RSA

RSA Archer Platform

Security Configuration Guide

6.8

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:
https://community.rsa.com/community/support.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and Dell are either registered trademarks or trademarks of Dell Corporation ("Dell") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to https://www.dell.com/learn/us/en/uscorp1/terms-conditions/trademarks-us?s=corp#rsa.

License agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on RSA.com. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

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.

For secure sites, Dell recommends that the software be installed onto encrypted storage for secure operations.

For customers in high security zones, Dell recommends that a full application sanitization and reinstallation from backup occur when sensitive or classified information is spilled.

Note on Section 508 Compliance

The RSA Archer® Suite is built on web technologies which can be used with assistive technologies, such as screen readers, magnifiers, and contrast tools. While these tools are not yet fully supported, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for RSA Archer.

The RSA Archer Mobile App can be used with assistive technologies built into iOS. While there remain some gaps in support, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer Mobile App.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. Use of the software described herein does not ensure compliance with any laws, rules, or regulations, including privacy laws that apply to RSA's customer's businesses. Use of this software should not be a substitute for consultation with professional advisors, including legal advisors. No contractual obligations are formed by publication of these documents.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

Preface

About this Guide

This guide provides an overview of security configuration settings available in the RSA Archer Platform and security best practices for using those settings to help ensure secure operation of RSA Archer® Suite.

RSA Archer Documentation

You can access RSA Archer documentation on the Archer Customer/Partner Community on RSA Link at: https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/documentation.

The following table describes each document.

Document	Description
Release Notes	A list of issues fixed in the release, a list of issues known at the time of the release, and an overview of the new and updated features in the current release. Available in an Excel workbook.
Installation and Upgrade Guide	Instructions for installing the latest RSA Archer release, and upgrading from 5.x and 6.x to the latest release. Available in PDF format.
Online Documentation	Information for using RSA Archer including how to set up and maintain the Platform, how to use the Platform features, how to use the RESTful, Web and Content APIs, security configuration information, and how to install and use the solution use cases. Available from within the product in HTML5 format using context-sensitive links, as well as in a ZIP format for local installation. The Online Documentation is also available in full on the RSA Archer Community on RSA Link at: https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/documentation.
Archer Control Panel (ACP) Help	Information for using the RSA Archer Control Panel module to manage the internal settings of the Platform, such as license keys, global paths and settings. Available from within the ACP module and in a ZIP format for local installation.

Document	Description
Planning Guide	Information about how to plan for your new RSA Archer installation. This document is intended for system administrators who are responsible for installing and managing RSA Archer. Available in PDF format.
Qualified and Supported Environments	Information on the required software platforms for running RSA Archer. This document is available on the RSA Archer Community on RSA Link at:https://community.rsa.com/docs/DOC-102657.
Security Configuration Guide	Information about security configuration settings available in the RSA Archer Platform and security best practices for using those settings to help ensure secure operation of RSA Archer. Available in PDF format.

Support and Service

Customer Support Information	https://community.rsa.com/community/support
Customer Support E-mail	archersupport@rsa.com

Other Resources

Resource	Description
RSA Archer Community on RSA Link	Our public forum, on the RSA Link Community platform, brings together customers, prospects, consultants, RSA Archer thought leaders, partners and analysts to talk about risk and compliance as a practice, and includes product demos, videos, white papers, blogs and more. https://community.rsa.com/community/products/archer-grc
RSA Archer Customer / Partner Community on RSA Link	Our private community, is a powerful governance, risk and compliance online network that promotes collaboration among RSA Archer customers, partners, industry analysts, and product experts. Engaging with the RSA Archer Community on RSA Link enables you to collaborate to solve problems, build best practices, establish peer connections and engage with RSA Archer thought leaders. https://community.rsa.com/community/products/archer-grc/archer-customer-partner-community

Resource	Description
RSA Ready	RSA's Technology Partner Program is where third parties gain access to RSA Software in order to develop an interoperability and have it documented and certified. RSA Ready certifications are posted to an online community and supported by RSA Support. https://community.rsa.com/community/products/rsa-ready
RSA Exchange for RSA Archer	The RSA Exchange for RSA Archer offerings help you rapidly deploy adjacent or supporting risk business processes, quickly integrate new risk data sources, and implement administrative utilities to make the most out of their risk and compliance investment. https://community.rsa.com/community/products/archer-grc/exchange

Chapter 1: Security Configuration Settings

User Access Control

Access control provides a framework for maintaining users, roles, and security parameters, and for assigning access rights at the system, application, record, and field levels.

- User accounts allow users to log on to RSA Archer.

- User groups provide a means of grouping users based on organizational structure or geographic locations.

- Access roles are collections of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete).

- Security parameters are rules for controlling user access to RSA Archer and its individual pages.

- LDAP synchronization streamlines the administration of users and groups by allowing updates and changes that were made in the LDAP server to be reflected automatically in RSA Archer.

It is important to have well-defined policies around Help Desk procedures for your RSA Archer installation. RSA strongly recommends that your Help Desk administrators understand the importance of password strength and the sensitivity of data, such as user logon names and passwords. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks. Train end users to provide, and Help Desk administrators to request, the least amount of information needed in each situation.

Preventing social engineering attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that they can then use to gain access to protected systems. RSA recommends that you use the following guidelines to help reduce the likelihood of a successful social engineering attack:

- If Help Desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call the Help Desk back at a well-known Help Desk telephone number to ensure that the original request is legitimate.

- The Help Desk telephone number should be well known to all users.

- Help Desk administrators should only ask for user name of the user over the phone when they call the Help Desk. Help Desk administrators should never ask for user passwords.

- Help Desk administrators should authenticate the user's identity before performing any administrative action on a user's behalf. RSA recommends that you verify user identity using the following methods:

  - Call the user back on a phone owned by the organization and on a number that is already stored in the system.

    Important: Be careful when using mobile phones for identity confirmation, even if they are owned by the company because mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.

  - Send an email to the user at a company email address. If possible, use encrypted email.

  - Work with the manager of the employee to verify the user identity.

  - Verify the identity in person.

  - Use multiple open-ended questions from employee records. For example: "Name one person in your group." or "What is your badge number?" Avoid yes or no questions.

Advice for your users

RSA recommends that you instruct your users to do the following:

- Never give their passwords to anyone, not even to Help Desk administrators.
- Change their passwords at regular intervals.
- Be aware of what information requests to expect from Help Desk administrators.
- Always log off from the RSA Archer web interface when finished.
- Always lock their desktops when they step away from their computers.
- Regularly close their browser and clear their cache of data.
- Do not upload any files to RSA Archer from sources other than themselves.
- Never enable active content when opening CSV files with spreadsheet applications like Microsoft Excel or LibreOffice Calc.

Note: RSA recommends that you conduct regular training to communicate this guidance to users.

Entity permissions

RSA Archer supports user permissions on multiple system components. RSA recommends that you grant permissions only to users who need to access these components. When granting permissions to these components, RSA recommends that you do not select the Everyone group because that group grants rights for all users. Additionally, RSA recommends that you review the granted permissions on a routine basis to ensure that the correct access is granted to the users.

The following table explains how user permission is configured on the supported components.

Component	Permissions Explanation
Workspaces, Dashboards, Global iViews	Configured from the Access tab in a workspace or dashboard. RSA recommends that you configure these components to be private.
Global Reports	Configured when you save a report. RSA recommends that you set the Permissions field to Global Report.
Record Permissions	Configured in a Record Permissions field in an application or questionnaire.
Field Permissions	Configured in the Access tab in a field in an application or questionnaire. RSA recommends that you configure fields to be private.

Component	Permissions Explanation
Configuration Administrators	Configuration administrators have rights to the configuration aspects (for example, fields, layout, data-driven events, notifications) of an application, questionnaire or sub-form. Configuration administrators have read rights to the content page for the application or questionnaires.
Content Administrators	Configured in applications and questionnaires. Inherently grants CRUD rights to all content within the application or questionnaire regardless of record permissions.
Global Report Administrators	Configured in Application Builder for the assigned report owners in a specific application or questionnaire.
Discussion Forum Roles	Configured in Discussion Forums. Discussion forum roles provide administration and forum creation rights for specific discussion communities.

Default User Accounts

The following table describes the default RSA Archer user accounts of a System Administration (sysadmin) account and several RSA Archer services accounts. When creating a new instance, the installer requires the user to enter a password for the sysadmin and service accounts.

It is important to remember the following:

- Standard users cannot log on to any of the default user accounts. Only the System Administrator can log on to the sysadmin account.

- You cannot delete or rename any of the default user accounts.

User Account	Description
sysadmin	The system administrator account for RSA Archer. This account can be disabled, but cannot be deleted or renamed.
userArcherAssetServer	A service account for the Asset service. This account can only be used by RSA Archer services.
userArcherAsyncService	A service account for job management. This account can only be used by RSA Archer services.
userArcherCalculationAccount	A service account for calculations. This account can only be used by RSA Archer services.

User Account	Description
userArcherDataFeedService	A service account for data feeds. This account can only be used by RSA Archer services.
userArcherLdapService	A service account for LDAP synchronization. This account can only be used by RSA Archerservices.
userArcherNotificationService	A service account for notifications. This account can only be used by RSA Archer services.
userMigrationUser	A service account for migration. This account can only be used by the installer.
userOfflineService	A service account for Offline Access. This account can only be used by RSA Archer services.

Adding User Accounts

You must create a user account for each user who needs access to RSA Archer. Login credentials are the same on the mobile device as they are for RSA Archer. Mobile users log in to mobile devices using their user name and password that is established in their user account.

Configuring new accounts

Each RSA Archer user must have an account to log on to the system.

New User Accounts

All new user accounts must have a unique password, generated under one of the following sets of circumstances:

- The system administrator assigns the password manually. RSA strongly recommends that you enable the Force Password Change with the Next Sign-In option in RSA Archer for all new user accounts. Configuring this option requires the user to change the password after the first successful logon attempt.

- If the single sign-on feature is in place on your system, RSA Archer automatically creates a random password for each new user.

Important: RSA strongly recommends that you ensure users are approved for logging on to the system before creating an account for them. Even when users are approved, RSA recommends that you only assign the minimum set of access permissions for users to perform their job.

New User Account with System Administrator Privileges

RSA recommends that you create a new user account and assign the System Administrator access role to it. This access role grants the account all rights within RSA Archer.

Important: RSA recommends that before issuing this account, you ensure that the user is approved for full access to the system.

Platform User Accounts

RSA Archer enforces the password strength, logon, and session time-out policies specified by the security parameters defined in the Administration workspace.

Note: These security parameters are enforced by RSA Archer across all user accounts except the sysadmin and service accounts. RSA strongly recommends that you instruct your administrators on your corporate IT policy and security best practices for generating and managing passwords for all accounts.

The following table shows the default security parameters settings for password strength.

Parameter	Setting
Minimum password length	9 characters
Alpha characters required	2 characters
Numeric characters required	1 character
Special characters required	1 character
Uppercase characters required	1 character
Lowercase characters required	1 character
Password change interval	90 days
Previous passwords disallowed	20 passwords
Grace logons	0 logon
Maximum failed logon attempts	3 attempts
Session time-out	10 minutes (sysadmin account)
	10 minutes (user account)
	30 minutes (service account)
Account lockout period	999 days

RSA recommends that you treat these settings as the minimum requirement for enforcing strong passwords and secure sessions in RSA Archer.

Important: Regardless of the security parameter settings, RSA Archer passwords cannot contain more than:

- Three consecutive matching characters, for example aaaa.
- Three consecutive characters from the user name.

Add a user account

1. Go to the Manage Users page.

   a. From the menu bar, click .

   b. Under Access Control, click Users.

2. Click Add New.

3. In the General Information section, enter the name of the user, the user name for log on, and the domain.

   The following table describes each property.

Property	Description
First Name, Middle Name, and Last Name	The valid name of the user. First and last names are required.
User Name	A seven character system-defined name in all lowercase. The user name contains the first six characters of the Last Name followed by the first character of the First Name. If the Last Name is fewer than six characters, the system uses additional characters from the First Name to make a seven-character user name. If the user name is not unique in the domain, the system appends a number (up to 999) to the end of the name to make the name unique.
User Domain	If your RSA Archer instance has one or more Lightweight Directory Access Protocol (LDAP) configurations defined, select the domain to which the user is a member. To use the RSA Archer domain, select No Domain.

4. (Optional) In the Contact Information section, enter the default email address and any other

pertinent information for contacting the user.

The following table describes each property.

Property	Description
Address	The complete address of the user.
Company	The company name.
Title	The title of the user.
Email	The following user email types are available: • Business • Mobile 2 • Business 2 • Other • Home • Other 2 • Home 2 • Pager • Mobile
Phone	The following user telephone number types are available: • Assistant • ISDN • Business • Mobile • Business 2 • Mobile 2 • Business Fax • Other • Home • Other 2 • Home 2 • Other Fax • Home Fax • Pager

5. (Optional) In the Localization section, enter the time zone, locale, and language if the location and language of the user is different from the system.

The following table describes the options.

Option	Description
Time Zone	The time zone for the location of the user. Time is based on Coordinated Universal Time (UTC). All time is stored as UTC and converted based on the time zone of the user.

Option	Description
Locale	The physical location of the user.
Manually select a language	Overrides the default language set for the instance. When you select this option, you must specify the language.

6. In the Account Maintenance section, enter the user password and assign the security parameter for this user.

The following table describes each property.

Property	Description
Status	The current status of the user account. The options are Active, Inactive, or Locked.
Password	For new user accounts, the password must be entered and confirmed. These entries must match exactly. The password must conform to the default security parameter password rules.
	For existing user accounts, use the Change Password link to change the password manually.
	The Send user a notification with password information option enables RSA Archer administrators to notify new users that the user account has been setup with a temporary password and may require a password change.
Force Password Change	Determines whether the user is forced to change the password the next time the user logs in.
Security Parameter	The security parameter assigned to the user. A user can only have one security parameter assigned at a time.
Notifications, Subscriptions	Enables users to select the records and applications for which they want to receive notifications when an update occurs.

Property	Description
Default Home Page	Sets a user's default home page to use either a task-driven landing page or a dashboard based on group, role, or user profile. If the user belongs to multiple roles or groups, the home page is based on the most recently assigned role or group. Once the user logs in, the selected home page becomes default and any changes to the home page of the role or the group do not affect the user's default home page. **Note:** If the user's permission to access the dashboard assigned to the home page is revoked, a message appears upon log in allowing them to select a new home page. **Important:** If the administrator sets the default home page while the user is logged in, the user must click the Home button to refresh the home page setting. If the user changes the default home page selection, the change is applied upon clicking Save.
Default Home Dashboard	Sets which dashboard displays on the default home page.
Enable Advanced Workflow Actions by Email for this user	Allows this user to complete simple advanced workflow actions from their email. **Important:** To use Advanced Workflow Actions by Email, you must have a user account with Advanced Workflow Actions by Email enabled. You must also ensure that Advanced Workflow Actions by Email is enabled in all applicable applications, questionnaires, notification templates, and advanced workflows.

7. (Optional) Select the Send user a notification with password information checkbox if you want to send the user an email notification of the password change.

   Note: If you do not select this checkbox, you must inform the user of the new password. The Default Email address is used for the notification email.

8. (Optional) In the Notes section, record any additional information about the user account, for example, list hours of availability or preferences for how the user should be contacted. Account notes appear when users click a linked user name in RSA Archer to view the user profile.

9. Click Save or Save and Close.

- Click Save to apply the changes and continue working.

- Click Save and Close to save and exit.

Access Roles

An access role is a collection of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete). For example, the access role of a General User can allow access only to applications, and the access role of an Administrative User can allow access only to RSA Archer features. RSA recommends that you assign permissions through group membership, and not assign permissions directly to user accounts.

RSA Archer includes an access role called System Administrator that you cannot delete or modify. The System Administrator role grants users unrestricted access to all RSA Archer features and to all records stored in applications, including records enrolled in content review. Only System Administrators can assign the System Administrator access role.

RSA Archer solutions include predefined access roles for use with the solution.

For instructions on assigning permissions through group membership, see Assigning Access Roles to Users and Groups.

As the number of users, groups, and applications increases, keeping track of who has access to what becomes more complex. RSA recommends simplifying the process. If you create granular access roles for each of your applications, for example, Policy Administrator, Policy Author, and Policy Reader, you can grant access to new or existing users and groups by selecting from a list of predefined access roles.

Importing access roles

Although access roles are supported objects in the packaging process, when you import access roles with groups during the packaging process, you must manually associate each access role to the respective group. After the package is installed, you must manually add users to each group in the target instance.

Adding Access Roles

RSA Archer supports role-based access control. RSA Archer allows you to create access roles that you can assign to users. Each access role is mapped to a list of user authorization settings. User authorization settings control rights or permissions that are granted to a user for accessing a resource managed by RSA Archer.

Creating an access role defines the application and page-level rights for all users assigned the role.

Page-level rights

The following table describes page-level rights.

Rights	Description
Create	Create new page content, such as records, fields, notification templates, and content review stages.
Read	Read page content.
Update	Modify existing page content.
Delete	Delete page content.

Add an access role

1. Go to the Manage Access Role page.

   a. From the menu bar, click .

   b. Under Access Control, click Access Roles.

2. Click Add New.

3. Do one of the following:

   - If you want to create a new access role, click Create a new Access Role from scratch, and then click OK.

   - If you want to create a new access role from an existing access role, click Copy an existing Access Role. Select the access role from the Access Role list, and then click OK.

4. In the General Information section, enter a name and description for the access role.

5. (Optional) To enter an Alias, click Apply, and then enter an Alias name.

6. (Optional) To set access role as the default for all users and groups, in the Default Access Role field of the Default Access Role section, click Assign as Default.

7. (Optional) In the Group Assignments section, assign groups to the access role.

8. Click Apply.

9. On the Rights tab, and select the (Create, Read, Update, and Delete) checkboxes that correspond to the appropriate rights for each page type.

   - User or group access to the Manage Global Values Lists page provides access to all global values lists in RSA Archer. If you want a user to have access to specific global values lists and not all lists, select the appropriate CRUD access for the individual global values list.

- If you grant access rights to import data, you must also grant rights to the content record that data will be imported into. For example, users can import data into the Policies application only if they have access to Integration: Data Imports; Create, Read, and Update rights to Policies: Content Record; and Policies: Data Import.

10. Click Save or Apply.

- Click Save to save and exit.

- Click Apply to apply the changes and continue working.

Assigning Access Roles to Users or Groups

RSA Archer allows creating one or more access roles. Each access role is mapped to a list of permissions that grant the user rights to perform certain tasks and create, read, update, and/or delete RSA Archer entities. RSA recommends that you limit privilege abuse and conflict of interests by configuring access roles that provide separation of duties.

Immediately after installation, RSA recommends you configure access roles as follows:

- Create a new access role with no rights and make it the default role. Grant additional roles to users as needed for appropriate access in RSA Archer.

- Create read-only roles that can be used by an auditor. RSA recommends that these roles only have permissions to view reports, configurations, and logs.

- Create a new Security Administrator role that has full rights to Access Control. Grant the Security Administrator role access rights to managing roles.

- Configure access roles to grant non-administrative users only the rights they need for each task based on their role in the organization. You can grant multiple access roles to each user. RSA recommends that these roles do not have permission to view or modify security configuration.

RSA recommends that you review users' task permissions on a routine basis to ensure that each user is granted the correct task permissions.

Access roles are cumulative and can be assigned to users, groups, and users with more than one access role.

Example

One access role grants create, read, and update privileges in the Policies applications and another access role grants only delete privileges. A user who is assigned both access roles has create, read, update, and delete privileges in the Policies applications.

Role Assignment by Group or User

RSA Archer allows access roles to be assigned to users through group membership or directly to user accounts. RSA recommends that you assign permissions through group membership and not directly through user accounts.

You can assign access roles to users in either of the following ways.

