RSA ARCHER® SUITE

Platform Installation and Upgrade Guide

6.7

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.

October 2019

Contents

Preface

About This Guide

This guide provides RSA Archer® Suite administrators with instructions for installing and upgrading RSA Archer. This guide assumes the reader has knowledge of Microsoft Internet Information Services (IIS)®, Microsoft SQL Server®, Windows Servers®, ScaleOut StateServer®, Redis™,and also has the appropriate permissions to the infrastructure.

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 GRC as a practice, and includes product demos, GRC 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. link_gt_exchange (snippet) https://community.rsa.com/community/products/archer-grc/exchange

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.

Document	Description
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.
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.

Chapter 1: Components and System Requirements

This chapter introduces the main components of RSA Archer installation, the types of available configurations, and the requirements for running your environment.

RSA Archer Components

There are several main components to an RSA Archer installation.

- Web Application
- Instance Database
- File Repository
- Configuration Database
- Services

Web Application

The RSA Archer Platform uses a web-based user interface that runs on a Web Server. Manage the Web Application through an Application Pool using Microsoft® Internet Information Services (IIS).

Microsoft Internet Information Service (IIS), Microsoft .NET Framework 4.7.2 is required for the application. For additional information, see System Requirements. The application is managed through an Application Pool through the Internet Information Services (IIS). For additional information, see Application Pool Requirements.

Instance Database

An RSA Archer instance is a single setup that includes unique content in a database, the connection to the database, the interface, and user credentials. For example, individual instances for each office location or region, or for development, test, and production environments.

The Instance Database stores the RSA Archer content for a specific instance. You might have individual instances for each office location or region or for development, test, and production environments.

File Repository

The File Repository serves many purposes for your RSA Archer configuration. For example, the File Repository provides storage for the following services:

- Attachments uploaded as content
- Temporary files, such as packages, exports
- Data feeds
- Charts created by reports and searches

Configuration Database

RSA Archer uses the Configuration Database to store data that is not instance specific; for example, client information and application information (including date and version).

Services

There are several services, listed with Microsoft Windows Services, that control various functions of RSA Archer. They control features such as configuration data, job engine, and advanced workflow.

The following table describes the RSA Archer services.

Service	Description
RSA Archer Configuration	Connects to the Configuration Database, where configuration parameters of the Platform and RSA Archer services are stored. **Note:** This service must be installed and enabled on all web and Services Servers.
RSA Archer Instrumentation	Supports message logging through Event Tracing for Windows (ETW) to a database. For more information, see Message Logging. **Note:** This service only needs to be active if you are using ETW.

Service	Description
RSA Archer LDAP Synchronization	Supports user and group maintenance by synchronizing the users and groups in RSA Archer to users and groups in another system through Lightweight Directory Access Protocol (LDAP). **Note:** This service only needs to be active if you are using LDAP to manage user accounts.
RSA Archer Job Engine	Administers all asynchronous job processing for RSA Archer data feeds, findings generation, notifications, recalculations, and system jobs. For a complete listing of processing and system jobs, see "Job Types" in the RSA Archer Control Panel Help. **Note:** This service is required to be installed for RSA Archer to run.
RSA Archer Queuing	Builds and maintains indexes for keyword search and file attachments. You can only have one RSA Archer Queuing service enabled for an RSA Archer instance. **Note:** This service is required on the Services Server assigned to queuing.
RSA Archer Advanced Workflow	Administers the Advanced Workflow feature for processing workflows. This service is an integral part of RSA Archer and should be running all the time. For solutions use cases in which the Advanced Workflow feature is available, workflow does not function unless the RSA Archer Advanced Workflow service is running. **Note:** As of version 6.1, the Advanced Workflow service can be installed on a Web Server or Services Server specified during installation. A example configuration dedicates Advanced Workflow service to two Web Servers behind a load balancer.

RSA Archer Configurations

RSA Archer can be structured in various configurations, depending upon your unique needs.

RSA recommends that you choose a configuration that is easily adaptable and scalable to the growing demands of your business. When determining which configuration is best for you, consider the expected user load, utilization, and availability requirements for your business operations. For additional information about optimizing performance, see the *RSA Archer Planning Guide*.

Recommended Configuration

For optimal scalability and performance, RSA recommends a multiple server configuration for RSA Archer. This configuration includes dedicated servers for hosting the Web Application and the services. Each server plays a specific role within the RSA Archer configuration.

