Configuration Guide*.

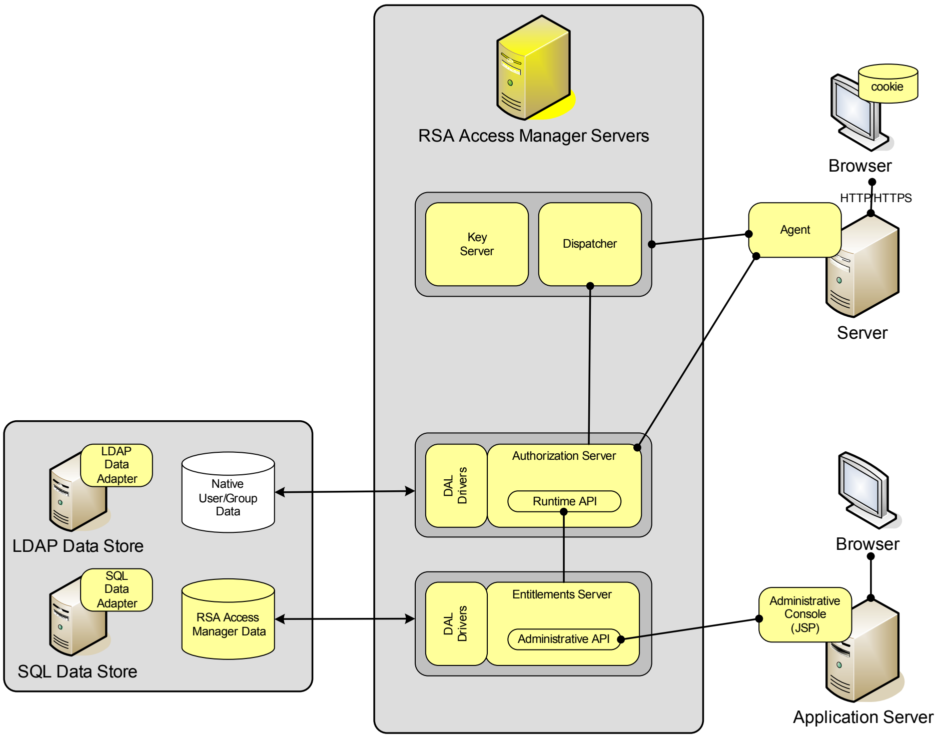
Standard Architecture

The standard architecture refers to the out-of-the-box deployment of Access Manager. Although the standard architecture may be suitable for very small implementations or for testing purposes, it is not recommended for large-scale production deployments of Access Manager.

The standard architecture includes:

- Access Manager Servers installed on one physical machine. The out-of-the-box installation consists of one Entitlements Server, one Authorization Server, and one Dispatcher/Key Server.
- Your data store (such as an LDAP directory) running on either the same machine as the Access Manager Servers or on a remote machine. You must install an Access Manager Data Adapter on the data store.
- At least one instance of the Administrative Console running on an application server, either on the same machine as your web server or on a remote machine.
- At least one remote web or application server on which you installed an RSA Access Manager Agent.

The following figure shows the components of the Access Manager standard architecture.



Keep in mind that you can have different components running on different platforms. For example, your Access Manager Servers can run on Solaris, while your web servers and Agents run on Windows. For a list of all supported platforms, see the *Servers Installation and Configuration Guide.*

Planning Your Data Store Deployment

LDAP Data Store

The Access Manager LDAP Data Adapter lets you use your LDAP directory as your Access Manager data store. Access Manager comes with a default LDAP schema that you can install and use. When you select the LDAP option during installation, the installer automatically installs and configures a fully-functional LDAP Data Adapter for that host.

To install Data Adapters on remote servers in a distributed environment, you must manually install the Data Adapters on each remote server. This includes LDAP servers used for referrals and replicas. For more information, see the *Servers Installation and Configuration Guide*.

Active Directory Data Store

The Access Manager LDAP Data Adapter enables you to use Active Directory as your Access Manager data store. The Data Adapter can access information in a single or multi-domain configuration.

You must manually install a Data Adapter on each host. For more information, see the *Servers Installation and Configuration Guide*.

Default Administrator for Active Directory Installations

When you install the Data Adapter, the installer does not prompt for, or create, an Access Manager administrator, as it does for other data stores. Instead, the default Active Directory administrator account becomes the default Access Manager administrator account.

Password Policies in Active Directory

RSA recommends that you set your general password policy in Active Directory. If you are using Access Manager to define a password policy for administrative groups, make sure it does not conflict with the password policy you defined in Active Directory. The password policy in Active Directory must always be less restrictive than the password policy defined in Access Manager.

Active Directory Application Mode Data Store

The Access Manager LDAP Data Adapter enables you to use Active Directory Application Mode (ADAM) as a data store that coexists with Active Directory. In such an installation, ADAM is used to store Access Manager policy and administrator assignments while Active Directory continues to store information about users, user attributes, and user groups.