Assign an access role to a user

1. Open the user account to which you want to assign an access role.

   a. From the menu bar, click .

   b. Under Access Control, click Users.

   c. Select the user account.

2. Click the Roles tab.
3. Click Lookup.
4. In the Available list, expand the Roles tree, and click the access role to assign.

   Note: To search for a specific role, enter the role name in the Find field and, if applicable, select the type from the adjacent list. Click . The results of your search appear in the Available list in the Search Results node.

5. Click OK.
6. Click Save or Apply.

   - Click Save to save and exit.
   - Click Apply to apply the changes and continue working.

Assign an access role to a user group

The group that you are assigning to the access role must exist.

If you associate a user group with an access role and the group contains subgroups, the subgroups are not automatically associated with the access role. To associate subgroups with an access role, you must also select the subgroups.

1. Open the access role to which you want to assign a user group.

   a. From the menu bar, click .

   b. Under Access Control, click Access Roles.

   c. Select the access role.

2. In the Group Assignments section, click Assign.

3. From the Available list, expand Groups, and select the group or groups to which you want to assign the access role. You can also use the Find field to search for a specific group.

4. Click Save or Apply.

- Click Save to save and exit.
- Click Apply to apply the changes and continue working.

Unassign an access role from a user account

You only can remove roles in which the Assignment Method is set to Manual.

1. Open the user account from which you want to unassign an access role.

   a. From the menu bar, click .

   b. Under Access Control, click Users.

   c. Select the user account.

2. Click the Roles tab.

3. From the Selected list, click to unassign the applicable access roles.

4. Click OK.

5. Click Save or Apply.

- Click Save to save and exit.
- Click Apply to apply the changes and continue working.

Configuring LDAP for Managing User Accounts and Groups

Before you can update your user accounts and groups through a Lightweight Directory Access Protocol (LDAP) server, you must:

- Configure your LDAP server.
- Map attributes from your LDAP directory to your user accounts in RSA Archer.
- Set the rules for creating, updating, activating, and reactivating the user accounts and groups.

You can also set a schedule to automate the synchronization process between your LDAP server and the RSA Archer database. RSA recommends that you select LDAP servers that communicate using LDAP over HTTPS, and that you set the LDAP Connection attribute to secure.

Note: RSA recommends requiring a domain for LDAP synchronizations and SSO. If domains are not used, RSA recommends disabling the display of the Domain field in the RSA Archer Control Panel.

The following fields change during mapping:

- A user profile field that is mapped to an LDAP attribute is populated for new accounts. The value is retained for existing accounts.

- A user profile field that is mapped to an LDAP attribute that does not have a value is not populated for new accounts. The value is retained for accounts that were previously created.

- When the Email Address or Phone field in the user profile is mapped to an LDAP value, the LDAP value is inserted in the first email or phone number field in the user profile for new user accounts. For existing accounts, the LDAP value replaces the value in the first email or phone number field in the user profile. If a user has modified the email address or phone number through the Platform, the modification is overwritten by LDAP synchronization unless the LDAP value is null.

- The Time Zone field in the user profile cannot be mapped to an LDAP attribute.

Task 1: Set up your LDAP server

1. Go to the Manage LDAP Configurations page.

   a. From the menu bar, click .

   b. Under Access Control, click LDAP Configurations.

2. Click Add New.

3. In the General Information section, enter the name and description.

4. Click the Configuration tab.

5. In the LDAP/Active Directory Server section, enter the user domain, IP address, and connection or binding preferences.

The following table describes each field.

Field	Description
User Domain	Specifies the domain to which user accounts from this LDAP server belong. The name must be unique for all LDAP configurations.
	If you are using Windows Authentication, ensure that the User Domain field matches the Windows domain name. If these values do not match, single sign-on (SSO) fails. These domain names are not case sensitive.
Connection	Specifies whether a secure connection is required.
Name/IP Address	Specifies the fully qualified name or IP address of your LDAP or Active Directory server. Selecting this option ensures that your server assumes responsibility for directing RSA Archer to the appropriate domain controller.
	If the previously contacted domain controller is unavailable, a secondary domain controller is identified and used instead. For example, if your primary LDAP server is down for maintenance, RSA Archer is directed to the secondary server to execute LDAP synchronization.
Binding	Enables you to bind the LDAP connection to a default domain controller without specifying the name of a default server. Microsoft recommends the use of serverless binding for fault tolerance.
	If you are using an Active Directory server, select whether to use serverless binding. If you select Use Serverless Binding, you do not need to enter a value in the Name/IP Address field.

6. In the LDAP/Active Directory Server Configuration section, enter the configuration options for your LDAP server.

The following table describes each field.

Field	Description
User Name	Specifies the user name of the user identified to access the LDAP or Active Directory server when additional authentication is required.
Password	Specifies the password of the user identified to access the LDAP or Active Directory server when additional authentication is required.
Active Directory Domain	Specifies the domain of the active directory when additional authentication is required.

Field	Description
User Identifier	Identifies the object as a user object: • For new LDAP configurations, the default value is user. • For Active Directory servers, the default value is user. • For other LDAP servers, the default value is inetOrgPerson. To obtain the actual default values for your organization, see your LDAP administrator.
Group Identifier	Identifies the object as a group object: • For new LDAP configurations, the default value is group. • For Active Directory servers, the default value is group. • For other LDAP servers, the default value is groupOfUniqueNames. To obtain the actual default values for your organization, see your LDAP administrator.
Additional Attributes	Provides additional attributes that must be retrieved from the LDAP source during search. For example, if you are using filters, enter the filters in this field.
User Group Identifier	Identifies the groups to which the user belongs: • For new LDAP configurations, the default value is memberOf. • For Active Directory servers, the default value is memberOf. • For other LDAP servers, the default value is uniqueMember. To obtain the actual default values for your organization, see your LDAP administrator.
Users and Groups	Sets the User/Group association: • Users contain groups: Specifies that the user-group association is defined in the user object of the active directory server. • Groups contain users: Specifies that the user-group association is defined in the group object of the LDAP server.
Connection Time-out	Inputs the time-out value in seconds for the LDAP query. This value must be a whole number greater than 0. For new LDAP configurations, the default value is 60.

Field	Description
Binding	Sets the Binding for an LDAP configuration from the following options: • Use Simple LDAP Binding: Use when your server does not allow connection using the Simple Authentication and Security Layer (SASL) protocol, or if you experience errors. • Disable page searching: Use when your server does not support paged searching. • Remove the whitespace from the DNs: Use to remove unnecessary white space in the Distinguished Name (DN) before the names are compared when you are using an LDAP server other than Active Directory.

7. (Optional) Click Test Connection to test your configuration settings.

8. Click Save or Apply.

   • Click Save to save and exit.

   • Click Apply to apply the changes and continue working.

Task 2: Map LDAP attributes to your user profiles

1. Go to the Configuration tab of the LDAP Configuration.

   a. From the menu bar, click 🔧 .

   b. Under Access Control, click LDAP Configurations.

   c. Click the Configuration tab.

2. Go to the User Field Mapping section.

3. In the Base DN field, enter the domain name.

4. (Optional) In the Filter field, enter the criteria for filtering the LDAP directory.

5. In the Attributes field, click Get Attributes to populate the field mapping.

6. In the Field Mapping field, select the attributes for each field in the user profile that you are synchronizing with the LDAP directory.

   The following table describes each field.

Field	Description
Base DN	Specifies the Base Distinguished Name (DN) for the location of user account information in your LDAP directory.

Field	Description
Filter	Filters the LDAP information available for mapping to user profile fields. Filters are entered using the following format: objectClass=class name.
	Example
	You want to map only LDAP values associated with the "user" class. You would enter objectClass=user as the filter. This entry results in the values associated with this class being available for mapping.
Attributes	Populates the Attribute lists in the Field Mapping section.
Field Mapping	Maps the attributes from the LDAP directory to the fields in the user profile. You must map all required fields in the user profile to an attribute.
Synch Connector Test	Tests the connection of an LDAP Configuration between the RSA Archer database and the LDAP server or active directory server.
	If an error message is displayed when the number of records returned exceeds the configured size limit for the active directory, contact your LDAP administrator to request a configuration change.

7. Click Save or Apply.

   - Click Save to save and exit.

   - Click Apply to apply the changes and continue working.

Task 3: Set rules for managing user accounts and groups

1. Go to the Data Sync tab of the LDAP Configuration.

   a. From the menu bar, click 🔧 .

   b. Under Access Control, click LDAP Configurations.

   c. Click the Data Sync tab.

2. In the User Account Management section, define the rules for updating, creating, deactivating, and reactivating accounts.

The following table describes each field.

Field	Description
Updating	Specifies the rules for updating the user profile. • Update all user accounts on each sync: Updates all user accounts based on the information contained in your LDAP server • Update only user accounts where the LDAP attribute meets the following criteria: Updates user accounts based on a specific LDAP attribute and the specified criteria. Example: You want to update only user accounts from your New York office. You would select Office from the Attribute list, select Equals as the operator, and enter New York in the Value field from the Operator list.
Create/Update	Creates or updates a user account if the account does not exist in RSA Archer. The name for the new user account is assigned the value of the LDAP attribute mapped to the User Name (Login) field.
Clear User DNs	Clears the distinguished names of all users just before the LDAP synchronization starts. The synchronization then repopulates the database with the most up-to-date list of distinguished names. If users have changed their login names, moved location, or are in a new part of the company, for example, the old distinguished names are no longer valid. Consequently, these users would not be able to log into RSA Archer. **Note:** RSA Archer strongly recommends that you enable this option.

Field	Description
Deactivation	Deactivates user accounts. • Deactivate all user accounts that do not have a matching LDAP user. Deactivates user accounts for which no matching LDAP account is found during data synchronization. • Deactivate those user accounts where LDAP attribute meets the following criteria and then enter the LDAP criteria. Deactivate user accounts based on a specific LDAP attribute. Example: You want to deactivate user accounts where the employment status for the matching LDAP user account is set to inactive. You would select Employment Status from the Attribute list, select Equals as the operator, and enter Inactive in the Value field from the Operator list.
Reactivation	Reactivates user accounts based on specific LDAP attribute criteria. Example: You want to reactivate inactive user accounts where the employment status in the matching LDAP user account is set to active. You would select Employment Status from the Attribute list, select Equals and enter Active in the Values field from the Operator list.
Send Notification	Sends a notification to each user that is created to alert the user of a new password. The Default Email Address in the user account must be present to send notifications. When you select this option, a notification message is sent to all users that are being created. RSA recommends disabling this option when synchronizing a large number of records because uploading a large number of users can cause the email server to exceed its capacity for sending email messages.

3. (Optional) In the Group Management section, enter the criteria for synchronizing the LDAP group structure with RSA Archer.

The following table describes each field.

Field	Description
Group Sync	Replicates your LDAP group structure in RSA Archer when synchronized. The common name (CN) of the group on your LDAP server is used as the group name in RSA Archer. If a group in RSA Archer is created before synchronizing with your LDAP server, and there is a group with a matching name in your LDAP directory, the group in RSA Archer is not synchronized with the LDAP group. Instead, a new group with the same name is created and is flagged with the Synchronization icon. Selecting the Group Synch option makes your LDAP server the authoritative system for RSA Archer group management. • Any groups that you delete from your LDAP server also are deleted from RSA Archer • Any changes made to your groups in the LDAP directory are reflected in RSA Archer. You cannot edit or delete groups in RSA Archer that were created through LDAP synchronization. You can create additional groups in RSA Archer that are not included in your LDAP group structure, and can fully manage these groups in RSA Archer.
Group Base DN	Specifies the Base Distinguished Name (DN) for your LDAP group structure. If you selected Group Sync and you do not specify a DN for your group structure, the group sync query defaults to the Base DN specified in the LDAP configuration.

4. Click Save or Apply.

   • Click Save to save and exit.

   • Click Apply to apply the changes and continue working.

Configuring an Instance for Single Sign-on

Single Sign-on (SSO) reduces administrative overhead that is related to user accounts. With SSO authentication enabled, you can retrieve user profile information at the time of initial account creation from an LDAP directory server. This optional step automates the configuration of basic user profile data. Configure Secure Sockets Layer (SSL) for SSO or as a stand-alone method. Set up the SSO authentication for Windows Integrated or for Windows Integrated and SSL. Setting up the authentication requires you to modify the web.config file.

RSA Archer supports two basic authentication mechanisms:

- Username/password login scheme (the default)

- SSO configuration, which facilitates user login in corporate computing environments and supports most popular web authentication products.

The RSA Archer Control Panel provides controls for enabling SSO and selecting an SSO method. When configuring SSO, you must set up LDAP integration from the Manage LDAP Data Configuration page on the Access Control feature.

Single Sign-on properties

The following table describes the SSO properties:

Option	Description
Single Sign-on Mode	Specifies the user login method By default, the method is Disabled. When you have enabled this option, the system grants the user access if the user exists in RSA Archer. If the user does not exist, an LDAP query retrieves the user profile information and creates an account. The other options are: - HTTP Header. This method requires an HTTP header parameter that identifies the user attempting to access the application. - Request Parameter. This method requires a request form or query string parameter that identifies the user attempting to access the application. - Windows Integrated Uses the "Integrated Windows Authentication" built into Internet Information Services (IIS) that uses the user credentials using NTLM/Active Directory. - Federation. This method allows RSA Archer to process Windows Federated claims from Active Directory Federation Services (ADFS). Use Federation to process claims generated from ADFS directly. You can also set up ADFS as a service provider to a SAML 2.0 identity provider (IDP) and convert the SAML 2.0 assertions to Federated claims. - SAML. This method allows you to set up a SAML 2.0 capable provider to work with RSA Archer and authenticate based on SAML assertions of IDPs. **Note:** Use ADFS as the service provider for the Federation option.
Username Parameter	Specifies the username of the user logging on to RSA Archer. This option is required when you have selected the Request Parameter or HTTP Header methods as the Single Sign-on Mode.

Option	Description
Domain Parameter	Specifies the domain to which the user can connect. This option is required when the Request Parameter or HTTP Header methods is selected as the Single Sign-On Mode.
Allow Manual Bypass	Activates manual login. Users can connect to the system manually by adding the parameter manuallogin with a value of true to the query string passed to default.aspx. For example, https://egrc.archer.rsa.com/default.aspx?manuallogin=true. When this parameter is in the query string, users see the Login dialog box rather than passing the user credentials into the application. This option benefits a system administrator who logs in with the System Administrator user account instead of SSO sending the credentials of the personal user account.

Authentication options

- Windows-Integrated SSO only
- Windows-Integrated SSO with SSL
- SSL only

Configuration procedure

Task 1: Enable authentication for Single Sign-on

1. Go to Internet Information Services (IIS) Manager.

2. Enable authentication for the following SSO modes for the current server desktop connection:
   - For HTTP Header, enable Anonymous Authentication
   - For Request Parameter, enable Anonymous Authentication
   - For Windows Integrated, enable Windows Authentication
   - For Federation, enable Anonymous Authentication
   - For SAML, enable Anonymous Authentication

   Note: RSA Archer requires that only one authentication type be enabled at a time.

3. In the RSA Archer Control Panel, specify and then enable the instance for which you are configuring SSO.

Task 2: Configure Single Sign-on

Note: You must have system administrator rights on the server running the RSA Archer web application.

1. Click the Single Sign-on tab of the instance you want to configure.

   a. Open the RSA Archer Control Panel.

   b. From the Instance Management list, double-click the instance.

2. In the Single Sign-on Mode field, select one of the following:

   - HTTP Header
   - Request Parameter
   - Windows Integrated
   - Federation
   - SAML

3. Do one of the following:

   - If you selected Request Parameter or HTTP Header methods, go to the next step.
   - If you selected Windows Integrated method, go to step 6.
   - If you selected Federation, go to step 7.
   - If you selected SAML, go to Configuring SAML Single Sign-on Mode.

4. In the Username Parameter field, enter the name of the user logon.

5. In the Domain Parameter field, enter the domain to which the user can log in.

6. Do one of the following:

   - To enable manual login to, click Allow Manual bypass, and then go to step 14.
   - To force SSO regardless of the user, go to step 14.

7. Configure the following options in the Single Sign-on section:

   a. Select Override Federation metadata to ignore Federation metadata at the installation level, which enables instances to use a different ADFS service provider.

      Note: Any change of the entity name or change of any certificates in ADFS requires that you reimport metadata into RSA Archer.

   b. If you selected Override Federation Metadata, you can click Select to go to a different metadata .xml file, and then select the file.

> **Note:** For instructions about how to get federationmetadata.xml, see the documentation from the service provider. For example, in ADFS, the URL to obtain the .xml file looks like https://server/FederationMetadata/2007-06/FederationMetadata.xml, where *server* is the name of your service provider.

   c. In the Relying Party Identifier field, enter the replying party identifier, which is provided in ADFS for this instance.

   d. In the Home Realm Parameter field, enter the name that you created to identify your realm. This name is the identifier that is used in the vanity URL. The syntax for this string is:

   https://servername/../Default.aspx?<HomeRealmIdentifier>=<IdpRealmName>

   For example, to skip the identity provider prompt, you can pass the home realm as a parameter:

   https://servername/../Default.aspx?Realm=ADFS-IDP

8. Configure the following options in the Identity Providers section:

   a. In the Decision Page Header field, enter the text that you want to appear as the heading at the top of the Decision Page.

   b. In the Dropdown Label field, enter the text that you want to appear on the Decision Page as the label for the drop-down that lists all identity providers.

   c. In the Identity Provider field, select an existing IDP. You can complete the following three fields to add an IDP. (See the Claim Names for the Federation table at the end of this procedure for RSA Archer supported claim names.):

- In the Realm field, enter the realm name for the new identity provider.
  You can link to the following website to learn how to set up the claim provider and relying party in ADFS:

  https://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides(v=ws.10).aspx

- In the Identifier field, enter the appropriate claim provider identifier which is provided in ADFS for a given identity provider. For a complete list of the claims that RSA Archer supports, see the table below.

- In the Display Name field, enter the display name for the new identifier, which then displays in the drop-down list of the Decision Page.

   To add more providers, click ➕, and then complete the same three fields for each provider.

9. (Optional) In the On Login Error field, enter the URL for the page you have created. The user is redirected here if there is a login failure.

10. (Optional) In the On User Not Found field, enter the URL for the page you have created. The user is redirected here if the username cannot be found in RSA Archer.

11. (Optional) In the On Provisioning Failure field, enter the URL for the page you have created. The user is redirected here if there is a provisioning failure. For example, if you have exceeded the maximum number of users for your instance.

12. Select the Provisioning Settings for the selected IDP as appropriate.

13. Enter the default First Name, Last Name, and User Role that RSA Archer uses if no name and user roles were specified at the time of provisioning. You can, later, edit these values for the new user.

14. On the toolbar, click Save.

Claim names for the Federation Option

Note: ADFS expects claims to be in URL format, for example http://schemas.xmlsoap.org/claims/Group.

The following table contains claims-mapping information. Items marked with an asterisk (*) are mandatory.

RSA Archer Field Name	RSA Archer Supported Claim Name/Namespace
User Identity Information	
User Name*	UPN*
Domain	UserDomain
First Name	FirstName
Last Name	LastName
Middle Name	MiddleName
Title	Title
Contact Details	
Email Address	EmailAddress
Phone Number	PhoneNumber
Company Name	CompanyName
Address	FullAddress
	Street
	City

RSA Archer Field Name	RSA Archer Supported Claim Name/Namespace
	State
	Zipcode
Localization	
Time Zone	TimeZoneId
Account Maintenance	
Security Parameter ID	SecurityParameterId
Access Control Roles/Groups	
Group	Group
Role	Role

Task 3: Set authentication for Single Sign-on

1. Enable LDAP synchronization enabled in Microsoft Internet Information System (IIS).

2. Specify and enable the instance for which you are configuring SSO.

3. Configure SSO for the instance.

4. Modify the web.config file for your authentication method.

Configuring SAML Single-Sign-on mode

1. Allow manual bypass.

   - Enabled allows you to bypass SSO mode and log in using RSA Archer credentials.