Database	Description
Instance	The primary database for storing RSA Archer content. The Content Database is synonymous with Instance Database.
Configuration	A central repository for configuration information for the Web Application and Services Servers. This database facilitates the installation and maintenance of multiple application servers in a multiple server deployment.
(Optional) Message Logging	RSA Archer logs Event Tracing for Windows (ETW) trace events and writes log messages to a specified database. RSA recommends that you create a dedicated database for message or any other event logging; do not use the Instance Database or the Configuration Database.

Test Environment Configuration

The test environment configuration consists of a single server that hosts the Web Application and services. This configuration is recommended for test environments only. Other resources can be installed on additional servers. For instructions on how to set up this environment, see the Appendix B: Test Environment.

Configuration Considerations

A recommended RSA Archer configuration meets the needs of current processing with room for future growth. It provides greater flexibility and is highly scalable because each layer can be scaled independently. The Web Application, services, and content reside in different databases on separate servers. This type of configuration also supports high-availability environments that use load balancing to distribute loads based on server availability. Incoming HTTP requests are directed across the Web Servers using a load balancer, which distributes loads based on server availability according to the selected criteria.

For enhanced security, the recommended configuration can incorporate a double firewall. This configuration places a firewall in front of the Web Server with another residing between the web and database servers.

For enhanced reliability, incorporate caching into your configuration by having multiple servers running simultaneously. To enable third-party caching, follow the recommendations from the caching provider. Caching is often installed one more than one server to ensure that if the main server goes down, the traffic shifts to the another running server. These servers run the Cache Services only.

Recommended Configuration

Each server plays a role and runs GRC components specific to that role. The following table shows the recommended configuration.

Services Server	Web Server	File Server	Database Server
RSA Archer Configuration Service	Web Application	File Repository	Instance Databases
RSA Archer Job Engine Service	RSA Archer Configuration Service		Configuration Database
Other Services	RSA Archer Workflow Service		

Recommended Configuration with Caching

You can configure RSA Archer to meet specific needs, like caching. In this case, your configuration might look similar to the following table:

Cache Servers	Services Server	Web Server	File Server	Database Server
Third-party caching application	RSA Archer Job Engine Service	RSA Archer Configuration Service		Configuration Database
	(Optional) ScaleOut StateServer Client	(Optional) ScaleOut StateServer Client		
	(Optional) Redis **Note:** Client installation is not necessary.	(Optional) Redis **Note:** Client installation is not necessary.		
	Other Services	RSA Archer Workflow Service		

System Requirements

The recommended system requirements vary based on the number of concurrent users and the amount of data stored in RSA Archer. RSA recommends using a server configuration that supports moderate transaction levels. For a complete list of system performance requirements and characteristics, see the *RSA Archer Platform Planning Guide*.

Recommended Configuration Requirements

RSA recommends the latest qualified versions of specific software for running RSA Archer in the recommended configuration. For more information, see "RSA Archer Qualified and Supported Environments" on RSA Link at: https://community.rsa.com/docs/DOC-102657.

License Keys

License keys are required for certain situations.

Process	License details
Install a new instance	Contact your RSA Archer account representative.
Upgrade from 5.x or 6.0	Contact your RSA Archer account representative and see the RSA Link article "RSA Archer 6.1 Upgrade Process".
Upgrade from 6.1 or later	No action needed.

Important: When upgrading, do not apply the new license key until after you upgrade the Platform. If you apply the license first before upgrading, you may lose access to legacy core applications that are no longer supported in the out-of-the-box use cases.

License Agreement - Instance Creation

With the purchase of each RSA Archer license, you receive permission to create a single environment for one production instance and two non-production instances.

Cloud and Hosting Support

RSA Archer supports hosting in Microsoft Azure® and Amazon Web Services® (AWS) cloud environments. This section provides information to assess and plan for an installation using cloud environments.

When using Cloud vendors, RSA only supports using virtual machines to run your RSA Archer environment.

Use the same process for a cloud or hosted environment as outlined in the *RSA Archer Platform Planning Guide* to determine your environment size. Choose a product from your cloud provider that most closely matches your configuration requirements.

For example, consider the specifications for a small environment given in *RSA Archer Platform Planning Guide*. As of this publication, the details in this table are accurate based on current vendor specifications.