For more information about applying the Data Adapter to ADAM, see the *Servers Installation and Configuration Guide*.

SQL Data Store

The Access Manager SQL Data Adapter enables you to use an SQL database as your Access Manager data store.

When you select the SQL option in your Access Manager Servers installation, the installer automatically installs and configures a fully-functional Data Adapter for that host.

To install Data Adapters on remote servers in a distributed environment, you must manually install the Data Adapters on each remote server. This includes replica SQL servers. For more information, see the *Servers Installation and Configuration Guide*.

Redundant Data Servers

You can configure Access Manager installations that use an LDAP directory to connect to multiple directories. If your primary LDAP directory fails, Access Manager attempts to connect to alternate directories that you specify.

Access Manager supports LDAP referrals for search operations. If your primary LDAP directory cannot fulfill a request, Access Manager can accept a referral URL to another LDAP directory. LDAP referrals can be used to deploy read-only server replicas for your Access Manager data stores.

Providing access to read-only replicas is one of many different load balancing strategies that can be implemented by using referrals. For more information about setting up referrals for your LDAP directory, see your LDAP directory documentation.

For more information about redundant data servers, see the *Servers Installation and Configuration Guide*.

Planning Your Authorization Server Deployment

Reliability of high volume components is a key requirement for distributed software. Because they are high volume, such components are also the most likely to suffer from performance and reliability problems. In Access Manager, the Authorization Server is the highest volume component. The Authorization Server handles authentication and authorization queries from the RSA Access Manager Web Server Agents and Application Server Agents.

The Access Manager system architecture provides for failover among multiple Authorization Servers, ensuring that an Authorization Server is always available.

Distributed Authorization Servers

When your Authorization Servers run in distributed mode—the default configuration—it means that Access Manager runs multiple Authorization Servers across multiple machines. Distributed Authorization Servers can run on Windows and UNIX servers simultaneously.

Distributed mode balances web server requests across all the Authorization Servers. If a single Authorization Server becomes unavailable, the remaining Authorization Servers continue to fulfill Web Server Agent requests. You can configure the Dispatcher to send you an e-mail notification if it determines that an Authorization Server is down.

Geographically Distributed Authorization Servers

You can configure the Web Server Agents to use a preferred set of Authorization Servers. This constrains the Agent to use an Authorization Server in the same geographic location, minimizing the response time for user requests.

When the Web Server Agent is configured to connect to Servers dynamically, the Dispatcher provides the Agent with a list of all Authorization Servers within a specified location. The Agent then connects to one of these Servers.

When the Web Server Agent is configured to connect to Servers statically, the Agent selects a Server from a configured list of local Servers. In this case, no communication between the Agent and the Dispatcher takes place.

It is also possible to configure the Agent to connect to locally available Servers using both a static list as well as the dynamic list generated by the Dispatcher. For more information, see you Agent documentation.

Authorization Server Cache

In Access Manager, the Authorization Server caches user entitlement data as well as resource and security policy data. To improve response time, the Authorization Server verifies runtime requests against the cache, instead of against the data stores. When you update records in the Administrative Console, the selected records can automatically be refreshed in the cache if the Entitlements Server has been properly configured.

You can configure the level of information kept in the cache, depending on the level of performance you want to achieve. Keep in mind, however, that the larger the cache size, the more memory you need on the machine that is running your Authorization Server. Plan for about 2 MB for every 1,000 records cached.

Planning Your Entitlements Server Deployment

The Entitlements Server generally needs to support only a small number of simultaneous user sessions, because only administrators use it. Although the Entitlements Server is not a high volume component, you may not want to risk having a single point of failure in your Access Manager system.

Redundant Entitlements Servers

In most installations, an Entitlements Server backup is not necessary because RSA Access Manager Agents and Authorization Servers continue to authenticate and authorize users if your Entitlements Server is unavailable. However, if your installation requires that Access Manager administrative capabilities be available at all times, you can configure a standby Entitlements Server to handle administration if your primary Entitlements Server fails.

Deploying a standby Entitlements Server requires additional third-party hardware, software, or both. You need to set up failover so that a different machine running an Entitlements Server can take over the IP address of the default server machine, if it goes down.

A hardware solution, for example, load-balancing hardware, is the simplest method. A software failover solution is also possible. This requires you to install high-availability (HA) tools on the servers.

For more information, see the chapter “Deploying RSA Access Manager in Production” in the *Servers Installation and Configuration Guide*.

Planning Your Dispatcher/Key Servers Deployment

Although the Dispatcher/Key Server is not a high-volume component, it is critical to the operation of the Access Manager system. If the Dispatcher/Key Server fails, authorization requests might not be fulfilled. To avoid this, you can install multiple Dispatcher/Key Servers to handle requests if your primary Dispatcher/Key Server becomes unavailable.

When you install redundant Dispatcher/Key Servers, you must configure them to communicate with each other, with the Authorization Servers, and with the Web Server Agents.