   - Disabled allows you to only use SSO through configured identity providers (IDPs).

2. Provide the Instance Entity ID (required).

   - The identifier for this instance acts as a SAML service provider when issuing authentication requests.

   - Entity IDs must be unique across RSA Archer instances using the same IDP and limited to 1024 characters in URL format.

3. Provide a certificate thumbprint (recommended).

   - An x.509 certificate is required to allow signing SAML requests and encryption of SAML assertions. RSA Archer signs requests when the IDP requires. The IDP uses the same

certificate when encrypting assertions.

- Provide a thumbprint for the x.509 certificate in the Windows Local Machine Certificate Store.

- The IIS Application pool identity running the RSA Archer application requires Private Key-Read permission.

- If you use multiple web servers, import the same certificate to all Local Machine Certificate Stores.

4. The service provider metadata exports RSA Archer service provider metadata XML for use when configuring Archer as a client with your IDP. Metadata includes:

- Instance Entity ID

- Redirection URL to RSA Archer assertion consumer service

- Required Name ID preference

- Public key of signing and encryption certificate

- Preference for signed assertions from the IDP

   Important: Save all pending changes before generating metadata. Regenerate the metadata after you revise the Instance Entity ID or base URL.

   Important: Regenerate the metadata after you revise the Instance Entity ID, base URL, or certificate thumbprint.

Identity Providers

1. Complete the following fields to add an IDP or select an existing IDP from the list to edit. If adding a second or multiple IDPs, click the ➕ icon then complete the following (required):

   a. In the Display Name field, enter the display name for the new identifier. The identifier displays in the drop-down list on the Single Sign-on Decision Page. The display name is shown when the instance URL is provided without the IDP parameter.

   b. In the Realm field, enter the Realm name for the new IDP. The Realm field value, instance URL, and parameter name IDP can be used to skip the Single Sign-on Decision Page.

   Example:

   - Instance URL: https://archer.domain.com Realm: CorpIDP

   - Going to https://archer.domain.com?IDP=CorpIDP skips the Decision Page and immediately redirects you to CorpIDP for authentication.

2. Import identity provider SAML metadata (required).

   a. Click import, and go to metadata .xml file.

   b. Click OK to finish the import.

   If successful, the IDP Metadata field shows value of EntityID contained in the entity descriptor from the metadata.

   Note: If Required Encrypted Assertions is enabled, RSA Archer will not accept unencrypted assertions from the IDP. A valid certificate thumbprint must be specified to require encrypted assertions.

3. Select the appropriate Provisioning Settings for the selected IDP (not required):

   - Enable User Provisioning. If an account does not exist, a new account is created based on the username.

   - Enable User Update. Profile information including email address, street address, First Name, Last Name, updates each time that a user successfully authenticates through SSO.

   - Enable Group Update. Group membership is updated on each SSO.

   - Enable Role Update. Role assignment is updated on each SSO.

4. Enter the default First Name, Last Name, and User Role (required). RSA Archer uses these defaults if no name and user roles were specified at the time of provisioning. Later you can edit these values for the new user.

5. Click Save to save all configuration settings in the Single Sign-On tab.

   Note: Any changes to the SSO section or IDP section are not saved until this step is completed.

RSA Archer Supported Attribute Mapping for SAML

The following table contains RSA Archer Supported Attribute Mapping information for SAML. Items marked with an asterisk (*) are mandatory.

RSA Archer Field Name	RSA Archer Supported Attribute Mapping
User Identity Information	
User Name*	NameID*
User Domain	UserDomain
First Name	FirstName

RSA Archer Field Name	RSA Archer Supported Attribute Mapping
Last Name	LastName
Middle Name	MiddleName
Title	Title
Contact Details	
Address	FullAddress
	Street
	City
	State
	Zipcode
Company	Company
Default Email Address	EmailAddress
Phone 1	PhoneNumber
Localization	
Time Zone	TimeZoneId
Account Maintenance	
Security Parameter	SecurityParameterId
Access Roles/Groups	
Groups	Group/Groups Use Group for single-value attribute. Use Groups for multiple-value attributes.
Roles	Role/Roles Use Role for single-value attribute. Use Roles for multiple-value attributes.

Note: To update the user address, use one of the following:

- FullAddress attribute. The Address field in the User Profile updates with the values provided in this attribute.

- Street, City, State, Zipcode attribute. The Address field updates with the values Street, City, State, Zipcode.

Note: See RSA Archer Supported Time Zone ID Values for a list of all RSA Archer Supported Time Zone ID Values.

Configuring the Instance Database Connection String and Pooling Options

You can configure the database connection string for either Windows Integrated Security or SQL Server encryption 2012 or 2014. RSA recommends that you configure authentication with this database based on Microsoft's recommended best practices for secure authentication to a database. RSA Archer supports using Integrated Security for connecting to the database.

- If using Windows Integrated Security, this option uses the current Windows identity established on the operating system thread to access the instance database. Selecting this option disables Login name and Password. Do not select this option if you are using SQL Server Authentication.

- If using SQL Server encryption, you must install separate certificates on each server (web application, services, and database) and you must enable encryption on the SQL server. Otherwise the connection will fail.

- If your application connects to an AlwaysOn availability group (AG) on different subnets, selecting the Multi-Subnet Failover option provides faster detection of and connection to the active server

Connection pooling is enabled for all instances and maintains a cache of database connections that you can reuse when requesting information from the database. Pooling reduces the number of new database connections that you must make.

Configure the instance database connection string

Complete this task for all configurations to set the database connection string for the instance.

1. On the instance you are configuring, go to the Connection Properties section.

   a. Open the RSA Archer Control Panel.

   b. From the Instance Management list, double-click the instance.

     c. Go to the Database tab, and then go to the Connection Properties section.

2. In the SQL Server field, select the database server for the instance.

3. Select the authentication method for connecting to the database server.
   Do one of the following:

   - If using Windows Integrated Security, select Use integrated security and skip to step 6.

   - If using SQL Server encryption, select Use encryption and continue at the next step.

   - If your application connects to an AlwaysOn availability group (AG) on different subnets, select the Multi-Subnet Failover option, and then continue at the next step. Enabling this option adds the following expression to the SQL connection string for the Instance database:

     MultiSubnetFailover=True

4. In the Login name field, enter the name of the SQL Server Authentication account.

5. In the Password field, enter the login password for the SQL Server Authentication account.

6. In the Database field, enter the instance database name.

7. Click Test Connection to test the connection string.

8. (Optional) In the Connection Timeout field, change the default duration of time for the connection timeout.

9. Designate the file repository path.

Override the pooling options for the instance database

By default, database pooling is enabled with a minimum of 0 connections and a maximum of 100.

1. Click the Database tab, and then go to the Pooling section.

   a. Open the RSA Archer Control Panel.

   b. From the Instance Management list, double-click to expand the Instances list.

   c. Double-click the instance in the list that you want to configure.

2. In the Pooling field, click Override connection pool size.

3. In the Min pool size field, enter the minimum pool size.

4. In the Max pool size field, enter the maximum pool size.

5. On the toolbar, click Save.

Changing SysAdmin and Services Account Passwords

RSA recommends that you instruct your administrators on your corporate IT policy and security best practices for generating and managing passwords for default System Administrator (sysadmin) and default services accounts.

After installing RSA Archer, you must change the passwords of the SysAdmin Account and Services Account. You should change both passwords at least every 90 days using the RSA Archer Control Panel. The new passwords must be strong, meeting the security parameter configuration for the accounts. You can disable the sysadmin account, but cannot delete or rename it.

Important: Do not use a semicolon (;) as the special character in a password. RSA Archer does not recognize this character.

Change the SysAdmin password

1. On the Accounts tab, go to the SysAdmin Account section of the instance you want to update.

   a. Open the RSA Archer Control Panel.

   b. From the Instance Management list, double-click the instance.

2. In the New Password field, enter the password for the SysAdmin account.

3. (Optional) Select Show Password to show the password as you enter it. If this option is not selected, the password is masked with substituted characters for the actual text.

Change the Services Account password

1. On the Accounts tab, go to the Services Account section of the instance you want to update.

   a. Open the RSA Archer Control Panel.

   b. From the Instance Management list, double-click the instance.

2. In the New Password field, enter the password for the Services account.

3. (Optional) Select Show Password to show the password as you enter it. If this option is not selected, the password is masked with substituted characters for the actual text.

4. Complete the Default Instance Creation.

For additional information on other options, see the RSA Archer Control Panel Help.

Configuring the Login Page

RSA recommends that you require a domain for LDAP synchronization and SSO. If you do not use a domain, RSA recommends that you disable the Domain field in the RSA Archer Control Panel.

If you are using SSO, the RSA Archer does not display a logon banner. In this case, RSA recommends that you ensure that the SSO provider displays the government or corporate-approved login banner.

Disable the domain field

1. Open the RSA Archer Control Panel, and then go to the Installation Settings tab.
2. On the General tab, go to the Login Page section.
3. In the Default field, select Hide Domain field on Login Page.
4. On the toolbar, click Save.

Display the login banner

1. Open the RSA Archer Control Panel, and then go to the Installation Settings tab.
2. On the General tab, go to the Login Page section.
3. In the Banner field, enter the banner that you want to appear at the bottom of the Login page. By default, the Hide Domain field on Login Page checkbox is blank, indicating that the Domain field appears.
4. On the toolbar, click Save.

Authentication Methods

Authentication methods authorize users to perform computer functions and determine the connectivity to the databases. The method you use is entirely up to your business operations. The authentication methods include:

- SQL Server Authentication. RSA Archer connects to each database using a SQL account created on the SQL Server instance. You provide the account information during the installation process.

- SQL Server Data bases. RSA Archer SQL Server 2014 or SQL Server 2016 databases for data storage. Restrict authorization to these databases to only the accounts that need access to the database.

During installation and upgrade, the account connecting to the databases from RSA Archer requires db_owner permission. Post-installation, the account connecting to both Instance and Configuration databases from RSA Archer requires the following permissions on the database:

- Data Read rights (member of db_datareader)

- Data Writer rights (member of db_datawriter)

- Execute permissions on all stored procedures and scalar functions

- Select permissions on all views, table-valued functions, and in-line functions

- Execute permissions on the system-stored procedure sp_procedure_params_100_managed

Important: Grant the same privileges to the user for both the Instance database and the Configuration database.

- Integrated Security. RSA Archer connects through a Windows identity established on the operating system thread using an Active Directory domain user account. You must configure the Application Pool Identity in IIS as the domain user account before installing RSA Archer. This domain user account has DB Owner (DBO) access to the instance database that serves as the process identity for applications assigned to the application pool. DBO access is only required during the installation.

  RSA recommends creating a custom domain services account dedicated to RSA Archer for the IIS Application Pool Identity, and then providing it access to the necessary resources. In addition, be prepared to provide the same account credentials for the RSA Archer Services account during the installation process.

  Note: The term Integrated Security may also be referred to as Trusted Connections. The Application Pool is a means of isolating Web Applications where there are multiple IIS worker processes that share the same Web Server.

Message Logging

A log is a chronological record of system activities that enables the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

RSA Archer logs Event Tracing for Windows (ETW) trace events and writes log messages to a specified database. ETW is a kernel-level API that enables high-performance data collection and tracing in Windows. It enables you to start and stop event tracing at a granular level, log to a very efficient buffering system, and consume events across a system.

You can monitor the log messages with any tool that consumes ETW trace events. Message logging provides an easier way to troubleshoot processing jobs when errors occur. For example, you can use this log to troubleshoot errors that might occur in a data feed job. Messages are grouped by each data feed with a Start and Stop event so that you can easily identify where the data feed failed.

Third-party tools request either the Provider Name or the Provider ID in order to consume the trace events generated in RSA Archer:

- Provider ID: 472DD2D1-1B28-5523-9DDD-B4DEB8924408

- Provider Name: RSA-Archer-GRC-Platform

If you are using message logging, you must create a database dedicated to the RSA Archer Instrumentation service. Do not use the same database that stores instance or configuration data.

Note: If you are specifying an account other than the Local System account to run the services and you are using the RSA Archer Instrumentation service, you must add this user to the Performance Log Users group to grant permission to write to ETW.

Log Description

The following table shows the security-relevant logs provided by RSA Archer.

Component	Location
Security Events Report	The instance database
RSA Archer Error Logs	File system in the configured logging directory
Windows Event Logs	Event Viewer

Security Events Report

The Security Events report contains a list of all of the security-related events that have occurred in RSA Archer. RSA recommends that administrators define and enforce a retention policy for the RSA Archer Error logs, as well as the Windows Event logs, in accordance with your corporate IT policy and security best practices. This report includes the following security events:

- Access Role Created

- Access Role Deleted

- Access Role Modified

- Account Status Modified

- Configuration Administrator Added

- Configuration Administrator Deleted

- Content Administrator Added

- Content Administrator Deleted

- Failed User Login

- Full Application Content Delete

- Global Report Permission Granted

- Global Report Permission Removed

- LDAP Configuration Delete Started

- LDAP Configuration Delete Completed

- Maximum Login Retries Exceeded

- Offline Access Sync Requested - Download

- Offline Access Sync Requested - Upload

- Password Changed by Administrator

- Password Changed by User

- Reset Password Requested

- Role Assigned to User

- Role Removed from User

- Security Events Started

- Security Events Stopped

- Security Parameter Assignment Modified

- Security Parameter Created

- Security Parameter Deleted

- Security Parameter Modified

- Sub-Form Configuration Administrator Added

- Sub-Form Configuration Administrator Deleted

- User Account Added

- User Account Deleted

- User Account Modified

- User Added to Group

- User Full Name Modified

- User Login

- User Login Name Modified

- User Logout

- User Removed from Group

RSA Archer Error Logs

You can configure the location of the RSA Archer error log in the RSA Archer Control Panel at both the installation and the instance level. The default log location for the instance is C:\ArcherFiles\logging.

RSA recommends that you configure the setting at the installation level and allow the location for the instance level to default based on the installation setting.

For more information, see "Logging Settings" and "Verify the Logging Properties" in the RSA Archer Control Panel Help.

Log Directory Permissions

RSA recommends that you restrict the permissions on the log files folder to the same read, write, and modify permissions of the account that the IIS processes and the RSA Archer-installed services are running.

For More information, see "Task 5: Grant Permissions to RSA Archer Directories" in the "Configuring the Web Server" section of the *RSA Archer Platform Installation and Upgrade Guide*.

Windows Event Logs

The following items are logged in the Windows Event logs by the RSA Archer services and Web Application:

- Service Start (Application and System logs)
- Service Stop (Application and System logs)
- .NET Runtime Errors

Port Usage

RSA recommends that you configure your firewall rules and access control lists to expose only the ports and protocols necessary for operation of RSA Archer.

The Job Engine and Configuration Service can run on multiple servers simultaneously. You should account for each server running those services when planning firewall rules. For a given item, you can omit the rule if the source and destination components run on the same server.

RSA Archer services and supporting services on the web server use specific ports to communicate with each other and with interfaces and applications external to RSA Archer.

You can modify the following ports:

- Configure the port used for SQL in SQL Server.

- Configure the port used for HTTPS in Microsoft IIS.

The following table lists ports used by RSA Archer. Rows in bold text identify the minimum set of ports that must be open for the application to work. Brackets around items in the Destination column indicate supporting hosts and servers that communicate with RSA Archer.

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
Client Web Connectivity	Platform Web UI	Web Server (IIS) or Load Balancer	HTTP(S)	80/TCP, 443/TCP	Mandatory
	See Web Server Communication. The destination is a Load Balancer if the Platform is deployed with a web server cluster or farm. RSA recommends that you rely only on HTTPS.				
	Platform Web API	Web Server (IIS) or Load Balancer	HTTP(S)	80/TCP, 443/TCP	Optional
	See Web Server Communication. The destination is a Load Balancer if the Platform is deployed with a web server cluster or farm. RSA recommends that you rely only on HTTPS. You can change the default port for use by your application.				
	Archer-to-Archer Data Feed	Web Server (IIS) or Load Balancer	HTTP(S)	80/TCP, 443/TCP	Optional
	See Web Server Communication. The destination is a Load Balancer if the Platform is deployed with a web server cluster or farm. You can change the default port for use by your application.				
	Offline Access	Web Server (IIS) or Load Balancer	HTTP(S)	80/TCP, 443/TCP	Optional
	Only required if using offline access.				

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
RSS Feeds	Web Server (IIS) or Load Balancer	[Remote Host]	HTTP(S)	80/TCP, 443/TCP	Optional
	See Web Server Communication. The destination is a Load Balancer if the Platform is deployed with a web server cluster or farm. You can change the default port for use by your application.				
Threat Feeds	Job Engine Service	[Remote Host]	HTTPS	443/TCP	Optional
	See Web Server Communication. Only required if using Threat Management to pull in a threat intelligence feed from Symantec DeepSight, Verisign iDefense, or other supported feeds.				
SQL Queries	Configuration Service, Job Engine Service, Queuing Service, Web Server (IIS)	[Database Server (SQL Server) running RSA Archer database]	SQL	1433/TCP	Mandatory
	See SQL Server Communication. You can change the default port for use by your application.				
	LDAP Synchronization Service	[Database Server (SQL Server) running RSA Archer database]	SQL	1433/TCP	Optional
	See SQL Server Communication. Only required if using LDAP synchronization.				

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	Configuration Service, LDAP Synchronization Service, Job Engine Service, Queuing Service, Web Server (IIS)	[Database Server (SQL Server) running RSA Archer database]	SQL	1434/UDP	Optional
	If using a named instance, SQL Browser is also required.				
Microsoft File Sharing	Job Engine Service, Web Server (IIS)	[File Server for document repository]	SMB/CIFS	445/TCP	Optional
	Only required if the document repository is not contained on a single web server.				
	Web Server (IIS)	[File Server for company_files]	SMB/CIFS	445/TCP	Optional
	Only required if the appearance files are not all contained in a single web server.				
	Queuing Service	[File Server for keyword indexes]	SMB/CIFS	445/TCP	Optional
	Only required if the keyword search indexes are not all contained on a single web server.				