Element	Small Environment	AWS (m4.xlarge)	Azure (Standard_ DS3 package)
Processor	Four cores	Four cores	Four cores
Memory	16 GB	16 GB	14 GB

Element	Small Environment	AWS (m4.xlarge)	Azure (Standard_ DS3 package)
Disk Space	50 GB HDD	100 GB SSD (Using Elastic Block Store)	100 GB HDD

Note: This table describes hardware requirements only. To understand all requirements for your configuration, see "Sizing Guidelines" in the *RSA Archer Platform Planning Guide*.

There are some factors to consider when preparing your cloud based configuration:

- Input/Output per second (IOPS) directly affects your RSA Archer performance. If you find your performance is slow, consider choosing a vendor product with more IOPS per disk.
- Communication between your on-premises systems and your cloud vendor is key. Contact your vendor to select a method that works best for your environment.

For more information about the different vendor products offered, review the Azure and AWS documentation:

- For Azure, see https://docs.microsoft.com/en-us/azure/.
- For AWS, see https://aws.amazon.com/.

Chapter 2: Installing RSA Archer

This chapter guides you through performing a new installation.

Installation

Your RSA Archer infrastructure configuration must meet the minimum requirements outlined in System Requirements. For more details on how to prepare, see Preparing the Servers.

These instructions follow the RSA recommended installation, in which you will install the Web Application and Services components on all Web Servers and the Services component on all Services Servers.

Preparing RSA Archer for Installation

To begin, plan and prepare your system for installing RSA Archer. This requires the expertise of IT and database administrators. A worksheet is provided to keep track of administrator credentials. See the Pre-Installation Worksheet in Appendix C.

Responsible Role	Administration Task
IT administrators	Install and configure these software packages: • Microsoft Windows Server 2012 R2 or 2016 ◦ Microsoft Internet Information Services (IIS) 8.5 or 10 ◦ Microsoft .NET Framework 4.7.2 • Microsoft SQL Server 2016 SP 1 (64-bit) or 2016 Enterprise Edition (64-bit) or 2017 (64-bit) • ScaleOut StateServer (Client and Server) • Redis (Redis 5.0.3 and Linux) See the documentation from Redis for supported Linux versions.
IT administrators	Configure network shares.
IT administrators	Run the IIS Application Pool and services as a domain-based services account to access the Network Share.

Responsible Role	Administration Task
Database administrators	Manage the following: • Databases with database owner roles. • Authentication methods for database connectivity.

Preparing the Servers

1. Prepare the Database Servers.
2. Prepare the Web Servers.
3. Prepare the Services Servers.
4. (Optional) Prepare the Cache Servers by following the guidelines from the caching provider.

See Appendix D: Preparation Checklist for worksheets and checklists that you can use to plan and track your work.

Preparing the Database Servers

The Database Server stores database information, such as the Instance Database and the File Repository, for RSA Archer. A configuration can have multiple Database Servers depending upon the environment complexity.

Prepare each database by following these tasks:

1. Verify that the database requirements are met.
2. Choose the Authentication method.
3. Repeat steps 1-2 on all databases in your RSA Archer configuration.

Prepare the following SQL databases before installing RSA Archer.

- Instance Database
- Configuration Database
- (Optional) Message Logging database

Task 1: Verify database requirements are met

Verify that the databases meet the requirements in the following table.

Field	Required Value
Collation Settings	Case insensitive
SQL Compatibility level	Microsoft SQL Server 2016 SP 1 (64-bit) or 2016 Enterprise Edition (64-bit) or 2017 (64-bit) = 130
User Account	Database Owner role
Locale	English (United States)
TCP/IP	Enabled SQL Server instance

Task 2: Determine the authentication method to use

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 following table describes two methods of connecting to the three databases in RSA Archer.

Database	Description
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.

Database	Description
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. 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 is synonymous with Trusted Connections. Use the Application Pool to isolate the Web Application when there are multiple IIS worker processes that share the same Web Server.

Preparing the Web Servers

The Web Server hosts the Web Application and RSA Archer Configuration service. A configuration can have multiple Web Servers depending upon the environment complexity.

Prepare the Web Servers by completing the following tasks:

1. Verify that the Web Server requirements are met.
2. Configure IIS.
3. Verify the application pool requirements.
4. Confirm the user account.