You can configure RSA Access Manager Agents to contact a list of multiple Dispatcher/Key Servers, which allows you to deploy redundant components. You can configure each Agent with the addresses and ports of one or more Dispatcher/Key Servers. The Agent tries to contact each Dispatcher in the list until it receives a response from one.

When the Authorization Servers start up, they notify all of the listed Dispatchers of their existence, and periodically send keep-alive signals to all Dispatchers. Similarly, the Key Servers send keep-alive signals to each other and periodically hold an election among all live Key Servers to determine which server provides the current SSO encryption key.

For more information, see the *Servers Installation and Configuration Guide*.

Planning Your System Logs

All Access Manager servers generate log information about their operations. Each server tags its log entries with a unique ID to identify which server generated the message, and then sends the entries to the Log Server, which writes the information to a single log file. For Log Server information and configuration options, see the *Servers Installation and Configuration Guide*.

The system creates log files in the **/logs** directory of your RSA Access Manager installation.

The following Access Manager Server components generate a log file:

- Authorization Server
- Entitlements Server
- Dispatcher/Key Server

For each of the Access Manager Server component log files, you can configure the level of information that is recorded. There are five levels that you can set. The logging levels are cumulative. Higher logging levels also include all the information recorded in lower levels. For example, level 30 includes levels 10 and 20. In addition, you can configure the Entitlements Server to provide complete object life cycle information in a human-readable form. For more information, see "Enhanced Logging" on page 37.

Web Server Logs

You can also find information about Access Manager activities in your web server logs. Most web servers, including iPlanet, Apache, and IIS, use separate log files for reporting errors and reporting normal access events. The name and location of your web server log files vary from one web server vendor to another. When Access Manager lets a user access a particular resource on the web server, your web server records the access as normal. Similarly, when denies access, your web server records it as an error.

Access Manager also records its own errors in the error log of your web server. For example, anytime the RSA Access Manager Agent contacts the Dispatcher/Key Server to get a new list of active Access Manager Authorization Servers, Access Manager makes a note in the error log.

Managing Your Log Files

Over time, your Access Manager log files grow in size and can consume large amounts of disk space. When a log reaches its maximum size, which is specified in the Access Manager configuration files, Access Manager:

- Closes the log file and starts a new log file
- Dates and time-stamps the log files
- Adds the date and time to the filename of the log

It is important that you develop a process for removing or archiving old log files so that your Access Manager system can continue to run efficiently.

Centralized Logging

Centralized logging is made possible by the Access Manager Log Server. The Log Server receives the log output of the Authorization Server, Entitlements Server, and Dispatcher/Key Server and records it in a single log file.

RSA recommends that you run a separate instance of the Log Server for each type of Access Manager Server on one host. For example, on the same host you would run one instance of the Log Server for multiple Entitlements Servers, one instance of the Log Server for multiple Authorization Servers, and one instance of the Log Server for multiple Dispatcher/Key Servers.

For more information, see "Managing RSA Access Manager Log Files" in the *Servers Installation and Configuration Guide*.

Enhanced Logging

Enhanced logging provides a more detailed record of Access Manager operations, making it possible to track the life cycle of an object in the system. Enhanced logging records details about:

- The administrator who performed an operation
- The role selected by the administrator for the session
- The time when the operation was performed
- The type of operation that was performed

Advanced Logging

You can also configure Access Manager logs to contain time taken for each event and audit trail of all API calls. By default, Access Manager events are configured to contain the message IDs in the logs.

While logging authorization requests, the Authorization Server provides details of the web server details or the API calls. The request served state as either from the database or the cache is also logged.

The SNMP support of Java Virtual Machine (JVM) relays monitoring and management details to the NMS browser. Using your NMS browser, you can view JVM related information, such as number of open sockets, number of threads in use, and memory used by the JVM.

For more information, see "Enhanced Logging" in the *Servers Installation and Configuration Guide*.

Integration with RSA enVision

You can integrate Access Manager with RSA enVision to manage your logs. To do this, you must install the enVision agent on all instances where you have the Log Server running.

enVision can read logs when you have:

- Only one Log Server running
- Multiple instances of the Log Server running. In this scenario, enVision will read logs from the distributed environment. You must install the enVision Agent on all instances where you have the Log Server running.
- No Log Server running. In this scenario, Access Manager will write messages from the native Access Manager logs.

For more information, see the *Servers Installation and Configuration Guide*.