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
LDAP Queries	LDAP Synchronization Service	[LDAP Server]	LDAP(S)	389/TCP (LDAP), 636/TCP (LDAPS over SSL), 3268/TCP (LDAP), 3269/TCP (LDAP to GC over SSL)	Optional
	Only required if performing LDAP synchronization. You can change the default port for use by your application. **Note:** If you have more than 1000 users, RSA recommends using a Global Catalog (GC) connection. For more information, see the Knowledge Base article, "LDAP Sync Unable to Create More Than 1000 Users in RSA Archer," at https://community.rsa.com/docs/DOC-46832.				
Audit Logging	Web Server (IIS)	[Remote Host]	TCP/UDP	Varies	Optional
	Only required if Audit Logging is enabled.				
Email Notifications	Job Engine Service	[SMTP Server]	SMTP(S)	25/TCP (SMTP), 465 (SMTPS)	Optional
	Only required if using email notifications. You can change the default port for use by your application.				
Mail Monitor	Job Engine Service	[POP3 or IMAP Server]	POP3(S), IMAP(S)	110/TCP (POP3), 995/TCP (POP3S), 143 (IMAP), 993/TCP (IMAPS)	Optional

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	Only required if leveraging Mail Monitor functionality.				
Read Receipts	Job Engine Service	[POP3 or IMAP Server]	POP3, IMAP	110/TCP (POP3), 143 (IMAP)	Optional
	Only required if leveraging Read Receipt functionality.				
Configuration Data Retrieval	Job Engine Service, Queuing Service, Web Server (IIS)	Configuration Service	WCF	13201/TCP	Mandatory
	Required for RSA Archer service to obtain Platform configuration data.				
	LDAP Synchronizatio n Service	Configuration Service	WCF	13201/TCP	Optional
	Only required if using LDAP synchronization.				
Configuration Data Updates	Configuration Service	Web Server (IIS)	WCF	13300-13304/TCP	Mandatory
	Required to push configuration data updates to the web servers.				
	Configuration Service	Job Engine Service, Queuing Service	WCF	13305-13350/TCP	Mandatory
	Required to push configuration data updates to RSA Archer services.				
	Configuration Service	LDAP Synchronizatio n Service	WCF	13305-13350/TCP	Optional
	Only required if using LDAP synchronization.				
Content API	Configuration Service	Content API	WCF	13351-13355/TCP	Optional

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	Only required if using the Content API.				
SSO Authentication	Web Server (IIS)	[Remote Host]	Varies	Varies	Optional
	Only required if using SSO, in which case additional traffic may need to be allowed. The destinations, ports, and protocols would vary based on the SSO provider and your specific implementation. You can change the default port for use by your application.				
Data Publication	Job Engine Service	[Remote Host]	Varies	Varies	Optional
	Only required if using the Data Publication feature, in which data can be extracted and written to a relational database system. The destinations, ports, and protocols vary based on the destination system. You can change the default port for use by your application.				
Client Web Connectivity	Web Server	Advanced Workflow REST URL or through a Load Balancer	HTTP(S)	Any unused port (defaults: 8000 for HTTP and 8443 for HTTPS)	Mandatory
	Only required if using the Advanced Workflow feature. You can change the default port for use by your application. Be sure that the support port number is available for use. The web server communicates with the advanced workflow job troubleshooting page when records are enrolled. The Advanced Workflow service requires dedicated port on the configured servers to communicate with RSA Archer.				

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
Client Web Connectivity	Services Server	Advanced Workflow REST URL or through a Load Balancer	HTTP(S)	Any unused port (defaults: 8000 for HTTP and 8443 for HTTPS)	Mandatory
	Only required if using the Advanced Workflow feature. You can change the default port for use by your application. Be sure that the support port number is available for use. The services server communicates when a new record is enrolled in an advanced workflow. The Advanced Workflow service requires dedicated port on the configured servers to communicate with RSA Archer.				
Remote Procedure Call (RPC)	Job Engine Service	[RPC Endpoint Mapper]	TCP	135	Mandatory
	Web Server used for Archer Configuration Report (ACR).				
Remote Procedure Call (RPC)	[Remote Host (s)]	Job Engine Service, Web Server	TCP	49152 to 65535	Mandatory
	RPC Server port used for Archer Configuration Report (ACR).				
Elasticsearch	Indexing Service, Web Server	[Elasticsearch Cluster Node]	HTTP(S)	9200 to 9300	Mandatory
	Only required if using the Elasticsearch feature. You can change the default port for use by your application.				
Other Data Feeds	Job Engine Service	[Remote Host (s)]	Varies	Varies	Optional

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	Only required if using RSA Archer to pull data from other systems using transfer protocols, for example, FTP, SMB, and SQL. The destinations, ports, and protocols vary based on your implementation. You can change the default port for use by your application.				

Network Encryption

The following sections provide information on how to secure communication protocols used by RSA Archer:

- Data Feeds

- Web Server Communication

- SSL Certificate Guidance

- SQL Server Communication

- RSA® Archer® Web Services API

Data Feeds

Data Feed Manager is a flexible, code-free tool for aggregating data in RSA Archer. Use the tool to:

- Configure multiple, dynamic data feeds, and manage those feeds without relying on programming resources.

- Build and configure dynamic integrations with external enterprise systems and files. From Data Feed Manager, you can build a transport path between RSA Archer and an external source and then map the data from that source to an existing target application or questionnaire in RSA Archer.

- Configure the data feed to run on a schedule. After the initial configuration, the data feed executes automatically with no need for you to intervene.

You can integrate data using Data Feed Manager for:

- Network and asset discovery data

- Vulnerability scan results

- Performance scorecards

- Incident reports

- Audit results and recommendations

Because RSA Archer is vendor neutral and content independent, you can use RSA Archer as a point of consolidation for enterprise data of any type for supporting analysis and process management. With a centralized view of data from point solutions, databases, spreadsheets, and other sources, you can access content more easily that is relevant to your job functions. Re-purpose data to support a variety of business processes.

A data feed must be both active and valid to run. As you configure your data feed, Data Feed Manager validates the information for you. If it is not valid, an error message appears. You can save the data feed and correct the errors later. However, the data feed does not process until you have corrected the errors and the data feed validates.

Data feed types

Important: To avoid potential conflicts with other data feeds, RSA suggests that you use a different user account for each data feed. Additionally, if you plan to run multiple data feeds simultaneously, create a unique name to prevent termination of session tokens.

Data Feed Manager supports standard and transport data feeds.

The following table describes each type of data feed.

Feed Type	Description
Standard	Brings data from an external source into an application or questionnaire. This data feed type requires that you: • Define the fields and data format. • Map the fields in the source file to the target. • Perform a report-based search for an application or questionnaire that contains the source data that you want to import into another application or questionnaire. • Set up a user account as a Service account, which means this user account has all necessary permissions to execute the data feed. You can specify the following: • Whether to send subscription notifications to specified users or groups when records are modified • Whether to send a notification to specified users or groups when a data feed job completes, identifying a successful or failed completion • The locale format of your source data. For example, different characters might be used to indicate a decimal place.
Transport Only	Locates a separate data file that contains additional instructions for launching subsequent, standard data feeds. • Ensure that a user account for the data feed and a target path for the separate data file exist, but no additional data configuration. • Create a unique name when running multiple data feeds simultaneously to prevent termination of session tokens.

Data feed transporter types

The Data Feed Service (DFS) architecture accommodates the definition of various data retrieval mechanisms.

The following table describes the out-of-the-box transporters.

Transporter	Description
Archer Web Services	Accesses the Web Services API and retrieves data from an instance of RSA Archer. This transporter is used in Archer-to Archer data feeds.

Transporter	Description
Database Query	Returns results using an SQL query.
DeepSight 2.0	Uses the v2 Symantec web service to retrieve vulnerabilities threat feed data. This transporter will soon become unusable because of deprecation by Symantec. For DeepSight v4 data feeds that are available on the RSA Archer Community on RSA Link, use the DeepSight 4.0 transporter.
DeepSight 4.0	Uses the v4 Symantec web service to retrieve security risk and vulnerability SCAP data feeds.
File	Retrieves delimited data files, including support for multi-file manifests.
FTP	Retrieves data files using the FTP protocol.
HTTP	Executes a GET or POST to retrieve data from an HTTP or HTTPS site.
iDefense	Retrieves vulnerabilities and geopolitical threat feed data.
JavaScript	Executes a user-provided JavaScript file. If the result of that execution is a data set, it is transformed and processed into the platform as normal.
Mail Monitor	Retrieves content from monitored email accounts.
RSS	Retrieves records from a configured RSS feed.

Supported and unsupported field types for data mapping

Supported Field Types

- Attachment
- CAST Detail
- Cross-Reference
- Date
- External Links
- Image
- Internal Reference
- IP Address
- Matrix

- Numeric
- Record Permissions
- Related Records
- Sub-Form
- Text
- User/Groups List
- Values List

Note: For User/Groups List and Record Permissions, for the source input username, the data field always tries to find a match in the User list first. If no match is found, then it will try to find a match in the Groups list.

Unsupported Field Types

- Access History
- CAST Score Card
- Discussion
- First Published Date
- History Log
- Last Updated Date
- MRDC (Must be populated through reference fields.)
- Record Status
- System-generated Related Record that points to a Questionnaire
- Voting

Schema sources

The source for the schema of your data feed depends on which transporter you are using. The following table identifies and describes the schema sources that are available for each of the out-of-the-box transporters.

Important: The process of loading a source definition for a data feed times out at five minutes. You may want to consider using a smaller set of source data when you set up the feed.

Source	Description
Execute Search	Executes the search in RSA Archer and detects the source schema from the results.
	Recommended approach for an Archer-to-Archer data feed. Loads the source fields directly from the report. When using this scheme, complete all required information on the Transport and Navigation tabs.
Execute Query	Executes the query specified on the Transport tab and detects the source schema from the resulting record set.
	Using this option may trigger actions in the database associated with this query.
Sample File	Uses a skeleton of your actual source data file. For example, if you are importing data from a .csv file, the source data file is a .csv file that includes the column names from your source data. If you are importing data from an .XML file, the source data file includes the structure of your .XML without the actual field values.
	When you select the sample file, the Source Fields section populates with the fields specified in the sample data file.
	For the Archer Web Services Transporter, select a file from an external location that contains the data in a same format as the report format.
Load URL	Loads the contents at the target URL and detects the source schema from the contents.
	Using this option may trigger actions associated with accessing the target URL.
Standard Schema	Uses the standard mail schema.

Updating locked records

RSA Archer has an important feature that prevents the updating or altering of a locked record. A record becomes locked when a user has opened it in Edit mode for the purpose of modifying it.

However, it is important to note that records can be updated through the RESTful and Web APIs, as well as through data feeds, even when a user has locked them. The following are examples of typical APIs that can update user-locked records:

- PUT content (RESTful)
- UpdateRecord (Web Services)
- UpdateRecords (Web Services)

Unique identifiers

A unique identifier is a field, or a combination of fields, whose values in individual records are different from all other records, thereby uniquely identifying the record. A compound unique identifier means that all fields in the key must match the fields in the target application in order for a match to occur.

By establishing a unique identifier, you instruct the Data Feed Manager on how to update existing data in the application or questionnaire from the matching source data. After setting the order of the key fields, the Data Feed Manager scans the data source for matches to each unique key in the specified order. If any key is found to match the field in the target application then the record is considered matched. If no match is found, the Data Feed Manager creates a new target application or questionnaire record.

For example, you can select an IP Address field in a record to be your unique identifier. If a data source record has a matching value for the target application field, the source record data updates the target application record data. If no match is found, the data feed creates a new application record.

Note: Matching logic includes text formatting when matching the key fields in the data feed source to a record in the RSA Archer database. When a data feed has two records with the same text, but with different formatting tags, the records are distinguished as separate records.

Fields that act as unique identifiers for your data feed do not have to be the same as the key fields for your target applications or questionnaires.

The following table lists the field types from a target application or questionnaire that can be selected as unique identifiers.

Text-Based Field Types	List-Based Field Types
Text	Values Lists
Numeric	Record Permission
Date	User Groups

Text-Based Field Types	List-Based Field Types
IP Address	Sub-form Fields
Tracking ID ("System ID" only)	

Note: You can only use the Tracking ID field as a key field if it is configured as System ID. If configured as Application ID, it is not available for use as a key field.

Note: If you map a source field for a sub-form and that source field value is blank, then the data feed will not process the sub-form record.

When selecting cross-reference or related records fields as unique identifiers, you must select a field from the related application matching one of the above field types. For example, if you select the Vulnerabilities cross-reference field, which cross-references the Vulnerabilities application, in an Assets application, you also select a qualifying field from the Vulnerabilities application to serve as a unique identifier.

Matching criteria for unique identifiers

The following table describes the matching criteria for unique identifiers.

Option	Description
MatchExact	Specifies that data source field must match the unique identifier value exactly for the target record to be updated. If the match is not exact, a new record is created.
	For example, if a data source field has a value of "Renee Jones" and a mapped application field that is specified as a unique identifier has a value of "Renee Ellen Jones," the target application record is not updated because it is not an exact match.
MatchAny	Specifies that the source data must match at least one condition in the list-based field for the target record to be updated.
	For example, if a target application record has the values Blue and Green selected in the field specified as the unique identifier, and the mapped field in the source data includes only the value Blue, the record is updated because at least one of the values matches.

Option	Description
MatchAll	Specifies that the source data must match all of the conditions in the list-based field for the target record to be updated. For example, if the target application record has the values Blue and Green selected in the field specified as the unique identifier, and the mapped field in the source data includes the values Blue and Green, the record is updated. However, if the source data includes only the value Blue, the record is not updated. A new target application record is created instead because there is not a complete match.

Data feed communication

The Data Feed Manager can be configured to retrieve or receive data from various external data sources using a variety of transport protocols. When given the option, RSA recommends that you select secured versions over unsecured versions.

To strengthen data feed security, RSA recommends that the Data Feed Manager require data feed paths to be specified as relative paths.

Note: Relative path entry is set up as the default starting with RSA Archer 6.0. Because the setting is not updated automatically on systems upgraded to version 6.0, RSA recommends manually setting the requirement on upgraded systems.

BatchContentSave data feed token

Data feeds leveraging the BatchContentSave token should be used with caution. RSA recommends using this token for high-volume ingestion of enrichment content. It is not recommended for content progressing through workflows. Content changes made by a BatchContentSave enabled feed are not tracked within the system History Log fields (though field audit information is retained).

Archer-to-Archer Data Feeds

An Archer-to-Archer data feed provides the ability to pull data from one instance to another through a report-based search. The source data is inserted in its raw or formatted state back into the same application, a different application in the same instance, or an application in a different instance.

An Archer-to-Archer data feed uses the Archer Web Services Transporter. The Archer Web Services Transporter accesses the RSA Archer Web Services API and retrieves data from the specified instance or another instance of RSA Archer. The user account running the search in the API must have at least Read access to the report being used and the application. Record permissions are evaluated as well, and could limit the source data retrieved from the application. Report-based data feeds can use either the report ID or the report GUID during configuration.

For report-based data feeds, create a Global Report and click Apply in the source application. Ensure that content exists for every field in the source application from which you want to import data. If a field in the source application is empty, it will not be available for you to select in the data feed. Use the report GUID when working with the data feed before closing the report.

Important: Do not run the Archer-to-Archer data feed using the same account with which you have logged in to RSA Archer. Using the same credentials logs you out of your session. In addition, do not run multiple data feeds using the same account credentials. Each Archer-to-Archer data feed must have its own separate and unique account for logging in and retrieving data.

Archer Web Services Transporter

The Archer Web Services Transporter must be configured with the same authentication method as configured in Microsoft Internet Information Services (IIS) on the web server. If you do not know the Microsoft IIS configurations, contact your system administrator before continuing.

Guidelines for designating the security credentials

- If IIS is configured for Anonymous authentication, use the Anonymous/Service Account User option. When IIS is set to Anonymous authentication, the user account credentials are not sent with the data feed request.

- If IIS is configured for Windows Integrated authentication, use either Anonymous/Service Account User or Specific.

  - If credentials are set to Anonymous/Service Account User, the service account running the asynchronous job is sent with the data feed request.

  - If credentials are set to Specific, the specified Windows account credentials are sent with the data feed request.

You must also define the transport configuration for this transporter. The Web API uses the search types described in the following table for processing data of a data feed.

Search Type	Description
Report ID	Retrieves data using the search report GUID or ID, which is provided in the search results for the report.
Search XML	Retrieves data using the module ID and a configuration string. This information is obtained by running an XML search using an API call.
Statistic Report ID	Retrieves data using the search statistical report GUID or ID, which is provided in the search results for the statistical report.

Additionally, a data feed can access the source data through a proxy server and can handle post-processing of the local copy of the source data.

Use the following tasks to add an Archer-to-Archer data feed:

- Adding Archer-to-Archer Standard Data Feeds
- Adding Archer-to-Archer Transport Only Data Feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

RSS Data Feeds

The RSS data feed provides the ability to retrieve records from a configured RSS feed into an RSA Archer instance.

Note: RSA recommends that you rely on HTTPS for secure communications between the web server and the RSS transporter. RSA also recommends that you set the RSS iView Content Handling option in the RSA Archer Control Panel to Scrub or Encode to address this issue.

Important: For the data feed to execute successfully, the server responsible for running the data feed must have a service account with valid logon credentials.

Use the following tasks to add an RSS data feed:

- Adding Standard RSS data feeds
- Adding Transport Only RSS data feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

HTTP Data Feeds

The HTTP Transporter data feed enables you to execute a GET or POST to retrieve data from an HTTP or HTTPS site. The data is inserted in its raw or manipulated state into the RSA Archer instance.

The source files must be text delimited files or XML files. You can use an XSLT to transform your XML data into a consumable format.

HTTP Transporter

The HTTP Transporter allows a file from an external source with unknown contents and integrity to be brought onto RSA Archer servers. This flexibility introduces a potential attack vector where the associated risk must be accepted by the customer.

RSA recommends that you disable the HTTP Transporter if a business need does not require its use. If you must use the HTTP Transporter, RSA recommends using HTTPS, selecting Zip File as the File Type, and using encryption by selecting an Encryption Type.

An HTTP Transporter data feed can be configured as a standard or transport data feed type.

Weak ciphers disabled

Important: When weak ciphers have been disabled, data access from an external HTTP or HTTPS site may be impacted. If data is from an external HTTP or HTTPS site, you must be able to access that external site from the server running the services for the data feed to execute successfully.

For more information about disabling weak ciphers, see Host Hardening.

Use the following tasks to add an HTTP data feed:

- Adding Standard HTTP data feeds
- Adding Transport Only HTTP data feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

FTP Data Feeds

The FTP data feed enables you to pull data files using the FTP protocol, and insert that data in its raw or manipulated state into the RSA Archer instance.

The source files can be delimited text files or XML files. You can use an XSLT to transform your XML data into a consumable format.

FTP Transporter

The FTP Transporter allows a file from an external source with unknown contents and integrity to be brought onto RSA Archer servers. This flexibility introduces a potential attack vector where the associated risk must be accepted by the customer.

RSA recommends that you disable the FTP Transporter if a business need does not require its use. If you must use the FTP Transporter, RSA recommends selecting Zip File as the File Type and using encryption by selecting an Encryption Type. You can use a secure connection by enabling SSL and including the IP address in the Outgoing IP Address field in the RSA Archer Control Panel. For more information, see "Configuring Outgoing IP Whitelist" in the RSA Archer Control Panel help.

An FTP Transporter data feed can be configured as a standard or transport data feed type.

Use the following tasks to add an FTP data feed:

- Adding Standard FTP data feeds
- Adding Transport Only FTP data feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

File Data Feeds

The File data feed enables you to pull data directly from a flat file and insert that data in its raw or manipulated state into the RSA Archer instance.

The source files must delimited text files or XML files. You can use an XSLT to transform your XML data into a consumable format. The Data Feed Manager can access files located on a network server that is accessible to the Data Feed Manger. For example, a delimited file must reside on the network server rather than your personal computer.

Important: For the data feed to execute successfully, the server responsible for running the data feed must have the required access to the files.

File Transporter

The File Transporter allows a file from an external source with unknown contents and integrity to be brought onto RSA Archer servers. This flexibility introduces a potential attack vector where the associated risk must be accepted by the customer.

RSA recommends that you disable the File Transporter if a business need does not require its use. If the File Transporter must be used, RSA recommends selecting Zip File as the File Type and using encryption by selecting an Encryption Type.

For more information, see "Transporter Availability" in the RSA Archer Control Panel Help. For information on configuring the File Transporter, see the "Data Feed Manager" section of "Define a File Transporter" in the RSA Archer Online Documentation.

A File Transporter data feed can be configured as a standard or transport data feed type.

Use the following tasks to add a file data feed:

- Adding Standard File data feeds
- Adding Transport Only File data feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

Threat Data Feeds

Threat data feeds aggregate data from external data feed sources into RSA Archer on a dynamic and scheduled basis. The Data Feed Manager supports iDefense and DeepSight threat feeds.

RSA recommends that you rely on HTTPS for secure communications between the web server and the threat feed. For information on enabling HTTPS, see Web Server Communication.

Supported DeepSight feed types

The following table describes the supported Deep-Sight feed types.

Transporter	Supported Feeds
DeepSight Transporter 2.0	Vulnerabilities
DeepSight Transporter 4.0	Security Risk
	Vulnerabilities SCAP

Note: Data feeds using the DeepSight 2.0 transporter will soon become unusable because of deprecation by Symantec. From the RSA Archer Community on RSA Link, download a copy of the data feeds that use the DeepSight 4.0 transporters and import them.