The Web Server hosts the Web Application and configuration service of RSA Archer. Use the *RSA Archer Platform Planning Guide* to determine the best configuration for your data.

Task 1: Verify the Web Server requirements are met

The following chart identifies each component on the Web Servers and its requirements. Set up your Web Servers accordingly.

Component	Requirement
Microsoft Windows Server 2012 R2 or 2016	Administrator rights during the installation process.
Microsoft Internet Information Services (IIS) 8.5 or 10	IIS must be installed prior to installing .NET. If not, the appropriate .NET mappings may not be applied. Failure to follow the proper installation sequence as presented in this guide may result in having to re-register Microsoft .NET Framework 4.7.2.
Microsoft .NET	Microsoft .NET Framework 4.7.2 The .NET directory structure is the same for version 4.7.2 as it is for version 4.0. If you are performing a new RSA Archer installation on multiple Web Servers, you must configure the domain service account with full access to RSA Archer and .NET 4.0 Temporary Files directories.
(Optional) Microsoft Filter Pack 2.0 or later	If you want keyword searches to include Microsoft Office documents, install this on your Web Servers.
(Optional) ScaleOut StateServer Client	If you want to enable caching with ScaleOut StateServer, install the client on Web Server.

Task 2: Configure IIS

It is assumed that the IT Administrator is familiar with the process of configuring your IIS. The IT Administrator should complete the following tasks after installing Microsoft .NET Framework 4.7.2. Use the Microsoft Server Manager Dashboard to configure the IIS accordingly.

1. Install Microsoft .NET Framework 4.7.2

Required Options	Value
Microsoft .NET Framework 4.7.2 Features	.NET Framework 4.7.2 ASP.NET 4.7.2
WCF Services	HTTP Activation TCP Port Sharing

2. Install the required IIS roles and features. Disable the WebDAV Feature (RSA Archer does not support this feature).

Required Option	Value
Common HTTP Features	Default Document Directory Browsing HTTP Errors Static Content
Health and Diagnostics	HTTP Logging
Application Development	.NET Extensibility 4.7.2 ASP .NET 4.7.2 ISAPI Extensions ISAPI Filters
Security	Request Filtering
Performance	Static Content Compression Dynamic Content Compression **Note:** HTTP compression is enabled by default. If using a load balancer, RSA recommends disabling HTTP compression from the Web Servers and configuring HTTP compression to occur on the load balancer.
Management Tools	IIS Management Console
Application Pool > Managed Pipeline Mode	Integrated

3. Input the required values for IIS.

Required Option	Value
ISAPI and CGI Restrictions	Allow ASP.NET 4.0
Authentication Method	Anonymous

   Important: Only enable one authentication method, as more than one authentication method causes errors in the Manage Users, Manage Groups, and Report features of RSA Archer.

4. Create the application pool. For information on how to create an application pool, go to technet.microsoft.com.

   Note: Ensure that the Managed pipeline mode is set to Integrated. Not all product features are supported in Classic mode.

5. Verify that the Server Runs.

Task 3: Verify the application pool requirements

An application pool is required for administrating the RSA Archer Web Application. The application pool defines the set of Web Applications that share one or more worker processes, which are Windows processes that run Web Applications.

Required values for configuring the application pool

Required Option	Value
Application Pool Name	Choose a name that makes sense to you.
.NET Framework version	Microsoft .NET Framework 4.7.2
Start application pool immediately	Select this checkbox.

Task 4: Confirm user account

RSA Archer requires a specified user account for accessing the various files in the Web Server. Make sure your credentials work appropriately.

Preparing the Services Servers

1. Verify the Services server requirements.
2. Configure the network share.

3. Configure the keyword indexing for attachments. (Optional)
4. Configure the message logging.

Task 1: Verify the Services Server requirements

Verify the following requirements:

Component	Requirement
Microsoft .NET	Microsoft .NET Framework 4.7.2
Microsoft Windows Server 2012 R2 or 2016	Administrator rights during the installation process

Task 2: Configure the network share

Configure your Network Share to:

- Maintain the File Repository and Company_files to be accessible to all servers.
- Allow read and write permissions to the pre-defined domain-based service account.

  Note: Running the IIS Application Pool and the services as a domain-based services account enables RSA Archer Platform to access the Network Share regardless of where they reside in the network.