Running RSA Access Manager Components Across a Firewall

Firewalls are part of the foundation of the virtual enterprise network, and typically provide protection against threats at the network layer. The categories of this network infrastructure device are:

- Packet-level (filter-based)
- Application-level (proxy-based)
- Circuit-level

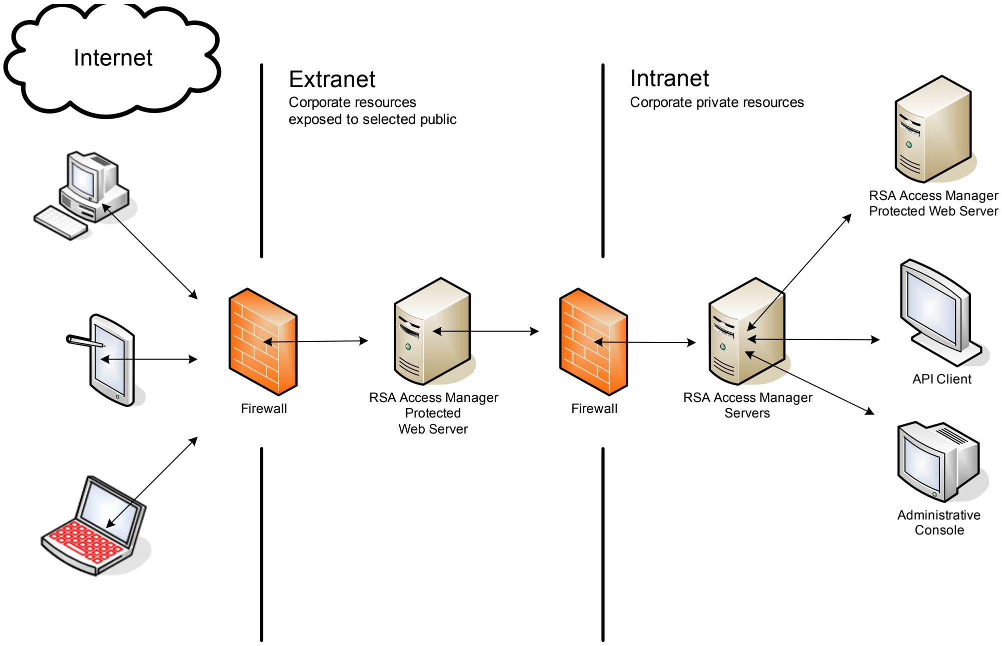
For any two Access Manager components to communicate across a firewall, you must configure the firewall to allow connections on a specific port. For specific port numbers and instructions, see the chapter "Deploying in Production Environments" in the *Servers Installation and Configuration Guide*.

To run a component across the firewall from your Access Manager server, you must configure your firewall to allow TCP/IP connections from the Web Server Agent, Administrative Console, or API Clients to the Access Manager Servers.

For extranet applications, you may want to run Access Manager components in various configurations with the firewall. You can configure the RSA Access Manager Web Server Agent, the Administrative Console, and the API Clients on the opposite side of the firewall from the Access Manager Servers.

You configure each of these components separately and can place each of them inside or outside the firewall regardless of how the other two are configured.

The following figure shows an Access Manager deployment with firewalls.


Internet
Extranet
Corporate resources exposed to selected public
Intranet
Corporate private resources
RSA Access Manager Protected Web Server
Firewall
RSA Access Manager Protected Web Server
Firewall
RSA Access Manager Servers
API Client
Administrative Console

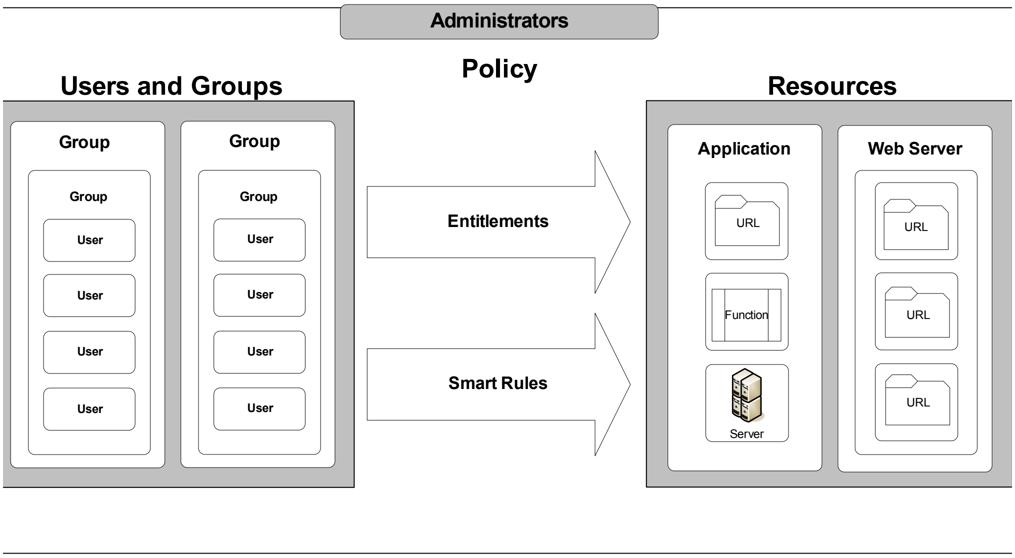
4 Planning Your Logical Deployment

Planning how to organize and use RSA Access Manager before you install the software ensures a smooth implementation that suits the specific needs of your company.

In planning your Access Manager implementation, you need to decide:

- How you want to protect your resources.
- How you want to administer Access Manager.
- How you want to organize your users.
- Which resources you want to protect.
- Who should have access to protected resources.