Supported iDefense threat feed types

- Vulnerabilities
- Geopolitical Threat

RSA Archer provides a configuration file to establish a connection between an iDefense or DeepSight threat feed and your instance of RSA Archer. Each of the threat feeds can be quickly integrated with your instance of RSA Archer by importing the configuration file.

For a new threat feed, the first run is the baseload run, which should take place before regular threat feeds run.

- For DeepSight threat feeds, the baseload runs as one job.
- For iDefense, the baseload runs in a series of jobs that pull up to 1,000 alerts at a time. Baseload runs may take a long time to complete—typically under 14 days.

Before you begin: Visit the Integration Exchange

Before you begin a new integration project with Data Feed Manager, visit the RSA Archer Community on RSA Link. In the Integrations category, you can review prebuilt integration packages from RSA Archer and third-party providers such as Qualys, nCircle, and Sendmail.

New integration packages are available regularly, and each package includes the following items:

- Data feed configuration file
- Target application(s)
- Any supporting files (such as an .xslt file)

When you download an integration package from the RSA Archer Community on RSA Link, you can import the configuration file directly into the Data Feed Manager and, if necessary, modify the configuration. You can also import the target applications into the RSA Archer environment and modify the applications through Application Builder.

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

Mail Monitor Data Feeds

The Mail Monitor Transporter data feed enables you to monitor email accounts using mail fields or plain text body XML to specific fields in an application. By pulling email content into RSA Archer, you can assess and process disparate email information, then create and document clear action plans based on the information.

When integrating an application or questionnaire with a Mail Monitor data feed, you can do the following:

- Insert email content into an application or questionnaire.
- Retrieve email messages, such as vulnerability alerts and open source monitoring alerts.
- Define field mapping from email content to content records.
- Configure mail protocols, mail servers, email accounts, and scheduling intervals.

Note: RSA recommends that you configure an SSL connection to connect with the email server.

Important: For the data feed to execute successfully, the server responsible for running the data feed must have a service account with valid logon credentials.

Use the following tasks to add a mail monitor data feed:

- Adding Standard Mail Monitor data feeds
- Adding Transport Only Mail Monitor data feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

Database Query Data Feeds

The Database Query Transporter data feed enables you to pull data directly from a database by query and insert the data in its raw or manipulated state into a RSA Archer instance.

The numerous types of supported database connections are Odbc, OleDb, Oracle, SQL, and many others. As long as the connection string is configured successfully and the client driver is installed on the system, RSA Archer can integrate regardless of the database type.

A Database Query Transporter data feed can be configured as a standard or transport data feed type.

RSA recommends that the external database from which you are capturing data is located within your corporate network and that data transmission occurs over an encrypted communications channel. RSA also recommends that the credentials you use to retrieve the data have read-only permissions. For more information, see "Define a Database Query Transporter" in "Data Feed Manager" in the RSA Archer Online Documentation.

Use the following tasks to add a database query data feed:

- Adding Standard Database Query data feeds

- Adding Transport Only Database Query data feeds

For more information, see "Data Feeds" in the RSA Archer Online Documentation.

Web Server Communication

By default, RSA Archer web clients communicate with the RSA Archer Web Server (IIS) over one of two ports:

- HTTP using default port 80

- HTTPS using default port 443

These web clients include:

- RSA Archer web user interface

- Third-party web applications, which are applications provided by the customer that use RSA Archer web APIs (SOAP and REST)

- Certain data feeds, for example, RSS and Threat Intelligence

RSA recommends that you enable web server communication using HTTPS and disable the HTTP service. In addition to providing encryption of data in transit, HTTPS allows the identification of servers and, optionally, of clients, by means of digital certificates. To enable HTTPS, update the following three components:

- IIS

- RSA Archer web.config

- RSA Archer Control Panel

For more information, see Appendix A: Authentication Configuration.

While HTTPS is recommended and helps prevent man-in-the-middle attacks, consider the following when enabling HTTPS and disabling HTTP:

- Redirecting connections from an unsecured HTTP port to a secured HTTPS port can cause your application to be vulnerable to these types of attack. Redirecting connections is not a complete disablement of the HTTP port.

- Disabling HTTP without ensuring that the SSL certificate is in the trusted certificate store displays an error message.

- Disabling HTTP causes the SOAP API forms to become non-functional. These forms only accept HTTP Post.

RSA recommends that you use TLS 1.2 to secure the HTTP communication between RSA Archer web clients and the RSA Archer Web Server. Secure this communication by configuring HTTPS connections between the client and the IIS web server.

For information on Microsoft recommendations, see the Microsoft Knowledge Base.

SSL Certificate Guidance

To enable Field Encryption in RSA Archer, it is advised that the certificate should be obtained from a trusted Certificate Authority (CA). However, you may choose to generate a self-signed certificate.

RSA recommends using a hardware security module (HSM) for field encryption over a certificate in a local store.

Field Encryption certificate requirements

Certificates must meet the following requirements:

- The certificate is present in the local machine store as a personal certificate.
- The certificate is exportable.
- The certificate is not expired.
- The certificate has a key size of 2048 bits.
- The certificate has a private key.

How to secure a Field Encryption certificate

The certificate being used for encryption should have very limited access. Here are some of the security measures that should be taken to protect the certificate:

- Give Full Control and Read access to the certificate only to the Administrator account. All other accounts should have only Read access.

- Give the certificate read-only access to the following accounts:

  - In a server hosting the archer web application, only the AppPool account used by the web application should be given access (Read-Only) to the certificate.

  - In a server hosting archer services, for example, Configuration Service and Job Framework, only accounts used by the services should be given access (Read-Only) to the certificate.

- Revoke access for all accounts that are not required.

- Back up the encryption certificate regularly. The backup should be password protected and stored safely.

For recommendations on generating/installing an SSL Certificate using IIS, see the Microsoft TechNet Library.

For information about industry best practices, see the following:

- NIST SP 800-52
- PCI-DSS v1.2, point 4.1

SSL Certificate Validation - Redis

Redis does not have built-in support for SSL. RSA recommends using tunneling software, such as stunnel, to enable SSL for your Redis Server. Stunnel configuration involves specifying the port for accepting secure connection and the certificate to be used as the server certificate.

To enable SSL with the Redis SSL client, the certificate thumbprint must be added in the RSA Archer Control Panel. RSA Archer is qualified for the stunnel server. The stunnel server can be configured to do a full certificate validation including certificate chain validation, or a name-sake validation. For the server certificate, the RSA Archer Control Panel does a strict validation of the certificate presented by the server as part of the handshake. For more information on using stunnel with Redis, see the documentation on the Redis website.

Verify that the certificate that is used with the stunnel server satisfies the following conditions:

- The certificate chain is trusted by the RSA Archer Control Panel and all RSA Archer Services and Web servers. All intermediate authorities and the root authority must be trusted on all the servers.

- The certificate is issued with the correct subject name. There cannot be any name mismatch or any other SSL policy errors.

- The certificate must be valid and not expired.

You can test the server connecting in the RSA Archer Control Panel. For more information, see "Testing the Cache Connection" in the RSA Archer Control Panel Help.

SQL Server Communication

RSA recommends that you use a secured database connection to secure the communications between the instance database server and the RSA Archer web and services servers. For recommendations on configuring a secure database connection, see the Microsoft MSDN Library.

The Configuration database cannot accept secure or encrypted connections. RSA recommends that you follow the guidance in SSL Certificate Guidance when issuing an SSL certificate to communicate with SQL Server.

RSA Archer Web Services API

The RSA Archer® Suite Web Services API is a collection of web services that provide a programmatic interface for interacting with the RSA Archer. Each web service supports multiple methods that can be used together to automate the exchange of information between the Platform and an external application.

RSA Archer Web Services

RSA recommends that you rely on HTTPS for secure communications between the RSA Archer web server and the following:

- Third-party web applications, which are applications provided by the customer that use the Platform web APIs

- Archer-to-Archer data feeds

For information on configuring the RSA Archer Archer Web Services transporter, see the RSA Archer Online Documentation.

The following table lists web services that are available.

Available Web Services	
Access Control	The Access Control class provides programmatic access to the Access Control feature, such as creating users and managing security parameters.
Access Role	The Access Role class provides programmatic access to options relating to managing access roles.
Field	The Field class allows you to manage and configure the values lists used in the applications, questionnaires, and sub-forms.
General	The General class allows you to create and terminate Web Services API user sessions.
Module	The Module class provides programmatic access to module information.

Available Web Services	
Record	The Record class allows you to create and manipulate content records in content applications.
Search	The Search class allows programmatic access to the Platform's search features.

Encryption of Data at Rest

RSA recommends that you back up your sensitive data, encrypt it, and keep it in a secure physical location in accordance with your corporate disaster recovery and business continuity policies, including the following:

- A full backup of your database (For more information, see the Microsoft TechNet Library.)
- Log files
- Configuration files
- Password for the RSA Archer System Administrator

To help protect online data, such as current database, log file, and configuration files, RSA recommends that you restrict access to the files and database and configure permissions only to trusted administrators.

The file repository and Windows certificate store must be located on separate machines.

Encrypting Data

RSA Archer allows you to encrypt the following field types in an application:

- Attachment
- Date
- IP Address
- Image
- Numeric
- Text

The purpose of encryption is to protect sensitive data in the database and the file repository. Encrypted field data is stored in the Encrypted folder in the file repository. When you encrypt a field, all data in that field, whether in the record or through a data feed or import, is encrypted in the database. Encrypted fields display data in the record as normal text. Files and images associated with encrypted attachment and image fields are decrypted when downloaded. You can encrypt new and existing fields.

The following table shows how encrypted fields affect other functionality in the application or RSA Archer.

Related Area	Impact
Calculations	You cannot reference encrypted fields in a calculated field. You can calculate encrypted fields.
Data feeds/imports	If the incoming data targets an encrypted field, the data will be stored in the database in an encrypted format. Archer to Archer data feeds support encrypted attachments and images. When encrypted files are exported from an instance, they are unencrypted. If the target instance has encryption enabled, the files are encrypted. If the target instance does not have encryption enabled, the files are not encrypted.
History log	History logs are kept for encrypted fields.
Search (global search)	Encrypted fields are not supported.
Advanced search filters	Encrypted fields support only Equals and Does Not Equal filters. Encrypted fields cannot perform statistical search operations, for example Group By and Count.
Layout rule filters	Encrypted fields are supported for all standard field filter options in a layout rule.
Record Lookup Configuration	Only the filter options Equals, Does Not Equal, Field Value Match, and Field Value Does Not Match are available for encrypted fields.
RSA Archer Mobile application	Encrypted fields are not supported.
RSA Archer BCM mobile application	Encrypted fields are not supported.
Offline sync	You cannot sync an application with encrypted fields offline.
Subscription Notification filters	Only the filter options Equals, Does Not Equal, Field Value Match, and Field Value Does Not Match are available for encrypted fields.

Enable field encryption at the instance level

You must enable field encryption at the instance level in the RSA Archer Control Panel. For more information, see "Enable Field Encryption for an Instance" in the RSA Archer Control Panel Help.

Note: If you do not first enable field encryption at the instance level, users receive the following message when they try to encrypt a field:

Field encryption must be enabled in the RSA Archer Control Panel.

Troubleshooting field encryption

The following table describes how to troubleshoot field encryption.

Issue	Cause	Resolution
Encrypted fields do not display the data.	The Key Encryption Key (KEK) for one or more of your instances is missing.	Verify whether the KEK is present on each of your Web Servers and Services Servers and add the KEK wherever it is missing. For instructions, see "Enable Field Encryption for an Instance" in the RSA Archer Control Panel Help.
When a user logs in, the following message appears: Configuration error, some of the data may be blank. Please contact your administrator.		
When the system administrator logs in, the following message appears: The encryption key is missing. Please provide a new key in the system. Dismiss?		
The following message appears in the error logs: Either Key Encryption Key is missing or inaccessible.		
When editing an encrypted field, you receive an unexpected error.		
When the Configuration Service is starting, the following message appears: Key Encryption Key for the following instances were either missing or could not be accessed: *Instance1*, *Instance2*.		

Configuring the Hardware Security Module

You can configure the settings for the Hardware Security Module (HSM) in connection with field encryption.

Note: You must complete this task before you can enable field encryption for an instance.

1. Locate and copy the module token for the key store and security pin (or pass phrase) as configured with the HSM hardware.

2. On the General tab, go to the Hardware Security Module section.

    a. Open the RSA Archer Control Panel.

    b. Go to Installation Settings.

    c. Click the General tab.

3. In the Hardware Security Module section, select a module from the drop-down list.

4. In Module Token, enter the module value.

5. In Security Pin, enter the security pin value.

6. On the toolbar, click Save.

Additional Security Considerations

- Application Programming Interface (API)
- Elasticsearch Security Considerations
- JavaScript Transporter Security Considerations
- Privilege Levels for Archer Services
- Least Privileges Requirements for RSA Archer Database Objects
- File Repository Path
- Restrict Permissions on Repository Files
- Keyword Index Files
- Company Files Path
- Building Global iViews
- Formatting iView Videos
- Adding Objects to the Layout
- Offline Access

- [Installing Offline Access](#)
- [Disabling Metadata Publishing in ASMX Web Services](#)
- [Proxy Bypass Security Considerations](#)
- [RSA Archer Suite Mobile App Security Considerations](#)

Application Programming Interface (API)

RSA provides three types of APIs for your use.

- RESTful API
- Content API
- Web Services API

With general API usage, RSA recommends logging and regularly auditing the source, time, and summary data submitted and received by APIs.

Elasticsearch Security Considerations

For a secure implementation for authentication, authorization, and secured information, RSA recommends implementing an Elasticsearch security plug-in that provides these features. A security plug-in enables users to configure a certificate to secure the transport layer using SSL/TLS. This ensures secured communication between RSA Archer and Elasticsearch as well as secure communication between Elasticsearch nodes.

RSA recommends deploying Elasticsearch in a secure cluster configuration. In the RSA Archer Control Panel (ACP), you can configure the connection parameters for communication between the cluster and RSA Archer. For more information about configuring Elasticsearch, see "Enabling Elasticsearch" in the RSA Archer Control Panel Help.

RSA recommends taking the following additional security considerations into account when using Elasticsearch:

- Elasticsearch should be configured for unicast network discovery. This prevents a new node from joining the cluster unless explicitly specified.

- In the event of index deletion or corruption, the Elasticsearch Index can be rebuilt. For more information, see "Rebuilding Search Indexes" in the RSA Archer Control Panel Help.

- When using Elasticsearch, data is stored in RSA Archer and the Elasticsearch cluster node. RSA recommends following best security practices for data in both locations as outlined in Encryption of Data at Rest.

- If visualization tools are used with Elasticsearch, users should ensure the tools are securely deployed following guidance from the tool provider to protect RSA Archer data.

- Encrypted field types in RSA Archer will also be stored as encrypted fields in the data store for Elasticsearch in the RSA Archer database. For more information, see Encrypting Data.

JavaScript Transporter Security Considerations

The JavaScript Transporter allows you to integrate RSA Archer with external systems without a middleware. You can use the JavaScript Transporter to upload and execute a NodeJS program. The NodeJS program can consume APIs exposed by external systems to process and feed data into RSA Archer. Here are a few security recommendations to consider when using this feature:

- Communicate with external systems using APIs protected by SSL\TLS protocol.

- Communicate with external systems using APIs that involve a strong authentication mechanism.

- Mark sensitive parameters as "Protected" in the Custom Parameters section of the Transport tab in the JavaScript Transporter Settings in the RSA Archer Control Panel.

- If you create a JavaScript file, it is recommended to sign the file and enter the digital thumbprint of the trusted certificate in the JavaScript Transporter Settings in the RSA Archer Control Panel. For more information, see "Obtaining Digital Thumbprints" and "Configuring JavaScript Transporter Settings" in the RSA Archer Control Panel Help.

Privilege Levels for Archer Services

RSA strongly recommends that you set Archer services to run with Domain User account privileges. In general, RSA Archer services should run with the lowest privilege level that allows them to work. For instructions on setting Archer service privileges, see "Task 14: Configure the service credentials" in the "Installing the Web Application and Services Components" section of the *RSA Archer Platform Installation and Upgrade Guide*.

Local System privileges give Archer services unrestricted access to local system resources. While this level of privilege allows the services to access all system resources easily, giving unrestricted access to many services and accounts increases the security vulnerability of a system. Organizations concerned with system security should avoid giving Local System privileges to services and accounts without serious justification.

To improve system security, set services and accounts to run with Domain User account privileges that limit their access to only the system resources they need for normal business operations. This approach to setting privilege levels keeps the number of services and accounts with unrestricted system access to a minimum, which reduces the number of entities that can unintentionally or intentionally violate system security.

Least Privileges Requirement for RSA Archer Database Objects

The principle of least privileges grants the minimum permissions required for day-to-day operations of RSA Archer. To operate on a day-to-day basis using least privileges, the database user account connecting to both the Instance and Configuration databases requires the following privileges:

- Data Reader Rights (member of the db_datareader).

- Data Writer Rights (member of the db_datawriter).

- Execute permissions on all stored procedures and scalar functions.

- Select permissions on all views, table-valued functions, and in-line functions.

- Execute permissions on the system stored procedure sp_procedure_params_100_managed of the master database.

- Execute permissions on the user-defined table type content_date_Table_Type of the Platform Instance database.

- Reference permissions on the user-defined table type content_date_Table_Type of the Platform Instance database.

- Execute permissions on the _BulkType user-defined table types of the Platform Instance database, if provisioned for Offline Access.

- Reference permissions on the _BulkType user-defined table types of the Platform Instance database, if provisioned for Offline Access.

Within the Instance and Configuration databases, the user must have access to objects belonging to both the dbo and mswf4 schemas.

When installing or upgrading RSA Archer, use an account with a membership to the db_owner.

File Repository Path

RSA Archer uses a folder on the file system for storing files. The default location is C:\ArcherFiles\Repository.

RSA recommends that you define the location of the repository folder in RSA Archer to be a share that uses a UNC path outside of any web and services servers. Doing so eliminates the possibility of denial of service attacks and large file creation.

Note: If you plan to use data encryption, the file repository and Windows certificate store must be located on separate machines.

For instructions on setting the repository path, see "Designate the File Repository Path" in the RSA Archer Online Documentation. For configuration and permission details for the repository folder, see the *RSA Archer Platform Installation and Upgrade Guide*.

Restrict Permissions on Repository Files

RSA recommends that you restrict permissions on the repository folder (default location C:\ArcherFiles\Repository) to read, write, and modify for the account that the IIS processes are running as and for the account that the Job Engine service is running as.

1. Log on to Windows servers.

2. Click Start > Administrative Tools > Services.
   For the Job Engine, the Log On As column identifies the account the service runs as.

3. Change each account as needed.

Note: The Microsoft IIS process account is configured in Microsoft IIS.

Keyword Index Files

RSA Archer uses a folder on the file system for storing keyword index files. The default location is C:\ArcherFiles\Indexes.

RSA recommends that you do the following:

- Restrict the permissions on the keyword index files folder to read, write, and modify for the account that the Queuing service is running as.

- Define the location of the indexes folder in RSA Archer to be a path set to off of any web server (avoid using a UNC path if possible to avoid performance impacts). The path can be a local path if the RSA Archer installation includes a dedicated Services server.

Company Files Path

RSA Archer uses the company_files folder to store company images and icons for the web application. The location of the folder is set during the initial installation and defaults to C:\Inetpub\wwwroot\RSAArcher\company_files.

RSA recommends that you define the location of the company_files folder in RSA Archer to use a UNC path outside of any web servers, which eliminates the possibility of denial of service attacks and large file creation.