- Place search indexes and RSA Archer Queuing services on the same server.
- Reside on one of the following:
  - One of the designated RSA Archer servers.
  - Standardized file server/NAS.

The following table describes the authentication details depending on the number of servers in the RSA Archer environment.

	SQL Database Servers	Windows Integrated DB Authentication
Number of Servers	2 or more	2 or more
Database authentication method	SQL credentials	Windows Integrated Security

	SQL Database Servers	Windows Integrated DB Authentication
Archer Services log on account	Domain account	Domain account
IIS Application Pool	Domain account	Domain account

Task 3: Configure the keyword indexing for attachments (Optional)

RSA Archer can perform keyword searches of Microsoft Office documents attachments. This configuration is optional, but necessary if you are using the Microsoft Filter Pack 2.0 or later or SMTP service.

If you are using localhost as the notifications mail relay server, install the SMTP Service in IIS and configure the Relay Restrictions with the loopback IP address.

Task 4: Configure the message logging

1. Create a database dedicated to the logs.
   RSA Archer Event Tracing for Windows (ETW) traces 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.
2. If you create an account separate from the Local systems account, add access to the Performance Log Users group.
3. Use a third-party tool to view these logs. For more information on logs, see Message Logging.
   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

Preparing the Primary and High Availability Servers

(Optional)

1. Verify the Cache Server software requirements from ScaleOut StateServer or Redis.
2. If you use Virtual Machines, contact your Virtual Infrastructure administrator to verify assigned memory and guarantee 100% CPU resources. Performance degradation can occur if you do not have sufficient resources

Installing Components

Once the servers are prepared, install RSA Archer using the following methods for each of your servers.

- Installing the Web Application and Services Components
- Installing the Services Server

See Appendix D: Installation Checklist for worksheets and checklists that you can use during installation.

Installing the Web Application and Services Components

Run this installation on your Web Server to install RSA Archer Web Application and configuration services.

Task 1: Prepare the installer package

1. Download the RSA Archer 6.7 installer package from RSA Link.

   https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/

2. Use the Run as Administrator option to extract the installation package on the server to a location that is accessible to other servers.
3. Back up the instance and configuration databases created during the server preparation process. This process ensures that your data is current so that you can recover it if necessary.

Task 2: Run the installer on all Web servers and Services servers

Run the installer on all web and services servers.

1. Open the installation folder, and right-click ArcherInstall.exe.
2. Select Run as Administrator.
3. Click OK to run the installer.
4. Select the appropriate language for the installer to use.
5. Read the license agreement, and select I accept the terms in the license agreement.
6. Read the Diagnostics and System Data License.
7. Click Next.

Task 3: Install the Web Application and services

Begin at the RSA Archer Platform - Installation Options page.

1. Verify that the following components are selected:
   - Web Application
   - Services
     Note: Disable unwanted services after installation.
   - Instance Database
   - Advanced Workflow Service
2. Click Next.

Task 4: Specify the X.509 certificate

Important: You must use the same X.509 certificate during installations on all types of servers. For more information, see X.509 Certificates.

Begin at the RSA Archer Platform - Specify Certificate page.

1. In Specify where to obtain the X.509 certificate, do one of the following:
   - Select Create a certificate to create a new certificate.
   - Select an existing certificate from a disk or a certificate store.
     - If selecting from a disk, follow these steps:
       a. Choose Select from disk.
       b. In Specify the file to import into the certificate store, click ... to display a Windows Explorer Open File window, and then navigate to the location of the certificate file.
       c. Select the file, and click OK.
       d. In Type the password for the private key, enter the applicable certificate password.
     - If selecting from a certificate store, follow these steps:
       a. Choose Select from certificate store.
       b. In Select a certificate from the store, expand the category and select the certificate.
2. Click Next.

Task 5: Set the configuration database options (if prompted)

Complete this task only if prompted during the installation process. If the installer detects the RSA Archer Configuration service, the RSA Archer Platform - Configuration Database Options page does not display.

Begin at the RSA Archer Platform - Configuration Databases Options page.

1. In SQL Server, enter the SQL Server that hosts the Configuration Database.
2. If you are using a SQL Server account, enter the following, otherwise go to step 4.
   - Login name
   - Password
3. If you are using integrated security complete the following, otherwise go to step 4.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
4. In Database, enter the Configuration Database.
5. Click Next.