The following figure depicts the high-level logical architecture of Access Manager.



Planning Resource Protection Mode

Before you use the Administrative Console to add resources, decide whether you want to configure your Access Manager environment for active or passive mode. Basic access to resources depends on this configuration:

> **Active Mode.** All resources are unprotected. The system only protects resources that you explicitly add to the Access Manager system. This is the default setting.
>
> **Passive Mode.** All resources are protected. To allow access to a resource, you must add the resource to Access Manager and grant access to users with an entitlement or Smart Rule.

A parameter in the configuration file, **aserver.conf**, determines whether the system behaves in active or passive mode. By default, the system is set to behave in passive mode.

Planning RSA Access Manager Administration

Access Manager administration is delegated, which allows the administrative burden to be shared by several individuals. This is accomplished through the use of administrators who have roles in an administrative group.

In planning your Access Manager administration, you need to decide:

- How many administrators to designate
- What roles to create
- What users and resources to include in an administrative group

Administrators

Access Manager administrators are users who have been assigned one or more roles. A role defines the specific tasks that an administrator is able to perform. The number of administrators you need depends on the requirements of your organization. You can create as many administrators as necessary. Each can have a different role, or you can create several administrators with the same roles.

As an optional privilege, you can assign following roles to any Access Manager administrator:

> **Super Admin.** The Super Admin role gives an administrator the highest level of administrative privilege. Super Admins can view, add, edit, or delete any object in the Access Manager system, including other administrators, regardless of the administrative group that owns the object.
>
> **Help Desk Admin.** The primary purpose of the Help Desk Admin is to reset passwords in Access Manager. The Help Desk Admin has the ability to view all user accounts and to view and edit passwords, regardless of the administrative group that owns the user. The Help Desk Admin can also restore access to a user who has been locked out.

Config Admin. The Config Admin role gives an administrator the privileges to modify the encrypted server configuration files.

Audit Admin. The Audit Admin role gives an administrator the privileges to make changes to the audit log parameters in the encrypted server configuration files.

Note: The Config Admin and the Audit Admin roles can be used only when you encrypt the server configuration files. To know more about encrypting the server configuration files, see the *Servers Installation and Configuration guide*.

Note: All administrators must have at least one role assigned to them.

The Default Administrator

When you install Access Manager with an LDAP or SQL data store, an administrator account with Super Admin privileges is automatically created during installation. You name this Super Admin account during the installation process. This Super Admin account is the starting point for setting up your Access Manager administration.

For information about the default administrator for Active Directory installations, see "Default Administrator for Active Directory Installations" on page 32.

Roles

A role is a set of privileges that determines what an administrator can do with Access Manager objects, such as users or applications, in a particular administrative group. For example, a role created for someone managing employee information might include the privilege to add, edit, and delete users, but not the privilege to edit passwords. Another role might include all of the privileges of a Super Admin except for the privilege to delete properties.

Each administrative group can have several roles, and administrators can be assigned one or more roles in a group. Administrators can also be assigned roles in other administrative groups.

The following privileges can be included in a role:

- Add, edit, delete roles
- Add, edit, delete administrators
- Add, edit, delete users
- Add, edit, delete user groups
- Add, edit, delete applications (and resources)
- Add, edit, delete servers
- Edit passwords
- Add, edit, delete properties

When you a create a role, you give it a name. Role names typically reflect an administrator's function in the system, such as IT Admin, or Human Resource Admin.

Normally, a role can only be exercised in the administrative group for which it was created. Therefore, if you want one administrator to manage several administrative groups, you must assign the administrator a role created for each group. An administrator with roles in several groups can only administer one group at a time.

