Rsam Platform

Integration with Third-Party Directories & Authentication Providers

Version: 9.2 | December 2018

Contents

Overview

The Rsam platform provides a robust set of security features that can be leveraged by customers to authenticate and manage their user base. This guide provides recommendations and an overview on the use of third-party User Directory and Authentication mechanisms with Rsam. While Rsam includes its own mechanisms for user management and authentication, customers may need to integrate Rsam with tools they have already standardized in their organizations.

Definitions

The following definitions must be understood before reading this guide:

LDAP: Lightweight Directory Access Protocol (LDAP) is a networking protocol that applications can use to query information from a centralized directory, such as Active Directory. This protocol is commonly used to allow Rsam to lookup users from the customer's corporate user directory.

Active Directory: Active Directory (AD) is a directory service developed by Microsoft and included in most Windows Server operating systems. Many organizations use Active Directory to centralize the management of their users and authentication.

Single Sign-on: Single Sign-On (SSO) mechanisms allow users already authenticated to one application (such as a corporate domain) to automatically be authenticated to a series of other applications, such as Rsam. In Rsam, SSO is commonly used to allow Administrators and end-users already authenticated to the customer's corporate directory to access Rsam without having to re-authenticate.

SAML: Security Assertion Markup Language (SAML) is a standard format for implementing SSO. It is an open standard that allows security credentials to be shared across multiple applications by allowing one application to perform certain security functions on behalf of other applications, primarily authentication.

SAML Identity Provider: A system entity that issues authentication assertions in conjunction with an SSO profile of the SAML.

SAML Service Provider: A system entity that receives and accepts authentication assertions in conjunction with an SSO profile of the SAML.

TFA: Two-Factor Authentication (TFA) adds an additional security layer to the user authentication process by requiring a unique token in addition to the normal login and password. In Rsam, unique tokens are sent through email, text, or an automated phone voice system.

Users and Groups in Rsam

Individuals accessing Rsam use user accounts that are stored in the Rsam platform. Users are assigned a role(s) and permissions directly or through a user group. These user accounts and groups can be created in Rsam by any of the following methods:

- Created manually in Rsam by an Administrator through the user interface or Rsam API. User Directories are not required in this case.
- Imported into Rsam from a standard data source (such as an Excel file or database query). User Directories are not required in this case.
- Imported into Rsam from a Directory search (such as an LDAP call to Active Directory).
- Automatically created when a user is assigned to an object or record through a Directory lookup.
- Automatically created when a user accesses Rsam for the first time through an SSO mechanism.

Note: Rsam includes settings and options to help manage user experience. Refer the *Rsam Online Administrator Help* for guidance around such user options.

Default Users in Rsam

The Rsam installation package includes a series of pre-defined users. Customers can use these user accounts as required. The following table lists the default users in Rsam.

User ID	Purpose	Recommendations
Administrator	The *Administrator* user is an account with access across all administrative items in Rsam. This is the only account with the *Super User* flag set and cannot be deleted or locked.	Set a strong password for this user. Use this account only if you get locked out of your other Rsam accounts.
R_ADMIN	This is a pre-defined user with *Account Admin* access and has been assigned most roles in Rsam. This is the easiest user to access Rsam in the beginning and explore the console.	Set a strong password for this user. Use this account to explore all areas of Rsam. Delete this user before Rsam goes live in your organization.
R_<sample user>	The pre-defined accounts that start with *R_* are explained in the *Rsam Step-by-Step Tutorials* and are used to provide an experience of certain roles and workflow. You can use these accounts when going through the tutorials and training.	Use these accounts to follow the *Step-by-Step Tutorials* and to experience specific roles. Delete all such users before Rsam goes live in your organization.

LDAP Integration with Rsam

User Directories, such as Active Directory, can be very useful when you want Rsam to leverage a centralized repository containing the user information. When setup correctly, LDAP can be used in the following scenarios:

- When performing a lookup for a possible user within the organization, Rsam can use one or more directories. This means you can leverage a user base that does not yet have an account in Rsam when selecting users for assignment, attribute lookups, and more.