Task 6: Configure Advanced Workflow HTTPS

Begin at the RSA Archer Platform - Specify HTTPS Binding Certificate page.

Note: Advanced workflow requires a dedicated certificate.

1. Enter the port to securely communicate with the Advanced Workflow Service in HTTPS Port.
2. Do one of the following:

   Note: The port numbers for Advanced Workflow REST URL and Advanced Workflow Communication Port cannot be the same when using HTTPS. For example by default, the Advanced Workflow REST URL default port is 8443 and the Advanced Workflow Communication default port is 8000.

   - Use HTTPS
     - Specify where to obtain the X.509, by doing one of the following:
       - If using current certificate, select Use current certificate.

         Note: This option is unavailable, if this is the first installation for your configuration.

        - If selecting from a certificate store, follow these steps:
          a. Select from certificate store.
          b. In Select a certificate from the store, expand the category and select the certificate.
      - Specify the HTTPS Port

        Note: If the system detects the specified port number is in use, you must confirm you wish to replace the certificate bound to the specified port.
   - Use HTTP only (Not recommended)
3. Click Next.

Task 7: Set the REST URL and Communication Port for Advanced Workflow service

Begin at the RSA Archer Platform Advanced Workflow Settings page.

1. If using HTTP, click Next.

   Note: During HTTP, the RSA Archer uses default ports and URLs.

2. If using HTTPS, do the following:
   a. Change Advanced Workflow REST URL to the same value specified when configuring Advanced Workflow HTTPS. For example, https://hostName:8000/ where hostName is the fully qualified domain name of the host where the Advanced Workflow Service is installed. If there are multiple Advanced Workflow Service hosts, hostName is the DNS name for the load balancer and the port number refers to the port for which you have configured the load balancer.
   b. Change the Advanced Workflow Communication Port to a different port than you specified when configuring Advanced Workflow HTTPS. (The default value is 8000.)

      Note: If this is a new install, the system populates this field with information from the certificate and HTTPS port used to configure Advanced Workflow HTTPS.
   c. Click Next.

Task 8: Select the language for RSA Archer and content (if prompted)

If you did not check the Instance Database box in Task 6, this task is skipped automatically.

Begin at the RSA Archer Platform Language page.

1. In Select the language for RSA Archer Platform, select the language that you want to use for RSA Archer. By default, the language is US English. The supported languages are English (US),

Chinese, French, German, Italian, Japanese, Portuguese (Brazil), and Spanish.

2. Click Next.

Task 9: Set the instance database

Begin at the RSA Archer Platform - Instance Database Options page.

1. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
2. If you are using a SQL Server account, enter the following, otherwise go to step 4.
   - Login name
   - Password
3. If you are using integrated security complete the following, otherwise go to step 4.
   a. Select User integrated security.
   b. In Database, enter the instance database.
4. Click Next.

Task 10: Set the default time zone for the configuration database (if prompted)

This time zone for the configuration database applies to all instances unless you override it for a specific instance in the RSA Archer Control Panel.

Note: If the installer detects a time zone, it does not prompt you to set the default time zone, and the Web Application Options page opens; skip this task.

Begin at the RSA Archer Platform - Time Zone page.

1. In Time Zone, select the default time zone for RSA Archer.
2. Click Next.

Task 11: Configure the Web Application options

Begin at the RSA Archer Platform - Web Application Options page.

1. In Website, select the destination site for the RSA Archer Web Application.
2. Under Destination directory, verify that destination directory is set to the Web Application installation:

   - Install in the website's default application.
   - Install in an IIS application.
3. Click Next.
4. Click Yes to confirm the destination directory.

Task 12: Enable HTTPS automatically for communication between Web Servers and web traffic

If prompted, begin at the RSA Archer Platform - Specify HTTPS Binding Certificate page.

1. Do one of the following:
   - Use Existing Binding
   - Create New Binding
     - Specify where to obtain the X.509, by doing one of the following:
       - If selecting from a disk, follow these steps:

         a. Select from disk.

         b. In Specify the file to import into the certificate store, click ... to display a Windows Explorer Open File window, and then navigate to the location of the certificate file.

         c. Select the file, and then click Open.

         d. In Type the password for the private key, enter the applicable certificate password.
       - If selecting from a certificate store, follow these steps:

         a. Select from certificate store.

         b. In Select a certificate from the store, expand the category and select the certificate.
2. Click Next.