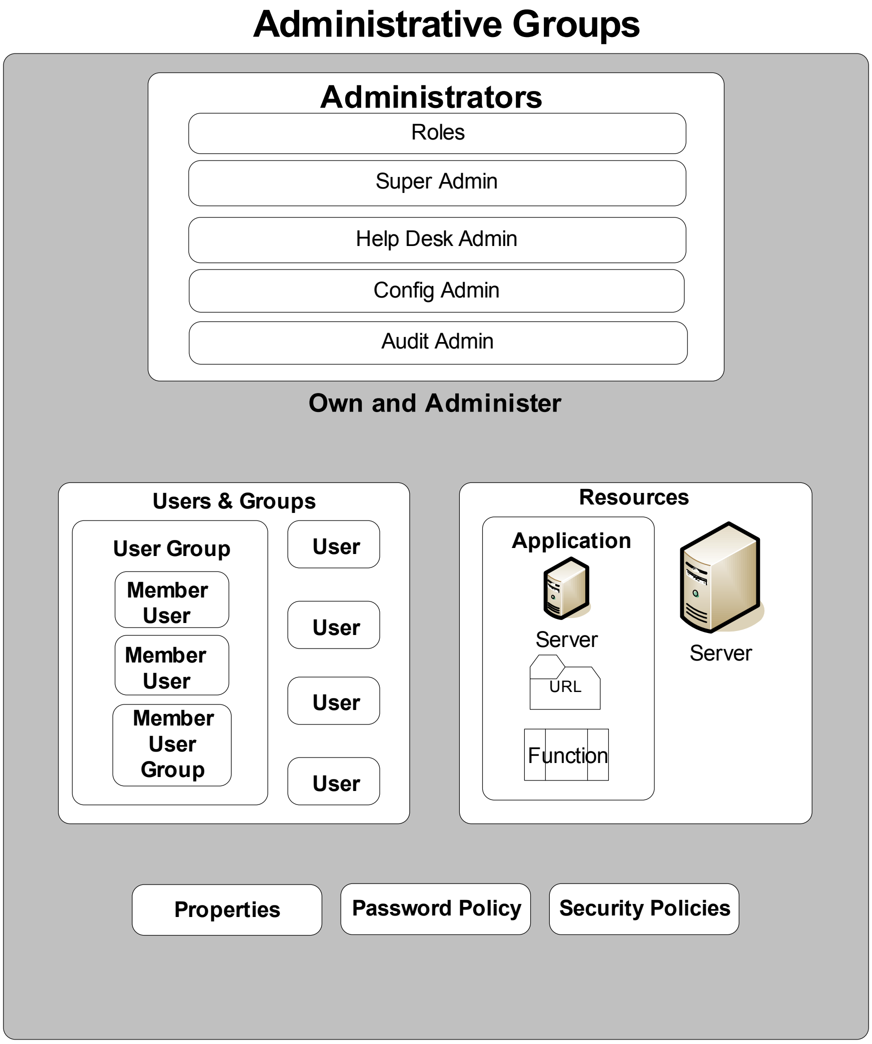
Though a role typically applies only to a single administrative group, it is possible for an administrator to assume the same role in more than one group. A role created for one group can be assumed in another group if the groups have a parent-child relationship. For example, if Group A is the designated parent of Group B, administrators in Group A who have logged on with a Group A role can also exercise that role in Group B. This makes it possible for an administrator to manage objects in both Group A and Group B without having to switch roles.

Administrative Groups

An administrative group is a collection of Access Manager objects such as:

- Users
- User groups
- Applications
- Servers
- Properties
- Roles

You can create several different administrative groups based on the needs of your organization. For example, administrative groups can be based on organizational structure and reflect departmental divisions, such as Marketing, Sales, Shipping, and Engineering. They can also be based on geography with separate groups created for the regions or administrative centers of your organization. Each of these groups can then be managed by the administrators best able to deal with the needs of each administrative group. The following figure is an example of the types of administrative groups that you can create.



Example

Company A has headquarters in Boston, Massachusetts, and has:

- Manufacturing operations in Pittsburgh, Pennsylvania
- Customer support operations in Charlotte, North Carolina

- Sales offices in the United States and Europe

The IT department at Company A might set up administrative groups in the following manner:

- An administrative group for each of the Boston, Pittsburgh, and Charlotte locations. An administrator at each site administers the administrative group for their respective site.
- Because each of the sales offices has only one or two employees:
  - An administrative group for all of the United States sales offices
  - An administrative group for all of the European sales offices

  A single administrator in the Boston headquarters administers both of these administrative groups.

Password Policies

Each administrative group must have a password policy. A password policy is a set of rules that establish the required length of passwords, restricted characters or words, the maximum password lifetime, password expiration dates, and user lockout rules. If you do not create a password policy, the system automatically assigns the default password policy.

When designing a password policy, balance the needs of your users with your security requirements. An excessively strict password policy, for example, one that requires overly long passwords or very frequent password changes, may cause users to compromise security, most commonly by writing down their passwords.

In addition, you can customize your password policy using the excluded words file, **words.txt**, which prohibits the use of certain words as passwords. By adding words, such as the name of your company to this file, you can restrict words that are particular to your situation. For more information, see the *Servers Installation and Configuration Guide*.

Planning User Organization

In planning how to organize your Access Manager users, you need to decide:

- Which properties users will have
- Which groups the users will belong to

User Properties

Access Manager users are stored in a data store such as LDAP or SQL. You can administer Access Manager users with the Administrative Console or with the native administration tools of your data store. RSA recommends that you use the Administrative Console to administer only those users added through the Administrative Console. Use the native administration tools of your data store to administer all other users.

A property is a custom data field that is specific to your organization, that you define, and in which you can store user information. The primary purpose of properties is to create evaluation criteria for Smart Rules that are used to control access to a resource. Properties can include any data that your organization stores or maintains for its users, such as age, account status, department, date of hire, customer type, and so on.

Note: If you are using an LDAP directory, you must map properties to attributes in your data store.

If you are using an LDAP directory, you can create properties with more than one value. For example, you can define a property called phone number, and enter multiple phone numbers for each user.

You can also define external properties. External properties are properties which have values that are stored in an external data store. You identify an external property in the Administrative Console. You also must create a property provider, which is the process or procedure that retrieves the property value from the external data store. You use the Property Provider API to create the external provider. For more information, see the *Developer's Guide*.