  For example, if you want to assign the user, *John Doe*, to complete an assessment, you can type in John's name or directory ID and Rsam searches the corporate directory for that user. If a match is found, Rsam can automatically create an Rsam account for him so that he can access his assigned assessment.

  Note: Rsam is licensed by the number of user accounts. However, you can locate any number of users in a directory without using any of your licensed user count. Users licenses are only counted if a user is established in Rsam (through direct permission assignment or through directory import).

- When directly importing users from an LDAP directory, Administrators can choose to import a series of users from the directory into Rsam. This is *not required* as Rsam queries the directories whenever looking up users. But customers can choose to import their users in advance to minimize the number of LDAP calls. Each user imported into Rsam will consume a user license count.
- Authenticating a user:
  - In addition to a directory lookup, customers can have Rsam pass the user authentication directly to the directory server. This means that users can use the same login and password that they already use with their other corporate applications.
  - When configuring users to authenticate to a directory, Rsam does not create, store, or manage passwords for those users. In that case, the password management is done through the directory service.

Note: Customers manage their own directory environment / infrastructure and *Rsam Customer Support* can provide guidance on Rsam configurations to connect to the customer directory. Rsam will be unable to help with any setup of customer's Directory environment.

Directory Connectivity

To leverage a directory, Rsam Web Server needs to access that directory over the network. Customers using the Rsam cloud offering require a VPN connection and access to the appropriate LDAP / Directory TCP & UPD Ports. For more information, see Connecting to VPN. If LDAPS is used, a trust must be established by using a trusted certificate.

Leveraging TFA with Rsam

When users are authenticating through a login / password, Administrators can enforce Two-Factor-Authentication. TFA can be required for individual users, groups of users, or across all users in Rsam. When TFA is enabled, users entering a password will also be required to enter a token string. This string will be sent to the user through the user's preferred method (an email, a text message, or an automated voice call).

Note: The Rsam TFA feature is not available for users leveraging SSO. If TFA and SSO are required, TFA will need to be implemented in the SSO IDP.

Leveraging SSO with Rsam

All Rsam users, whether an internal user authenticated by Rsam or a directory user authenticated by LDAP, need to enter a login and password on the Rsam Sign-In page. This manual authentication can be eliminated by the of SSO mechanism.

Note: SSO mechanism is not related to the user lookup / directory search capabilities of Rsam. SSO is only an authentication mechanism. For Rsam to search for users / assign users from the directory, the directory connectivity must be established separate from SSO.

Customers that have installed and configured an SSO mechanism, like a SAML2 service, can allow their users to authenticate to their own SSO application or portal, and the authentication of that application will be accepted by Rsam (bypassing the Rsam authentication page). For this, Administrators must establish a trust relationship between the SSO application and Rsam. On successfully establishing this, users will no longer need to enter their login / password on the Rsam Sign-In page.

Note: Customers manage their own directory environment / infrastructure and *Rsam Customer Support* can provide guidance on Rsam configurations to connect to the customer directory. Rsam will be unable to help with any setup of customer's Directory environment.

Connecting to VPN

Corporate Directories such as LDAP and Active Directory are usually hosted within the protected network of organizations and are inaccessible to the outside world. Customers using the Rsam cloud can leverage a Virtual Private Network (VPN) connection between the Rsam AWS network and their own network. While this is not always required, this can be a requirement when leveraging an LDAP connection.

You can check with your organization's Network Administrators to determine if you need to use a VPN connection.

Configuring Directory / LDAP

For detailed information about configuring Directory / LDAP Access, see the *Rsam Online Administrator Help*.

Configuring SSO / SAML Authentication

For detailed information about configuring SSO / SAML Authentication, see the *Rsam Integration with SAML-based SSO Guide*.