For configuration and permission details for the company_files folder, see the *RSA Archer Platform Installation and Upgrade Guide*.

Building Global iViews

iViews are configurable according to the specific iView type.

For example, for a Report iView, you can include one or many reports, determine the selection order of the reports in the iView, and identify the report that is initially displayed to the user. You can move across and expand iViews in six columns to display more information. You can also allow horizontal scrolling for any of the selected reports to extend the report contents beyond the width of the iView.

iView types

The following table describes the types of iViews.

iView Type	Description
Canvas	Displays predefined templates with various presentations for content and graphics.
Custom	Displays custom text, HTML, or Flash presentations or to run custom scripts, such as JavaScript. RSA recommends that only trusted Administrators have permission to create and edit custom iViews.
Embedded URL	Embeds entire web pages directly in an iView. **Note:** Embedded URL iViews do not support scroll bars.
Global Search	Displays search criteria options in an iView for the user to search records across applications.
Landing Page	Displays links to frequently used tasks. You can use the Landing Page iView as a home page to easily access your selected links.
Links List	Displays links to websites, intranet sites, and frequently used internal application pages in a single iView.
Report	Displays global reports in a single iView. Also, you can display charts that are generated through a statistics search.
RSS Feed	Displays data from an RSS feed. RSS feeds contain headlines and summary information from articles on websites supporting RSS.
Video	Embeds video directly in an iView using HTML.

Before you begin

1. Build a workspace.
2. Build a dashboard.

Build a global iView

1. Go to the Manage Global iViews page.

   a. From the menu bar, click 🔧 .

    b. Under Workspaces and Dashboards, click Global iViews.

2. Click Add New, and do one of the following:

- To create a new iView, select Create a new Global iView from scratch.

    a. Select the type of global iView you want to create.

    b. Click OK.

- To create a global iView from an existing iView, click Copy an existing Global iView, and then select the Global iView you want to copy.

3. Click OK.

4. Complete the setup for your iView.

Build a canvas iView

    a. In the General Information section, enter the name and a description.

    b. In the Folder field, select or create a folder.

    c. In the Options section, in the Canvas Style field, click ⸱⸱⸱ to select a layout in the Selected Layout Template dialog box.

    d. Select the layout that you want, and click OK.

    e. Enter a name in the Title field.

    f. Enter the content in the Content field.

    g. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build a custom iView

    a. In the General Information section, enter the name and a description.

    b. In the Folder field, select or create a folder.

    c. In the Options section, in the Custom Content field, enter the content.

    d. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build an embedded URL

    a. In the General Information section, enter the name and a description.

    b. In the Folder field, select or create a folder.

    c. In the Options section, in the URL filed, enter the URL you want to embed.

d. (Optional) Select an option from the Refresh Rate list.

e. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build a global search iView

a. In the General Information section, enter the name and a description.

b. In the Folder field, select or create a folder.

c. In the Options section, in the column Display field, choose One Column or Two Columns.

d. (Optional) In the Description field, select Embed the iView description in the iView to display the description in the iView.

e. (Optional) In the Search Button field, click Add to add a search button.

    i. In the Files to Upload section, click Add New.

    ii. Select the file you wish to add, and click OK.

    iii. In the Available Graphics section, click Add New.

    iv. Click OK again.

f. (Optional) In the Applications section, click Add New to define the applications for the search.

    i. From the Application Name list, select the application that you want to associate the iView to.

    ii. Make selections from the Visibility field and Defaulted Behavior field.

g. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build a landing page iView

a. In the General Information section, enter the name and description.

b. In the Folder field, select or create a folder.

c. In the Background field, select an available image from the Standard and Custom tabs.

    i. To add a custom background image, on the Custom tab, click Add New.

    ii. In the File to Upload section, click Add New.

    iii. Select the file you want to add, and click OK.

    iv. On the Custom tab, select the background image.

    v. Click OK.

    d. In the Title field, enter a title for the Landing Page iView.

    e. In the Configuration section, add columns.

        i. Click Add New.

        ii. To add a link, do one of the following:

             ○ To select a link from the Available Links field, double click the link.

             ○ Enter a link and click Add.

        iii. Repeat the previous step to add up to eight links to the iView.

            Note: If you select more than four links, the iView will automatically use two columns.

        iv. To configure the display order, click Display Order.

        v. Click OK.

    f. (Optional) In the Documentation section, click Add New to add documentation.

    g. Click OK.

Build a links list iView

    a. In the General Information section, enter the name and a description.

    b. In the Folder field, select or create a folder.

    c. In the Options section, in the Layout field, select Simple List or Descriptive Links.

        Note: If you selected Descriptive Links, enter a name and description.

    d. Insert a link in one of the following ways.

        ● Select a link from the Available Links field by double clicking it.

        ● Type in a link and click Add.

    e. In the Background field, select an image from the Standard or Custom tabs.

        i. To add a custom background image, on the Custom tab, click Add New.

        ii. In the File to Upload section, click Add New.

        iii. Select the file you want to add, and click OK.

        iv. On the Custom tab, select the background image.

        v. Click OK.

    f. In the Column Display field, select One Column or Two Columns.

    g. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build a report iView

a. In the General Information section, enter the name and a description.

b. In the Folder field, select or create a folder.

c. In the Options section, in the Reports field, select the report or reports that you want displayed in the iView from the Available Reports list.

d. To determine the selection order of the reports in the iView, highlight the report title and use ⬇⬆ to arrange the reports in the preferred order.

   Note: The first report listed is the report that is initially displayed to the user.

e. Select Enable Scrolling for each report that you want to allow horizontal scrolling.

f. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build an RSS feed iView

a. In the General Information section, enter the name and a description.

b. In the Folder field, select or create a folder.

c. In the Options section, in the URL field, select an address from the URL list and enter the URL address.

d. In the Feed Elements field, select the display options that you want.

e. In the Articles Displayed field, select the number of articles that you want to display.

f. In the Refresh Rate field, select how often you want the feed refreshed.

g. In the Authentication field, select your authentication preferences.

h. In the Days Displayed field, select the number of days to display the feed.

i. (Optional) In the Documentation section, click Add New to add documentation to your iView.

Build a video iView

a. In the General Information section, enter the name and a description.

b. In the Folder field, select or create a folder.

c. In the Embedded Video HTML field, enter the embedded HTML or the URL.
   Important: For proper formatting guidelines, see Formatting iView Videos.

d. (Optional) In the Documentation section, click Add New to add documentation to your iView.

5. Click Save or Apply.

- Click Save to save and exit.

- Click Apply to apply the changes and continue working.

Create a folder for a Global iView

1. Go to the General Tab of the iView that you want to modify.

   a. From the menu bar, click 🔧 .

   b. Under Workspaces and Dashboards, click Global iViews.

   c. Select the global iView.

2. In the General Information Section, in the Folder field, click Edit.

3. In the Manage Folders window, click Add New.

4. Enter the name of the folder, and click OK.

5. In the Folder list, ensure that the correct folder is selected.

6. Click Save or Apply.

   - Click Save to save and exit.

   - Click Apply to apply the changes and continue working.

Update an iView display

1. In the iView title bar, click ⋯ and select Edit Properties.

2. In the Options section, edit the iView display as needed, and click OK.

   Note: The list of available menu options depends on the type of iView that you are viewing and the access rights assigned to you by your administrator.

3. (Optional) To resize the iView, click, hold and drag the arrow in the bottom-right corner of the iView, and click Save Changes.

4. (Optional) To move the iView, click the title bar of the iView and drag the iView to the new location, and click Save Changes.

Delete a global iView

Deleting a global iView permanently purges the dashboard from the database. Only administrators can delete global iViews.

Important: If you delete an iView, it cannot be recovered.

1. Go to the Manage Global iViews page.

   a. From the menu bar, click ⬩ .

   b. Under Workspaces and Dashboards, click Global iViews.

2. In the Actions column of the iView you want to delete, click 🗑.

3. Click OK.

Formatting iView Videos

You can embed videos into an RSA Archer iView from both external or internal sources.

Embedding From an External Source

If you are embedding a video from an external source, such as YouTube, you must take the embed code provided by YouTube and add ?wmode=transparent to the end of the URL. For example:

Sample YouTube source embed code:

<iframe width="560" height="315" src="https://www.youtube.com/embed/xyz" frameborder="0" allowfullscreen></iframe>

Add ?wmode=transparent to the end of the URL:

<iframe width="560" height="315" src="https://www.youtube.com/embed/xyz?wmode=transparent" frameborder="0" allowfullscreen></iframe>

Important: If you do not add ?mode=transparent to the end of the URL, the video displays improperly.

Embedding From an Internal Source

If you are embedding a video that is being hosted locally, use the <video> tag to ensure proper functionality. For example:

Sample internal source embed code:

<video width="320" height="240" controls>

<source src="/ACME_Company/video.mp4" type="video/mp4">

</video>

Adding Objects to the Layout

You can drag-and-drop objects, such as fields, tab sets, sections, text boxes, placeholders, custom objects, and trending charts on the layouts of applications, questionnaires, and sub-forms. After adding an object to the layout area, you can move the object up or down, from column to column, or from tab to tab. You can also configure some objects to span across multiple columns in the layout.

Key guidelines for adding objects to the layout

- To move a single object, click the object and drag it to the location you want.

- If you are working in a multi-tab layout and you want to move an object from one tab to another, click and drag the object to the tab you want.

- If you are working in a two-column layout and want a custom object, placeholder, text box, or trending chart to span across columns, do the following:

  1. Click the drop down arrow on the layout object.

  2. Select Edit Span Properties and select one of the following options from the Column Span section.

     The following table describes the options.

Option	Description
Do not span columns	The element consumes only one column of space.
Span two columns	The element always spans across the two columns.

  3. Select one of the following options from the Row Span section.

     The following table describes the options.

Option	Description
Do not span rows	The element consumes only one row of space.
Span	The element consumes the number of rows you select from the Rows span box.

Add tab sets to the layout

Tab sets provide a means for grouping related tabs and fields, especially when there is a large number of fields, to help users quickly find the fields they need to add or edit in a record.

For more information on adding tab sets, see "Adding Tab Sets to the Layout" in the RSA Archer Online Documentation.

Add sections to the layout

Add sections as headings to group related fields together. For example, create a section called "Contact Information" to group together a contact's phone, fax, and email information.

1. Open the layout that you want to update.

   a. From the menu bar, click   .

   b. Under Application Builder, click Applications, Questionnaires, or Sub-Forms.

   c. Select the application, questionnaire, or sub-form.

   d. Click the Layout tab.

   e. If you have Advanced Workflow enabled, open the layout that you want to update, and click the Designer tab.

2. In the left pane, expand the Add New Layout Object list.

3. Click and drag the Add Section option to the layout area.

4. In the Section Name field, enter the heading that you want to display in the layout.

5. In the Default Visibility field, select the Expanded or Collapsed option depending on whether you want the section to be expanded or collapsed by default.

6. (Optional) Do one or both of the following to add panel text or help text to the section:

   - To add an information panel to provide your users with additional details about the section, select Panel Text and enter the text that you want to display.

   - To add Help text to provide your users with detailed instructions and background information about the section, select Help Text and enter the text that you want to display.

7. (Optional) Customize your text and add dynamic elements, such as images and Flash animation, using the options available in the Rich Text Editor toolbar.

8. Click OK to close the Section Description dialog box.

9. Click Save or Apply.

   - Click Save to save and exit.

   - Click Apply to apply the changes and continue working.

Add text boxes to the layout

Text boxes provide guidance or additional information that users need to successfully interact with fields.

1. Open the layout that you want to update.

   a. From the menu bar, click 🔧 .

   b. Under Application Builder, click Applications, Questionnaires, or Sub-Forms.

   c. Select the application, questionnaire, or sub-form.

   d. Click the Layout tab.

   e. If you have Advanced Workflow enabled, open the layout that you want to update, and click the Designer tab.

2. (Optional) For a leveled application, select the data level from the Level list in the left pane for the layout you want to update.

3. In the left pane, expand the Add New Layout Object list.

4. Click and drag the Add Text Box option to the layout area.

5. In the Text Box Name field, enter a name for the text box.

6. In the Text field, enter the text that you want to display in the text box when it is displayed for users as they add, edit, or view records.

7. Select one of the following options.

   The following table describes the options.

Field	Description
Edit Mode	Displays the custom object when editing a record.
View Mode	Displays the custom object when viewing a record.
Both	Displays the custom object when viewing or editing a record.

8. Click OK.

9. Click Save or Apply.

   - Click Save to save and exit.

   - Click Apply to apply the changes and continue working.

Add placeholders to the layout

Placeholders create space between other layout objects, such as fields, sections, text boxes, and custom objects.

1. Open the layout that you want to update.

   a. From the menu bar, click .

   b. Under Application Builder, click Applications, Questionnaires, or Sub-Forms.

   c. Select the application, questionnaire, or sub-form.

   d. Click the Layout tab.

   e. If you have Advanced Workflow enabled, open the layout that you want to update, and click the Designer tab.

2. (Optional) For a leveled application, select the data level from the Level list in the left pane for the layout you want to update.

3. In the left pane, expand the Add New Layout Object list.

4. Click and drag the Add Placeholder option to the layout area.

5. Click Save or Apply.

   - Click Save to save and exit.

   - Click Apply to apply the changes and continue working.

Add custom objects to the layout

Custom objects enable you to enter code you have written to create buttons or other objects. For example, you can create Next and Previous buttons using JavaScript code so that your user can click to move from tab to tab when adding or editing records.

Note: RSA recommends that only trusted administrators create and edit custom layout objects, as this flexibility introduces a potential attack vector.

1. Open the layout that you want to update.

   a. From the menu bar, click .

   b. Under Application Builder, click Applications, Questionnaires, or Sub-Forms.

   c. Select the application, questionnaire, or sub-form.

   d. Click the Layout tab.

   e. If you have Advanced Workflow enabled, open the layout that you want to update, and click the Designer tab.

2. If you are working in a leveled application, from the Level list in the left pane, select the data level that contains the layout you want to manage.

The fields and other page elements for that level are displayed in the layout area and in the Available Fields list.

3. In the left pane, expand the Add New Layout Object list.

4. Click and drag the Add Custom Object option to the layout area.

5. In the Name field, enter a name for the custom object.
   This name is displayed on the Layout tab of the Manage Applications or Manage Questionnaires page, but it is not displayed for users when they add, edit, or view records in the application.

6. In the Description field, enter a description for the object.

7. In the Code field, enter or paste the HTML or JavaScript code for the object.

8. In the Display section, select one of the following modes for the object to be displayed as users add and edit records in the application.

   The following table describes the options.

Field	Description
Edit Mode	Displays the custom object when editing a record.
View Mode	Displays the custom object when viewing a record.
Both	Displays the custom object when viewing or editing a record.

9. Click OK.

10. Click Save or Apply.

   - Click Save to save and exit.

   - Click Apply to apply the changes and continue working.

Add trending charts to the layout

On a trending chart, you can view historical data for a Numeric or Values List field that has trending enabled, in order to identify patterns in the data for a specified period of time. Trending charts must be added to another container object, such as a section.

1. Open the layout that you want to update.

   a. From the menu bar, click   .

   b. Under Application Builder, click Applications, Questionnaires, or Sub-Forms.

   c. Select the application, questionnaire, or sub-form.

    d. Click the Layout tab.

    e. If you have Advanced Workflow enabled, open the layout that you want to update, and click the Designer tab.

2. In the left pane, expand the Add New Layout Object list.

3. Click and drag the Add Trending Chart option to the layout area.

4. In the Name field, enter the heading that you want to display in the layout.

5. From the Trending Field list, select the trending-enabled field for which to display chart data.

6. (Optional) In the Show Title field, click the Display the chart name as the title when users open the application or questionnaire.

7. Click OK.

8. Click Save or Apply.

- Click Save to save and exit.

- Click Apply to apply the changes and continue working.

Add report objects to the layout

Report Objects allows you to embed reports directly within records. The system applies default filters based on the filters used to create the base report. However, administrators can override default filters, as well as the advanced operator logic. When viewing a report object record, users can click on the report, which opens a new search results page with the filters already applied. Based on user permissions, users can modify the report.

1. Open the layout that you want to update.

    a. From the menu bar, click   .

    b. Under Application Builder, click Applications or Questionnaires.

    c. Select the application or questionnaire.

    d. Click the Layout tab.

    e. If you have Advanced Workflow enabled, open the layout that you want to update, and click the Designer tab.

2. In the left pane, expand the Add New Layout Object list.

3. Click and drag the Add Report Object option to the layout area.

4. In the Name field, enter a name for the report object.

   Note: This name displays on the Layout tab of the Manage Applications or Manage Questionnaires page, but does not display for users when they add, edit, or view records in the application.

5. In the Description field, enter a description for the record object.

6. Under Report Selection, select the report from the Available Reports column.

   Note: Only one report can be selected.

   Note: Only global and search based reports are available for selection.

7. (Optional) Add or update filter options for how you want to view the report.

   Note: If the selected report has default filters, they are automatically populated as existing filters.

   a. In the Field to Evaluate field, select the field to evaluate for one or more specific values.

   b. In the Operator column, select the filter operator. For more information, see "Report Operator Field Types" in the RSA Archer Online Documentation.

   c. In the Value(s) column, select the values for the condition. Depending on the operator type, the selection can be a value or a field.

   d. (Optional) To create additional conditions, click Add New and repeat steps a-c.

   e. (Optional) If you create more than one condition, apply logic to your filter criteria in the Advanced Operator Logic section. For more information, see "Advanced Operator Logic" in the RSA Archer Online Documentation.

8. In the Load Report section, select one of the following modes for the report object to be displayed as users add and edit records in the application.

   The following table describes the modes.

Field	Description
Immediately	Displays the report object when the page loads.
On Demand	Displays the report object on user click.

9. In the Display section, select one of the following modes for the record object to be displayed as users add and edit records in the application.

The following table describes the modes.

Field	Description
Edit Mode	Displays the report object when editing a record.
View Mode	Displays the report object when viewing a record.
Both	Displays the report object when viewing or editing a record.

10. Click OK.

11. Click Save or Apply.

- Click Save to save and exit.

- Click Apply to apply the changes and continue working.

Offline Access

Offline access enables Audit Engagements & Workpapers users to conduct audits offline on a laptop. Offline access is available with an active Audit Engagements & Workpapers license and is configurable for each instance. You must enable offline access in the RSA Archer Control Panel. For a complete list of requirements, see Installing Offline Access.

As an administrator, you select the application or questionnaire that is eligible for offline access. What you select determines which records an offline access user can select for offline use. All data, including cross-referenced and related records, for the specified records download to the offline access database and are available for offline use on a laptop.

RSA recommends that only trusted users with secure laptops with strict firewall rules restricting remote access to Offline Access have permission to Offline Access.

RSA Archer features not supported for offline access

The following are features not supported for offline access:

- Application Builder

- Data Feeds

- Data Publications

- Data Imports

- Discussion Forums

- LDAP Synchronization

- Notifications

- Packaging

- Training and Awareness

- User Preferences

Note: Records from a retired application are not supported in offline access. You can view User Preferences, but you cannot edit them in offline access.

Use the Offline Access Gateway to select the application or questionnaire that will have offline access for RSA Archer. After you determine which application or questionnaire you want for offline access, you can then manage the records in the offline access library.

Installing Offline Access

The installation process for Offline Access is separate from the RSA Archer installation. RSA recommends installing Offline Access on a client laptop or computer. To install Offline Access, use the installation wizard to guide you through the process.

Note: Currently, Offline Access supports the Audit Engagement, Audit Entity, Audit Plan, Audit Workpaper, IA Engagement and Assessment Results, Internal Audit Department Annual Review, Plan Entity and Question Library applications.

Preparing for Offline Access Installation

The following table lists the requirements your system must meet before installing offline access.