You can configure Access Manager to automatically publish selected property values to the HTTP header. This allows any Access Manager Runtime API client program to read the property values.

For more information about properties, see the chapter "Managing Security Policies" in the *Administrator's Guide*.

User Groups

To help you organize access to resources protected by Access Manager, you can create user groups. User groups include users as well as other user groups. A user that belongs to a user group is called a member user. A user group that belongs to another user group is called a member group. Users can belong to more than one user group.

User groups allow you to use entitlements and Smart Rules to grant or deny resource access to groups of users, rather than to one user at a time. An entitlement granted to a user group is automatically granted to all members of the group.

When you plan your logical deployment:

- Take an inventory of the types of users who access the system.
- Identify the structure of your organization and set up groups to mirror that structure.
- Determine which users belong to which groups and which groups belong to other groups.

You can organize your users into groups to fit the needs of your organization. For example, a school might create three groups:

- A group called Teachers, with access to word processing software, database software, student records, assignments, and test answers
- A group called Students, with access only to software and assignments

- A group called Administration, with access to all of the above plus teachers' salaries

Nested User Groups

Access Manager supports nested user groups, which is the practice of adding one user group to another user group. Nesting groups allows your Access Manager organization to more closely resemble your organization's hierarchy, which makes administering your system easier. For example, you can include all managers in a user group called Managers, and you can include all senior managers in a member group called Senior Managers, which is nested in the user group Managers. You can then allow different levels of access to each level of nesting. For example, managers might be allowed access to all resources relating to current projects but only senior managers would be allowed to access resources relating to strategic planning.

Planning Resource Protection

In planning to protect your resources with Access Manager, you need to determine:

- Which resources need protection.
- How to group these resources.

Resources are the objects that you protect with Access Manager:

- Servers
- URLs
- J2EE objects such as Enterprise Java Beans (EJBs)
- Files on a server
- Functions

Applications

When you protect resources with Access Manager, you must add them to an application. An application is a "container" for resources. It can contain one resource or several. Typically, resources within a single application are related. For example, an application might include directories and URLs that contain information for your Human Resources department. Different resources within a single application do not have to reside in the same directory, or even on the same server. For example, if you have two directories that contain related information but are located on different servers, you can add them to the same application.

When you grant access to resources, you can grant access to the individual resource, or to the entire application that contains the resource. For example, suppose you have an application that contains a group of URLs. You can grant access to an individual URL or to all the URLs in the application.

When you plan your logical deployment, identify the resources on your network, and determine logical groupings for the resources you want to protect.

After you identify all the resources you want to protect and decide how to group them, you can begin creating applications using the Administrative Console. For more information about applications, see the chapter "Managing Resources" in the *Administrator's Guide*.

Functions

A function is an Access Manager representation of a function or method in any type of custom application that you build. Modeling a method as a function allows Access Manager to control access to that method. This allows you to implement RSA Access Manager Agent-like controls (similar to building an Access Manager WAX) governing access to methods in your custom applications.

Example

If you create a non-web Java application that has a sensitive method that you do not want to make available to all users, you can govern access to this method by creating a function for it.

For a method called updateBalance(), you can create a function entry in the Administrative Console with the following name, description, and policy conflict resolution setting:

Name. updateBalance.

Description. Allows users with the appropriate credentials to access update account balances.

Policy Conflict Resolution. Deny access when policy conflicts occur.

Assuming that the updateBalance function has been integrated with Access Manager through the API, you can apply Smart Rules or entitlements to this application-level resource using the defined name.

When setting policies in the Access Manager system, you treat a function like you would treat a URL. That is, you collect related functions (along with any related URLs) into applications, and you grant users or user groups permission to use these applications, functions, and URLs. For more information about adding a function, see the Help topic "Adding a Function."

If you are not building stand-alone applications, you generally do not need to use functions. For most dynamic web content such as Common Gateway Interfaces (CGIs) on web pages, you control access by creating a URL that matches the URL request string or the name of the CGI script being called. Once you have created Entitlements based on these URLs, the RSA Access Manager Web Server Agents can control access to the functions in the CGI script. In contrast, functions are useful for access checking in situations that do not involve URL requests, that is, in situations where the RSA Access Manager Agents cannot be used.

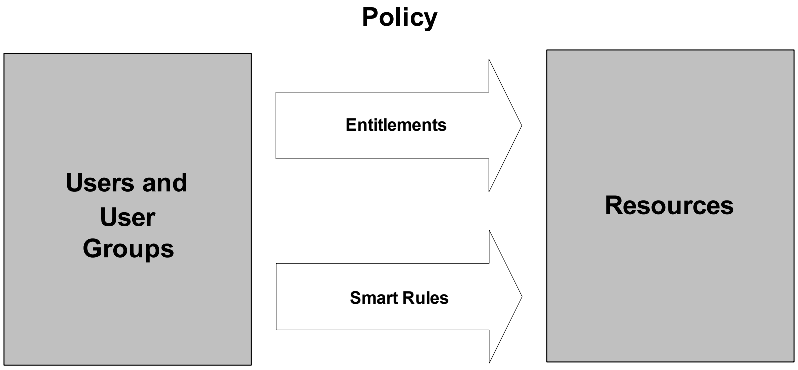
Planning Your Security Policy

To protect your resources with Access Manager, you need to decide:

- Who will be allowed access to protected resources.