Important: RSA recommends removing any existing HTTP binding from IIS to ensure secure configuration.

Task 13: (Optional) Set the instrumentation database options for message logging

If you are using Message Logging or other event logging, enter the connections to the instrumentation database. RSA recommends using a dedicated database and not the instance or configuration database for this purpose.

Begin at the RSA Archer Platform - Instrumentation Database Options page.

1. Specify the setting for the Not using RSA Archer Instrumentation service option:
   - If you do not want to use the service, select the option (default). Go to step 5.
   - If you want to use the service, clear the option. Go to step 2.
2. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
3. If you are using a SQL Server account, enter the following, otherwise go to step 5.
   - Login name
   - Password
4. If you are using integrated security complete the following, otherwise go to step 5.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
5. Click Next.

Task 14: Configure the service credentials

Begin at the RSA Archer Platform - Services Credentials page.

1. Select
   - Use the Local System account to run all services.
   - Use the specified account to run all services and provide Account Credentials.
2. Click Next.

Note: To allow correct RSA Archer Services installation, ensure that Log on as a Service is enabled for the Window Services Account.

Task 15: Set the services and application file paths

Begin at the RSA Archer Platform - Services and Application Files page.

1. In Services, enter the path where the services are installed.
   By default, the path is C:\Program Files\RSA Archer\Services.
2. In Application Files, enter the path where the application files are installed.
   By default, the path is C:\Program Files\RSA Archer.

> **Note:** RSA recommends that you do not install Web Application or products in the same virtual directory or Root of Archer. Browsers send Cookies if more than one Web Application resides in same space; this behavior may lead to passing Archer cookies to any other application installed in same Root or Virtual Directory.

3. In Program Group, select one of the following options, and click Next.
   - Create RSA Archer program group for the current user only
   - Create RSA Archer group for all users (Recommended)
   - Do not create RSA Archer program group
4. Click Next.
5. Click Yes to confirm the newly created directories and program group.

Task 16: Set the path for the installer log file

Begin at the RSA Archer Platform - Log Location page.

1. In Log Path, enter the folder in which you want to store the log files. All servers in the RSA Archer environment use this path for logging events. When setting this path, use the same path for all web and services servers.
2. Click Next.

Task 17: Perform the installation

Begin at the RSA Archer - Perform Install page.

1. Click Next.
   The installer starts installing the applicable components. A progress bar opens.
2. Wait for the installer to complete installing the applicable components.
3. Click Finish.
   The RSA Archer Control Panel opens.

Task 18: Set the instance database options

In the RSA Archer Control Panel, begin at the RSA Archer Platform - Instance Database Options page.

1. In SQL Server, enter the server name. If the SQL Server is configured for a custom port, enter [servername],[portID].

2. Do one of the following for connecting to the instance database:

Database Management System	Do the following
SQL Server	Enter Authorization credentials
Integrated Security	In Database, select Use integrated security

3. Click Next.

Task 19: Stop all RSA Archer services except RSA Archer Configuration and RSA Archer Workflow services

Ensure all RSA Archer services are stopped but the RSA Archer Configuration service continues to run.

1. Run Windows Services as Administrator.
2. Scroll until the RSA Services appear.
   a. Right click each Service in turn.

      Note: Do not select RSA Archer Configuration or RSA Archer Workflow services.

   b. Select Stop.

Installing the Services Server

Run this installation on each services server.

Task 1: Prepare the installer package

1. Download the RSA Archer 6.7 installer package from RSA Link.

   https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/

2. Use the Run as Administrator option to extract the installation package on the server to a location that is accessible to other servers.
3. Back up the instance and configuration databases created during the server preparation process. This process ensures that your data is current so that you can recover it if necessary.

Task 2: Run the installer as administrator

Run the installer on all web and services servers.

1. Open the installation folder, and right-click ArcherInstall.exe.
2. Select Run as Administrator.
3. Click OK to run the installer.
4. Select the appropriate language for the installer to use.
5. Read the license agreement, and select I accept the terms in the license agreement.
6. Read the Diagnostics and System Data License.
7. Click Next.

Task 3: Install the Services component

Begin at the RSA Archer Platform - Installation Options page.