Component	Requirement
Operating System	Windows 10 64-bit
Memory	8 GB RAM
Disk Space	100 GB Hard Drive
Additional Software	Microsoft .NET Framework 4.7.2

Important: Microsoft Sync Framework 2.1 is required and must be installed on the Services Server. For more information, see "Preparing the Services Servers" in the *RSA Archer Installation and Upgrade Guide*.

By default, the offline access data is stored on the local computer at C:\Users\[username]\AppData\Roaming\RSA Archer\Offline Access\. Isolating the offline access data ensures that each offline access user has their own environment for working offline. For example, when a user purges offline access data, only the offline access data of that user is purged.

Anti-virus and firewall applications may interfere with Offline Access run-time activities. You must add the Offline Access installation file as a trusted file/process/installer/updater for any anti-virus and firewall applications that may interfere with the installation.

Before running offline access, start the Distributed Transaction Coordinator service on the laptop using offline access.

Install Offline Access

The offline access version must always match the RSA Archer version.

Important: You must have administrator rights to install offline access. If you are upgrading offline access, close the Offline Access utility before starting the installation.

1. Contact your IT Administrator to obtain the Offline Access installation file.
   The IT Administrator downloads the Offline Access installation file from the RSA site and can provide it to you or auto-deploy the file through a software management system.

2. Double-click the Offline Access installation file.

3. On the RSA Archer Offline - InstallShield Wizard page, click Next.

4. Read the license agreement. Select I accept the terms in the license agreement. Click Next.

5. Do one of the following:

   - To accept the default installation folder, click Next.

   - To designate a different installation folder, click Change and specify the path to the folder where you want to install offline access.

6. Click Install. This process takes several minutes to complete.

7. Click Finish to complete the installation.

8. Add the following Offline Access files as trusted processes for any anti-virus and firewall applications.
   The following table lists the files and their default locations.

File or Process	Default Location
Archer.Offline.Tools.Controller.exe	C:\Program Files\RSA Archer\Offline Access
Archer.Services.Queuing.exe	C:\Program Files\RSA Archer\Offline Access\services
ArcherTech.JobFramework.Cache.exe	C:\Program Files\RSA Archer\Offline Access\services

File or Process	Default Location
ArcherTech.JobFramework.Host.exe	C:\Program Files\RSA Archer\Offline Access\services
ArcherTech.JobFramework.Job.exe	C:\Program Files\RSA Archer\Offline Access\services
iisexpress.exe	C:\Program Files\IIS Express
sqlservr.exe	C:\Program Files\Microsoft SQL Server\110\LocalDB\Binn\sqlservr.exe
SqlLocalDB.exe	C:\Program Files\Microsoft SQL Server\110\Tools\Binn\SqlLocalDB.exe

Disabling Metadata Publishing in ASMX Web Services

ASMX web services have metadata publishing enabled, which allows WSDL and DISCO metatdata to be retrieved. In order to protect web services from attackers, turn off the documentation protocol in ASMX web services on RSA Archer production servers.

Disable ASMX metadata publishing

Configure the RSA Archer web.config file to remove the documentation protocol publishing on ASMX web services.

1. In the web.config file, locate <system.web>.

2. In the child expression <webServices>, add the following:

   <protocols>

   <remove name="Documentation"/>

   </protocols>

3. Click Save.

4. Perform an IIS reset.

Proxy Bypass Security Considerations

When a proxy is configured and enabled in the Archer Control Panel (ACP), RSA Archer components interacting with one another via proxy may cause undue system load. However, an IP/DNS exception—available in the proxy settings of the ACP—allows for communication between components without using a proxy.

When configuring this feature to bypass your existing, configured ACP proxy, there are some security recommendations to be considered:

- Carefully consider the additions and removals of the IP/DNS entries, as the bypass is a whitelist.

- Only bypass external systems which have SSL/TLS protection enabled to allow communication with internal systems.

- Only bypass external systems with strong authentication systems in place.

- Only bypass URLs/IPs approved by your IT department.

Chapter 2: Secure Deployment and Usage Settings

Secure Deployment and Usage Settings

It is important to secure the deployment and usage settings in RSA Archer. Doing this helps protect the RSA Archer environment.

Protect all physical, local, and remote access to the servers hosting RSA Archer. Restrict all access methods to the absolute minimum required to maintain RSA Archer.

RSA recommends that you do not set up RSA Archer test environments to contain exact copies of the full production environment's data or to use the same system or authentication secrets. If the test environment contains any sensitive information from the production environment, take the same precautions to protect the test environment as you do in the production environment.

Security Controls Map

An RSA Archer deployment consists of three physical tiers: a web tier, a services tier, and a database tier. An organization can deploy RSA Archer in a single host configuration or a multi-host configuration. For more information, see the *RSA Archer Platform Installation and Upgrade Guide*.

When deploying RSA Archer on-premise within a corporate network, RSA recommends that you do the following:

- Deploy RSA Archer hosts within the corporate network. The DMZ-to-Corporate-Network Firewall intercepts all communication between the single host and the other components in the network.

- Ensure that users are accessing RSA Archer from within the corporate network. If users must access RSA Archer from the internet, RSA recommends that they connect to the corporate network through a secure VPN connection.

- Allow only remote access to RSA Archer hosts for secure maintenance using the Remote Desktop Protocol (RDP) through a secure VPN connection.

- Configure firewall rules to ensure secure communication between RSA Archer and other components in the network.

Important: RSA recommends that you deploy RSA Archer services in a secure location, where physical access to the servers is restricted to the personnel who manage the servers.

The following figure shows an example of a multi-host configuration.

For multi-host configurations, RSA Archer recommends that you do the following:

- Deploy RSA Archer web, services, and database servers in the corporate network.

- Deploy data feed servers in the corporate network, except those that provide information using HTTPS, such as, RSS and Threat Intelligence services.

- Deploy a Web Application Firewall between the DMZ and Public network.

- Ensure that all RSA Archer servers in a site are connected to the same sub-network.

- Deploy firewalls at each site to ensure secure transfer of data from an instance of RSA Archer at one site to another instance of the RSA Archer located at a different site.

- Configure firewall rules to intercept all communication between RSA Archer components in the network, as shown in the preceding figure. For more information, see Firewall Rules.

While the previous figure shows multiple types of data feeds, the following figure expands on the Archer-to-Archer data feed type using the example of one geographic site to another.

When deploying RSA Archer in multiple geographically dispersed sites and configuring one instance of RSA Archer at one site to feed data to another instance of RSA Archer at another site, RSA recommends that you do the following:

- Configure firewall rules to intercept all communication between the RSA Archer components in the network and between different sites, as depicted by the firewalls in the preceding figure. For more information, see Firewall Rules.

- Implement data transfer between sites using a secure tunnel as shown in the preceding figure.

Firewall Rules

Use firewalls to restrict network traffic between RSA Archer and external systems. For graphical depictions of restricting network traffic, see Security Controls Map.

RSA strongly recommends that you configure firewall rules as described in the following sections. These recommendations are based on the following assumptions:

- You have a stateful firewall, indicating that only the establishment of TCP ports is considered.

- You specify the direction of communication for the UDP ports because the connections are sessionless.

- The firewall processes the rules top to bottom, finishing with a generic drop of all packets.

- You deploy RSA Archer as shown in one of the figures in Security Controls Map.

RSA recommends that you configure firewall rules to ensure secure communication for the following connections:

- DMZ to Corporate Network

- Corporate Network to Site Sub-Network

- Archer-to-Archer Data Feeds

DMZ to Corporate Network

RSA recommends that you do the following:

- Configure whitelist communication from the VPN server in the DMZ to the client machines on which the RSA Archer web user interface runs.

- Create firewall rules for all machines from which you intend to remotely access the corporate network through RDP.

Corporate Network to Site Sub-Network

For corporate network to site sub-network configurations, RSA recommends the following:

- Allow firewall access at each site only from designated RSA Archer client machines through a whitelisted IP address and port.

- Set firewall rules to drop all unless explicitly allowed.

Single-Host Configuration

RSA recommends that you secure the following default ports to ensure a secure communication between client machines running the RSA Archer web user interface and the RSA Archer web server:

- TCP 80

- TCP 443

The following table shows the firewall rules for a single host configuration.

Purpose	RULE | DIRECTION	Source IP Address --> Destination IP Address	Protocol	Port
Client Web Connectivity	ALLOW | INBOUND	ArcherWebUI_IPAddr --> ArcherWebServer_IPaddr	TCP	443
	ALLOW | OUTBOUND	ArcherWebServer_IPaddr --> ArcherWebUI_IPAddr	TCP	443
\<Default\>	BLOCK | INBOUND	All_* --> All_*	*	*
	BLOCK | OUTBOUND	All_* --> All_*	*	*

Multi-Host Configuration

RSA recommends that you secure the following default ports to ensure a secure communication between client machines running the RSA Archer web user interface and the RSA Archer web server:

- TCP 80
- TCP 443

The following table shows the firewall rules for a multi-host configuration that includes a reverse proxy/load balancer.

Purpose	RULE | DIRECTION	Source IP Address --> Destination IP Address	Protocol	Port
Client Web Connectivity	ALLOW | INBOUND	ArcherWebUI_IPAddr --> ArcherWebServer_IPaddr	TCP	443
	ALLOW | OUTBOUND	ArcherWebServer_IPaddr --> ArcherWebUI_IPAddr	TCP	443
RSS Feeds	ALLOW | INBOUND	RSSServer_IPAddr --> ArcherWebServer_IPaddr	TCP	443
	ALLOW | OUTBOUND	ArcherWebServer_IPaddr --> RSSServer_IPAddr	TCP	443

Purpose	RULE | DIRECTION	Source IP Address –> Destination IP Address	Protocol	Port
Threat Feeds	ALLOW | INBOUND	ThreatFeedServer_IPAddr –> ArcherWebServer_IPaddr	TCP	443
	ALLOW | OUTBOUND	ArcherWebServer_IPaddr –> ThreatFeedServer_IPAddr	TCP	443
<Default>	BLOCK | INBOUND	All_* –> All_*	*	*
	BLOCK | OUTBOUND	All_* –> All_*	*	*

Archer-to-Archer Data Feeds

RSA Archer might run in multiple sub-networks within your corporate network, where each sub-network is called a site. You can configure RSA Archer to allow the RSA Archer located in one site to feed data to the RSA Archer in another site. For more information, see Archer-to-Archer Data Feeds.

For this scenario, RSA recommends that you do the following:

- Ensure that the firewall at each end of the data transfer allows communication only through a whitelisted IP address and port.

- Secure the following default ports to ensure a secure communication between two RSA Archer instances located in different sites:

  - TCP 80

  - TCP 443

The following table shows you how to configure the site's firewall rules.

Purpose	RULE | DIRECTION	Source IP Address –> Destination IP Address	Protocol	Port
Archer Data Feed	ALLOW | INBOUND	ArcherDataFeed_IPAddr –> ArcherWebServer_IPaddr	TCP	443

Purpose	RULE | DIRECTION	Source IP Address –> Destination IP Address	Protocol	Port
<Default>	BLOCK | INBOUND	All_* –> All_*	*	*
	BLOCK | OUTBOUND	All_* –> All_*	*	*

Secure Deployment Settings

The following table shows the security controls that RSA recommends to be in place for securing the deployment of RSA Archer.

Deployment Settings	Secure Deployment Setting	Pros of Secure Deployment Setting	Cons of Secure Deployment Setting	Instructions on How to Configure Secure Deployment Setting
HTTPS is enabled on a new 6.x installation, by default, between client and server. Remove any existing HTTP bindings (port 80) via IIS Manager.	For best possible security between client and server, enable HTTPS and disable HTTP in Microsoft IIS.	Provides a high level of protection for the communication between client and server by avoiding tampering, spoofing, and man-in-the-middle type of attacks.	Could impact performance.	See "Web Server Communication" in the RSA Archer Online Documentation.

Deployment Settings	Secure Deployment Setting	Pros of Secure Deployment Setting	Cons of Secure Deployment Setting	Instructions on How to Configure Secure Deployment Setting
Database Encrypted Communication	Encrypting the communication between the RSA Archer Web Server and the Instance Database increases security.	Provides increased security by implementing secure communication between the Web Server and Instance Database.	Could impact performance.	See "Maintaining Security" in the RSA Archer Online Documentation.
Persistent Session Cookie Configuration	Deleting the cookie holding the session token when the client is closed increases security.	Provides increased security by requiring reauthentication after logout or browser close.	User has to reauthenticate.	See "Enabling Storing the Session Token in a Persistent Cookie" in the RSA Archer Control Panel Help.
Windows Server Security Configuration	Hardening the web server based on industry best practices reduces the likelihood of vulnerabilities.	Provides improved security and reduced risk for the servers deployed for RSA Archer.	Could cause some unsecured Windows Server features to become unavailable.	Follow Microsoft security configuration recommendations for the applicable IIS version.

Deployment Settings	Secure Deployment Setting	Pros of Secure Deployment Setting	Cons of Secure Deployment Setting	Instructions on How to Configure Secure Deployment Setting
SQL Server Security Configuration	Hardening the SQL Server installation hosted on the database server based on industry best practices reduces the likelihood of vulnerabilities on the servers.	Provides improved security and reduced risk for the database server deployed for the Platform installation.	Could cause some unsecured SQL Server features to become unavailable.	Follow Microsoft security configuration recommendations for the applicable SQL server version.

Web Server Security Configuration

For recommendations on IIS security configuration, see the Microsoft Knowledge Base.

In addition to Microsoft's recommendation, RSA recommends that you configure Microsoft IIS to do the following:

- Enable SSL communications. See See "Web Server Communication" in the RSA Archer Online Documentation.
- Disallow arbitrary file extensions.
- Remove IIS and ASP.NET Version Information from HTTP Headers.

Disallow IIS Arbitrary File Extensions

Request Filtering is a built-in security feature in Internet Information Services (IIS). The settings for this feature are located within the <requestFiltering> element and contains a child element for <fileExtensions>. This element can contain a collection of file name extensions that IIS either denies or allows. For example, you can block all requests for Web.config files.

For more information, visit the Microsoft Web pages File Name Extensions at https://docs.microsoft.com/en-us/iis/configuration/system.webServer/security/requestFiltering/fileextensions/index and Request Filtering at https://docs.microsoft.com/en-us/iis/configuration/system.webServer/security/requestFiltering/.

When using the IIS <fileExtensions> element, do not prevent the uploading of files with the following IIS file extensions, as this will cause RSA Archer to malfunction.

- .ASAX
- .ASCX
- .ASHX
- .ASMX
- .ASP
- .ASPX
- .AXD
- .BAT
- .BMP
- .CAB
- .CONFIG
- .CSHTML
- .CSS
- .DAT
- .DLL
- .EJS
- .EOT
- .FPJ
- .GIF
- .HTC
- .HTM
- .HTML
- .ICO
- .JPG
- .JS
- .MASTER
- .MCWEBHELP
- .PNG
- .SETTINGS
- .SVC
- .TDF
- .TTF
- .TXT
- .WOFF
- .XAP
- .XML
- .ZIP

Disallow Arbitrary File Uploads

RSA Archer allows users to upload files with any type of extension. RSA recommends training your users on good security practices including not uploading any file from sources other than themselves to prevent introducing potentially malicious files to the RSA Archer Platform. To tighten security, you can prevent users from uploading files with specific extensions. For more information, see "File Creation Restriction" in the RSA Archer Online Documentation.

Prevent certain file types, depending on what your users do with RSA Archer, For example, prevent the upload of executable .exe files to RSA Archer. However, if your users investigate security incidents, you want to allow the upload of executable files containing viruses and other potential malware for use in investigations.

The following table provides a list of file extensions used by normal RSA Archer operations. Do not prevent uploads of files with these extensions.

- .AI
- .BMP
- .CSS
- .CSV
- .GIF
- .ICO
- .JPEG
- .JPG
- .PPS
- .PPSM
- .PPSX
- .PPT
- .WMF
- .XLA
- .XLAM
- .XLS

- .DOC
- .DOCM
- .DOCX
- .DOT
- .DOTM
- .EMF
- .EPS
- .EXIF

- .PDF
- .PNG
- .POT
- .POTM
- .POTX
- .PPA
- .PPAM

- .PPTM
- .PPTX
- .PS
- .RTF
- .TIF
- .TIFF
- .TXT

- .XLSB
- .XLSM
- .XLSX
- .XLT
- .XLTM
- .XLTX
- .XML

Remove IIS and ASP.NET Version Information from HTTP Headers

To make it more difficult for attackers to identify vulnerabilities in the software that is powering the Web Server, do not disclose the types of applications and their respective version numbers in HTTP headers. While certain HTTP headers are necessary, the HTTP headers that identify the Web Server are not necessary, including the following:

- Server: Microsoft-IIS/<version_ number>
- X-Powered-By: ASP.NET
- X-AspNet-Version: <version_ number>

AspNet-Version HTTP Header

RSA recommends that you do the following:

- Remove the HTTP headers that identify the web server.
- Ensure that <httpRuntime enableVersionHeader="false"/> is set in the RSA Archer web.config file, located at:
  - IIS\DefaultWebSite\RSAArcher\web.config
  - IIS\DefaultWebSite\RSAArcher\api\web.config

Remove X-Powered-By HTTP Header

1. Launch the Microsoft IIS Manager.
2. Expand the Sites folder.
3. In the IIS grouping, select the website that you want to modify, and double-click the HTTP Response Headers section.

4. If "X-Powered-By: ASP.NET" is displayed in the Custom Header listbox, click the Remove link in the right-hand column.

Note: To ensure that the server header is not automatically added to the outgoing HTTP response by Microsoft IIS, use Microsoft's free UrlScan utility.

IP Whitelist

The IP Whitelist allows for the ability to define a range of IP addresses that can access RSA Archer. The IP Whitelist restricts incoming connections only, and should include the following items:

- Web Application servers
- Services servers
- Client machines accessing the Web Application

Optionally, the following items can also be included:

- Data Feed source servers
- LDAP servers

RSA recommends implementing the IP Whitelist to limit the availability of the Platform as a potential attack vector.

Host Hardening

To ensure secure operation of RSA Archer, the underlying components of the host must be hardened so that the server will function properly and opportunities for vulnerabilities are removed.

RSA Archer recommends hardening the host system under it to only allow TLS 1.2 on all RSA Archer supported clients and servers.

- Make sure that SQL servers, Web Services, and clients have the latest service packs using TLS 1.2.
- Make sure that all security updates are applied before additional hardening is performed on all underlying components, including, but not limited to, the Operating System, SQL, and IIS.

Recommendations for TLS/SSL cipher hardening

Once all underlying components are up-to-date, TLS/SSL cipher hardening can be applied. A cipher suite is a set of algorithms that help secure a network connection using Transport Layer Security (TLS). Cipher hardening will prevent known cipher attacks in TLS/SSL (for example, Sweet32, BEAST, POODLE).

Disabling SSL 2.0 and SSL 3.0

Due to the issues presented in SSL 2.0, the protocol is deemed unsafe to use and should be completely disabled. Similarly, the POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability causes SSL 3.0 to be unsafe for use and should be disabled.

Disabling TLS 1.0 and 1.1

Unless there is a need to support legacy browsers, TLS 1.0 and 1.1 should also be disabled.

Disabling weak ciphers

Web server communication over HTTP relies on the SSL/TLS ciphers and key lengths provided by the version of IIS on which RSA Archer is installed. Ensure that IIS is configured for cryptographic support, which cannot be easily defeated. RSA recommends that you configure Microsoft IIS to only allow ciphers with key lengths of 128 bits or greater.

Weak ciphers, such as DES and RC4, should be disabled.

Cipher configuration

A chosen Cipher Suite is unique to the security guidelines set forth by a user's organization. It is usually based on the level of restrictions required in the server environment, as well as the age of the software and devices connecting to the servers (for example, the need to support legacy browsers and regulatory requirements).