- How the resources will be protected.

You control access to resources with security policies. The following figure shows the two methods used by Access Manager to create a security policy—entitlements and Smart Rules.



Entitlements

You use entitlements to allow or deny a user or user group access to a resource. Entitlements are the most specific type of security policy. They always take precedence over Smart Rules. Use entitlements when you want to:

- Explicitly grant a user or user group access to a resource.
- Explicitly deny a user or user group access to a resource.

Example

- If a user must always be allowed access to a protected resource, such as a web server, create an entitlement that grants the user access to the web server. After you create the entitlement, the user is always allowed access to the web server.
- If a user must never be allowed access to a protected resource, such as an application server, create an entitlement that denies the user access to the application server. After you create the entitlement, the user is always denied access to the application server.

You create entitlements in the Administrative Console. You can specify two types of entitlements:

User entitlements. Entitlements assigned at the user level that affect only one specific user.

User group entitlements. Entitlements assigned at the user group level that affect all member users and member groups in the user group.

Resolving Conflicting Entitlements

Because entitlements can exist both on the user and user group level, conflicting entitlements sometimes occur. If entitlements conflict, access is resolved according to the most specific match with the resource. This means that user entitlements take priority over user group entitlements.

For example, if an entitlement allows the user group West Coast Users access to the resource shipping/index.html, all members of West Coast Users are allowed access to shipping/index.html. Chris Jackson is a member of West Coast Users who has an entitlement that specifically denies access to shipping/index.html. In this case, all members of West Coast Users are allowed access to shipping/index.html, except for Chris Jackson.

In a similar way, member user group entitlements take priority over entitlements on user groups that include them. Security policies based on resources and functions take priority over security policies based on the applications that include them. For more information about entitlements, see the chapter "Managing Security Policies" in the *Administrator's Guide*.

When specificity is equal, the policy conflict resolution setting for the resource determines the resolution of conflicting entitlements. For more information, see "Policy Conflict Resolution" on page 50.

Smart Rules

You use Smart Rules to allow or deny a user access to a resource based on the value of a user property at the moment the user attempts to access the resource. You can apply Smart Rules to any resource.

When a user tries to access a protected resource, Access Manager checks the user properties associated with the Smart Rules protecting the resource and grants or denies access based on each Smart Rule's criterion.

Example

Users have a property called Job Title. A resource, payroll.html, is protected by a Smart Rule that only allows access to users whose Job Title is "Manager."

If a user whose Job Title is "Clerk" tries to access payroll.html, Access Manager checks the user's Job Title property to see if the user must be allowed access. Because the user's Job Title is Clerk, the user is denied access.

However, if a user whose Job Title is "Manager" tries to access payroll.html, the user is allowed access, because the user's Job Title meets the necessary criterion at the moment access is attempted.

Smart Rule Evaluation

There are three types of Smart Rules—Allow, Deny, and Require. These three types can be combined in various ways to implement business rules in controlling access to a resource. If Smart Rules of different kinds all protect a resource, the order in which they are evaluated is governed by the policy conflict resolution setting applied to the resource. For more information, see the following section, "Policy Conflict Resolution."

Smart Rules decide a user's access to a specified application only if no relevant entitlement exists at any level (user or group). Entitlements always take precedence over Smart Rules.

For more information on entitlements and Smart Rules, see the chapter "Managing Security Policies" in the *Administrator's Guide*.

Policy Conflict Resolution

For each application or resource you create in Access Manager, you select one of the following policy conflict resolution settings:

- Allow access when policy conflict occurs (default).
- Deny access when policy conflict occurs.

You can change this setting when you edit an application or resource.

The policy conflict resolution setting is important when the system makes access control decisions. If one rule allows access and another rule denies access to a given resource, and the rules are of equivalent specificity, the system checks your policy conflict resolution setting to decide which rule takes priority.

Therefore, when setting the policy conflict resolution setting for a given resource, you must consider the sensitivity of the resource and the manner in which you want to resolve conflicting access rules to the resource. To allow access when access rules conflict, set the policy conflict resolution setting for each resource to "allow access in case of conflict." To deny access when access rules conflict, set the policy conflict resolution setting for each resource to "deny access in case of conflict."

In the case of Smart Rules, when the default conflict resolution setting, "Allow access when policy conflicts occur," is selected, Allow rules are evaluated first, then Deny rules, and finally Require rules. When the alternative setting, "Deny access if policy conflicts occur," is selected, Deny rules are evaluated first, then Allow rules, and finally Require rules. The Smart Rules are evaluated until a user is either denied or allowed access.

Index