Users should implement a Security Best Practices cipher suite with Triple DES168 Cipher excluded (from SChannel) on RSA Archer Servers including the web. RSA recommends that you place the most secure cipher suites first because servers often select the first supported suite from the client's list.

As guidance, RSA Archer has been tested with, as limited as, the following list of Cipher Suites and the product remains functional:

Hexcode	Cipher Suite Name (OpenSSL)	KeyExchange	Encryption	Bits	Cipher Suite Name (RFC)
xc028	ECDHE-RSA-AES256-SHA384	ECDH 521	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014	ECDHE-RSA-AES256-SHA	ECDH 521	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Hexcode	Cipher Suite Name (OpenSSL)	KeyExchange	Encryption	Bits	Cipher Suite Name (RFC)
x9d	AES256-GCM-SHA384	RSA	AESGCM	256	TLS_RSA_WITH_AES_256_GCM_SHA384
x3d	AES256-SHA256	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA256
x35	AES256-SHA	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA
xc027	ECDHE-RSA-AES128-SHA256	ECDH 521	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013	ECDHE-RSA-AES128-SHA	ECDH 521	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9c	AES128-GCM-SHA256	RSA	AESGCM	128	TLS_RSA_WITH_AES_128_GCM_SHA256
x3c	AES128-SHA256	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA256
x2f	AES128-SHA	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA

Verify cipher configuration

You can use various tools to verify the Cipher Suite hardening that you have enabled. Cipher Suite hardening may lead to limited connectivity; old clients cannot connect to servers with strong security requirements. Some of the tools will provide the details on these limitations.

Special cipher vulnerability cases

- **BREACH (CVE-2013-3587)** - This cipher vulnerability is related to web server HTTPS Compression and can be handled via Web Server / Load Balancer Configuration.

- **LUCKY13 (CVE-2013-0169)** - This cipher vulnerability is a timing attack used against implementations of the TLS protocol using the Cipher Block Chaining (CBC) Ciphers. To prevent this vulnerability, make sure that you do not use cipher suites in the CBC mode.

Physical Security Controls Recommendations

Physical security controls are designed to protect resources against unauthorized physical access and physical tampering. RSA recommends that the physical servers for RSA Archer be deployed in a secure data center leveraging the organization's best practices for physically securing a data center, server rack, and server.

Chapter 3: Maintaining Security

Security Patch Management

Security patches are released on an as-needed basis.

All security patches for RSA Archer originate as RSA and are available for download as an update, as long as you have a current maintenance agreement in place with RSA. Updates are available from RSA SecurCare Online. Product documentation is posted on the RSA Archer Community on RSA Link. RSA recommends you register your product and sign up for the RSA Archer Community on RSA Link.

Note: It is recommended to run the latest security patches for any software that you are using with RSA Archer from the Qualified and Supported Environments Guide.

The following table lists the third-party components for which patches are needed.

Third-Party Component for which Patch Is Needed	Frequency of Patch	EMC Responsibility (Yes or No)	Customer Responsibility (Yes or No)	Reference to Instructions for Applying Patch
Windows Server 2012 R2 & 2016	Determined by vendor.	No	Yes	Based on vendor recommendations.
SQL Server 2014 & 2016	Determined by vendor.	No	Yes	Based on vendor recommendations.
Microsoft IIS	Determined by vendor.	No	Yes	Based on vendor recommendations.
.NET Framework	Determined by vendor.	No	Yes	Based on vendor recommendations.

Malware Detection

RSA recommends that you deploy a malware detection solution on the web and database servers. The malware detection solution should be based on your standard tools and best practices. It is your responsibility to deploy patches and updates for the malware detection tools.

Virus Scanning

RSA recommends that you run virus scanning software on the deployed servers on a routine basis. If you are running Threat or Vulnerability feeds, RSA strongly recommends that you disable virus scanning for the folder in which the Threat or Vulnerability data files are temporarily stored. A virus scanning engine could interpret the data as a virus or malware.

For information on configuring the folder, see Threat Data Feeds.

Ongoing Monitoring and Auditing

As with any critical infrastructure component, RSA recommends that you constantly monitor your system and perform periodic and random audits, for example, configuration, permissions, and security logs. Ensure that the configurations and user access settings match your company policies and needs.

Chapter 4: FIPS Compliant Mode

The Federal Information Processing Standard (FIPS) is a United States and Canadian government standard that is intended to ensure secure data communications among compliant systems. FIPS 140-2 specifies the Security Requirements for Cryptographic Modules, including the approved encryption algorithms and hashing algorithms and the methods for generation and management of encryption keys. To qualify as FIPS compliant, RSA Archer must be configured and operated in accordance with FIPS 140-2 requirements, using FIPS-certified components and algorithms in all required instances.

Platform Release Supporting FIPS

RSA Archer 6.0 and later can be configured for FIPS compliance.

FIPS-Compliant Operation Requirements

You can configure FIPS compliance on any Windows system that supports RSA Archer, including Windows Server 2012 R2 and 2016.

Note: This requirement applies to all RSA Archer components.

You must configure web browsers for FIPS operation. See Configure Browser for FIPS Compliance.

FIPS Certificates

Cryptographic modules that are FIPS 140-2 certified have undergone testing and verification by a government-approved evaluation laboratory. You can obtain the required FIPS certificates from the National Institute of Standards and Technology (NIST) website at:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

For a list of certificates applicable to RSA Archer, see Platform FIPS Certification.

Set Up FIPS for Windows

Use the Local Security Policy tool to perform the FIPS setup for Microsoft Windows.

Procedure

1. Log on to Windows as a Windows system administrator.
2. Click Start > Control Panel.
3. In the Control Panel window, click Administrative Tools.

4. In the Administrative Tools window, click Local Security Policy.

5. In the Local Security Policy window, in the navigation pane, click Local Policies > Security Options.

6. In the Policy pane, double-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

7. On the Local Security Setting tab, click Enabled.

8. Click Apply.

9. Click OK.

10. Close the Local Security Policy window.

SQL Server FIPS Setup

All versions of SQL Server that support RSA Archer are configurable for FIPS compliance. For instructions on setting up FIPS on SQL Server, see the Microsoft SQL Server documentation.

Note: SQL Server 2014 or SQL Server 2016 must be installed on a Windows Server 2012 R2-based server. The Windows server must be FIPS enabled prior to starting SQL Server.

For dialog security between services, the encryption uses the FIPS-certified instance of AES if the FIPS mode is enabled. If the FIPS mode is disabled, the encryption uses RC4. When a Service Broker endpoint in the FIPS mode is configured, the administrator must specify AES for the Service Broker. If the endpoint is configured to RC4, the SQL Server generates an error, and the transport layer does not start.

Messages in two logs verify that the SQL Server is running in FIPS mode:

* When the SQL Server service detects that FIPS mode is enabled at startup, it logs this message in the SQL Server error log:
   Service Broker transport is running in FIPS compliance mode.

* This message is logged in the Windows Event log:
   Database Mirroring transport is running in FIPS compliance mode.

Configure Browser for FIPS Compliance

In addition to FIPS enablement on the host system, you must configure any web browser used to connect to the RSA Archer for FIPS compliance. For more information, see Set up FIPS for Windows

When using supported versions of Microsoft Internet Explorer with the Platform in FIPS mode, enable TLS 1.2 or higher in the browser. For more information, see the RSA Archer Qualified and Supported Environments Guide.

1. Open Internet Explorer.

2. Click Tools, and then click Internet Options.

3. On the Advanced tools tab, select Use TLS 1.2.

4. Verify that both Use SSL 2.0 and Use SSL 3.0 options are cleared.

LDAP Configuration for FIPS Mode

Note: RSA assumes that you use Microsoft Active Directory as the LDAP server. For other types of LDAP servers, see their product-specific documentation.

Connections to Active Directory from RSA Archer can be unencrypted or encrypted. If you intend to encrypt connections, you must configure Active Directory with a server certificate. You can achieve this with a server certificate on the Windows server, which installs the server certificate, using auto enrollment on Active Directory.

To configure Active Directory in FIPS mode, the Windows server hosting Active Directory must be FIPS enabled. For more information, see Set Up FIPS for Windows.

Platform FIPS Certification

The following tables list the FIPS certificates for the cryptographic components that RSA Archer uses.

Secure Hash Algorithm (SHA) Standard (FIPS 180-3)

Algorithm	Operating System	Certificate Number
SHA-108-3	Windows Server 2012 R2	2373
	Windows Server 2016	3347

Advanced Encryption Standard (AES) Algorithm (FIPS 197)

Algorithm	Operating System	Certificate Number
AES-197	Windows Server 2012 R2	2832
	Windows Server 2016	4064

Enable FIPS Window Server Configuration for 140-2 on the Web and Services Server

1. Enable FIPS mode on the web server.

   a. Go to Administrative Tools.

   b. In Administrative Tools, select Local Security Policy.

   c. Expand Local Policies, and select Security Options.

   d. Double-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

   e. Select Enable.

2. Download and install the JCE Unlimited Jurisdiction Policy files.

   a. Go to http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html and follow the steps provided to download the JCE Unlimited Jurisdiction Policy files.

   b. Extract and open the ZIP file.

   c. Edit the jar file names by adding the extension .org to the end of the files so that they are not overwritten later.

   d. Paste the renamed files in %SystemDrive%\Program Files\Java\<java_version_directory>\lib\security.

3. In the %SystemDrive%\Program Files\Java*java_version_directory*\lib\security directory, edit the java.security file by doing one of the following:

   - Add the line com.rsa.cryptoj.fips140initialmode=FIPS140_MODE..

   - Change the line com.rsa.cryptoj.fips140initialmode=NON_FIPS140_MODE to com.rsa.cryptoj.fips140initialmode=FIPS140_MODE.

Appendix A: Authentication Methods

User authentication settings control the process of verifying an identity claimed by a user for accessing RSA Archer.

A new installation of RSA Archer is secure by Default (HTTPS protocol enabled) with anonymous authentication. For versions of RSA Archer upgraded from prior to 6.x, installation has a default anonymous HTTP authentication configuration. RSA Archer has a default anonymous authentication configuration that simplifies the installation process and prevents problems during installation. Anonymous authentication is sufficient for most environments. For those environments where it is not sufficient, more sophisticated authentication methods are necessary. Configuring authentication methods requires changes to multiple server-side components, some of which are outside the scope of RSA Archer.

Important: Before making any of the authentication configuration changes below, be sure to back up the RSA Archer web.config file, the Configuration database, and the IIS settings.

Note: An incorrectly configured authentication method can prevent the entire RSA Archer from being accessible.

The following are supported protocol methods.

HTTPS/SSL protocol

The certificate for SSL must be available in the Server Certificates component (Machine Name > Server Certificates) within IIS. When the certificate is available, an https Binding which uses the SSL certificate must be added for the RSA web site.

Use the following tasks to configure IIS, the web.config files, and the RSA Archer Control Panel for HTTPS/SSL.

Note: If you need to restore HTTP after configuring for HTTPS/SSL protocol, implement the process by undoing all the HTTPS/SSL steps.

Configure IIS for HTTPS/SSL protocol

1. Select the Platform web site in the Connections pane.
2. In the Actions pane, click Bindings.
3. Click Add.
4. In the Type list, select the https option.
5. In the SSL certification list, select the applicable certificate.
6. Click OK.

7. Do one of the following:

    - To continue without removing the HTTP Site Binding, go to the next step.

    - To remove the HTTP Site Binding, do the following:

        a. Select the HTTP Site Binding.

        b. Click Remove.

        c. Click Yes.

8. Click Close.

9. Perform an IIS reset.

Configure Platform web.config file for HTTPS/SSL protocol

RSA Archer must be configured to run either in HTTP or HTTPS, not both. Edit the RSA Archer web.config in the base RSA Archer web site directory.

1. Find the expression <!-- for HTTPS, and then do each of the following:

    - Replace httpGetEnabled with httpsGetEnabled="false".

    - Uncomment the line <security mode="Transport" />.

    - Replace the httpTransport attribute with httpsTransport.

2. Find the expression <customHeaders>, and then add each of the following configurations in a separate new line within the custom headers section:

    - <add name="Strict-Transport-Security" value="max-age=31536000; includeSubDomains" />

    - <add name="X-Content-Security-Policy" value="default-src 'self';" />

    - <add name="X-XSS-Protection" value="1; mode=block"/>

3. Click Save.

4. Perform an IIS reset.

Configure REST API web.config file for HTTPS/SSL protocol

The REST API child API IIS application inherits properties from the parent RSA Archer application. Similar to the Platform web.config, RSA Archer must be configured to run either in HTTP or HTTPS, not both. Edit the REST API web.config in the api directory within the base RSA Archer web site directory.

1. Find the expression <!-- for HTTPS.

2. Replace httpGetEnabled with httpsGetEnabled="false".

3. Uncomment the line <security mode="Transport" />.

4. Replace the httpTransport attribute with httpsTransport.

5. Click Save.

6. Perfor's m an IIS reset.

Configure RSA Archer Control Panel for HTTPS/SSL

All URLs in the RSA Archer Control Panel must include HTTPS.

1. Open the RSA Archer Control Panel.

2. In Instance Management, double-click the instance you want to configure.

3. Click the Web tab.

4. Change all applicable Platform Web site URLs to include HTTPS.

5. Repeat steps 2 – 4 for all other instances.

6. Click Save All.

Windows Authentication

The authentication mode must be set to Windows Authentication in IIS. All other authentication modes must be disabled.

Note: If Windows Authentication is not available for selection, it must be installed. Do not enable Extended Protection because Microsoft Silverlight does not support it.

Important: The REST API does not support Windows Authentication. Windows Authentication must be disabled for the child API IIS application, and Anonymous Authentication enabled again.

Use the following tasks to configure IIS and the web.config file for Windows HTTP or HTTPS protocols.

Configure IIS for Windows Authentication

1. Select the Platform Web site in the Connections pane.

2. Select the Authentication feature.

3. Set Windows Authentication to Enabled.

4. Disable all other authentication modes, for example, Anonymous.

5. Perform an IIS reset.

Configure Platform web.config file for Windows Authentication - HTTP

Edit the RSA Archer web.config file in the base RSA Archer web site directory.

1. Find the expression <!-- For Windows Authentication, change mode to 'Windows'.

2. Replace <authentication mode="None" /> with <authentication mode="Windows" />.

3. Find the expression <!-- For Windows Authentication, and uncomment the lines.

4. Uncomment the lines related to <authorization><allow users="*" /></authorization>.

5. Find the expression <!-- For Basic Authentication (without SSL), and uncomment the lines.

6. Uncomment the lines related to security mode.

7. Find the expression <!-- for Windows Integrated Authentication, and add authenticationScheme="Negotiate".

8. As instructed, add authenticationScheme="Negotiate" /> to httpTransport or httpsTransport.

9. Click Save.

10. Perform an IIS reset.

Configure Platform web.config file for Windows Authentication - HTTPS

Edit the RSA Archer web.config in the base RSA Archer web site directory.

1. Open the web.config file in a text editor.

2. Locate the <authentication mode> tag and change the authentication mode from None to Windows.

3. Locate the <authorization> and <allow users> tags and remove the comments.

4. Locate the <serviceMetaData> tab and change the HTTP identifier to HTTPS.

5. Locate the <webHttpBinding> section.

6. Remove the comments in the <security mode> and <transport> tabs identified for Windows Authentication and change the security mode as follows:

   <security mode="Transport">

   <transport clientCredentialType="Windows" />

   </security>

7. Locate the <httpTransport> tag for the binaryHttpBinding.

8. Add the authenticationScheme="Negotiate" attribute to the tag and the HTTPS identifier.

   <httpTransport maxReceivedMessageSize="1024000000" maxBufferSize="1024000000" authenticationScheme="Negotiate" />

9. Locate the <httpTransport> tag for the binaryHttpBindingStreaming binding.

10. Add the authenticationScheme="Negotiate" attribute to the tag and the HTTPS identifier.

    <httpsTransport transferMode="StreamedRequest"
    maxReceivedMessageSize="1024000000" maxbufferSize="1024000000"
    authenticationScheme="Negotiate" />

11. Locate the <location> tag and remove the comments.

12. Save the web.config file

13. Perform an IIS reset.

Single Sign-on for Windows integrated authentication

Use the following tasks to configure Single Sign-On for Windows integrated authentication.

Configure Platform web.config file for Single Sign-On

Edit the RSA Archer web.config file in the base RSA Archer web site directory.

1. Find the expression </configuration>.

2. On a preceding blank line, insert <location
   path="default.aspx"><system.web><authorization><deny
   users="?"/></authorization></system.web></location>.

3. Click Save.

4. Perform an IIS reset.

Configure RSA Archer Control Panel for Single Sign-On - Single Instance

1. Open the RSA Archer Control Panel.

2. In Instance Management, double-click the instance you want to configure.

3. Click the Single Sign-On tab.

4. Select Windows Integrated as the single sign-on mode.

5. Click the Installation Settings tab.

6. Select the Default Instance box.

7. Click the arrow in the Instance list, and then select the instance.

8. Click Save All.

Configure RSA Archer Control Panel for Single Sign-On - Multiple Instances

1. Open the RSA Archer Control Panel.

2. In Instance Management, double-click the instance you want to configure.

3. Click the Single Sign-On tab.

4. Select Windows Integrated as the single sign-on mode.

5. Click the Web tab.

6. Enter a unique Instance URL.

   Note: If a matching DNS entry does not exist for the Instance URL, it does not resolve.

7. Click Save.

Enabling Kerberos Authentication

Use the following tasks to configure Windows authentication for single and multiple web hosts.

Configure Windows Authentication for Single Host

If it does not already exist, an HTTP service principal name (SPN) must first be registered with the domain by a domain administrator. The following is the command to do so:

Setspn -S HTTP/{ArcherURL} {App Pool Identity}

For example, Setspn -S HTTP/all.archer.local archer.local\Administrator is the command to inject a SPN add into the domain if the following were true:

- Archer is installed into Default Web Site.

- Archer URL is https://all.archer.local

- Archer Application Pool identity is: archer.local\Administrator

If Archer is installed into the RSAArcher site—located inside of Default Web Site—the command to inject is Setspn -S HTTP/all.archer.local archer.local\Administrator.

1. Open Microsoft IIS.

2. Select the Archer site (default or otherwise).

3. Select Authentication.

4. Enable Windows Authentication.

5. Select Advanced Settings.

6. Unselect Enable Kernel-mode authentication and click OK.

7. Select Providers.

8. Select Negotiate: Kerberos from the Available Providers drop-down.

9. Click Add.

10. Move Negotiate Kerberos to the desired order under Enabled Providers and click OK.

    Ensure that these steps have been completed for at least the RSA Archer site. These steps may also need to be performed to the Default Web Site and Server level components in IIS depending on your own needs.

11. Perform an IIS reset.

Configure Windows Authentication for Multiple Web Hosts in Load-Balanced Environment

When IIS is run in clustered or load-balanced environments, applications are accessed using the cluster name rather than a node name. This scenario includes network load balancing. In cluster technology, a node refers to one computer that is a member of the cluster.

To use Kerberos as the authentication protocol, the application pool identity on each IIS node must be configured to use the same domain user account. To configure each IIS node to use the same domain user account, use the following command:

Setspn –A HTTP/CLUSTER_NAME domain\username

For example, the command may resemble the following:

Setspn –A HTTP/www.myIISCluster.com mydomain\appPool1

1. Open Microsoft IIS.

2. Select the Archer site (default or otherwise).

3. Select Authentication.

4. Enable Windows Authentication.

5. Select Advanced Settings.

6. Unselect Enable Kernel-mode authentication and click OK.

7. Select Providers.

8. Select Negotiate: Kerberos from the Available Providers drop-down.

9. Click Add.

10. Move Negotiate Kerberos to the desired order under Enabled Providers and click OK.

Ensure that these steps have been completed for at least the RSA Archer site. These steps may also need to be performed to the Default Web Site and Server level components in IIS depending on your own needs.

11. Perform an IIS reset.