1. Verify that only desired components are selected.

   Note: When upgrading, options used in past installations are automatically selected.

   - Services Server
2. Click Next.

Task 4: Specify the X.509 certificate

Important: You must use the same X.509 certificate during installations on all types of servers. For more information, see X.509 Certificates.

Begin at the RSA Archer Platform - Specify Certificate page.

1. In Specify where to obtain the X.509 certificate, do one of the following:
   - Select Create a certificate to create a new certificate.
   - Select an existing certificate from a disk or a certificate store.
     - If selecting from a disk, follow these steps:
       a. Choose Select from disk.
       b. In Specify the file to import into the certificate store, click ... to display a Windows Explorer Open File window, and then navigate to the location of the certificate file.
       c. Select the file, and click OK.
       d. In Type the password for the private key, enter the applicable certificate password.

- If selecting from a certificate store, follow these steps:
    a. Choose Select from certificate store.
    b. In Select a certificate from the store, expand the category and select the certificate.

2. Click Next.

Task 5: Set the configuration database options

Complete this task only if prompted during the installation process. If the installer detects the RSA Archer Configuration service, the RSA Archer Platform - Configuration Database Options page does not display.

Begin at the RSA Archer Platform - Configuration Databases Options page.

1. In SQL Server, enter the SQL Server that hosts the Configuration Database.
2. If you are using a SQL Server account, enter the following, otherwise go to step 4.
    - Login name
    - Password
3. If you are using integrated security complete the following, otherwise go to step 4.
    a. Select User integrated security.
    b. In Database, enter the Instance Database.
4. In Database, enter the Configuration Database.
5. Click Next.

Task 6: (Optional) Set the instrumentation database options for message logging

If you are using Message Logging or other event logging, enter the connections to the instrumentation database. RSA recommends using a dedicated database and not the instance or configuration database for this purpose.

Begin at the RSA Archer Platform - Instrumentation Database Options page.

1. Specify the setting for the Not using RSA Archer Instrumentation service option:
    - If you do not want to use the service, select the option (default). Go to step 5.
    - If you want to use the service, clear the option. Go to step 2.
2. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].

3. If you are using a SQL Server account, enter the following, otherwise go to step 5.
   - Login name
   - Password
4. If you are using integrated security complete the following, otherwise go to step 5.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
5. Click Next.

Task 7: Configure the service credentials

Begin at the RSA Archer Platform - Services Credentials page.

1. Select
   - Use the Local System account to run all services.
   - Use the specified account to run all services and provide Account Credentials.
2. Click Next.

Note: To allow correct RSA Archer Services installation, ensure that Log on as a Service is enabled for the Window Services Account.

Task 8: Set the services file and application file paths

Begin at the RSA Archer Platform - Services and Application Files page.

1. In Services, enter the path where the services are installed.
   By default, the path is C:\Program Files\RSA Archer\Services.
2. In Application Files, enter the path where the application files are installed.
   By default, the path is C:\Program Files\RSA Archer.

   Note: RSA recommends that you do not install Web Application or products in the same virtual directory or Root of Archer. Browsers send Cookies if more than one Web Application resides in same space; this behavior may lead to passing Archer cookies to any other application installed in same Root or Virtual Directory.

3. In Program Group, select one of the following options, and click Next.
   - Create RSA Archer program group for the current user only
   - Create RSA Archer group for all users (Recommended)
   - Do not create RSA Archer program group
4. Click Next.
5. Click Yes to confirm the newly created directories and program group.

Task 9: Set the path for the installer log file

Begin at the RSA Archer Platform - Log Location page.

1. In Log Path, enter the folder in which you want to store the log files. All servers in the RSA Archer environment use this path for logging events. When setting this path, use the same path for all web and services servers.
2. Click Next.

Task 10: Perform the installation

Begin at the RSA Archer - Perform Install page.

1. Click Next.
   The installer starts installing the applicable components. A progress bar opens.
2. Wait for the installer to complete installing the applicable components.
3. Click Finish.

Chapter 3: Upgrading RSA Archer

This chapter guides you through the process of upgrading your RSA Archer in the recommended configuration, including preparing for the upgrade and the tasks for upgrading the RSA Archer Platform components.

RSA Archer for Upgrading

To prepare for your upgrade, RSA recommends the following:

- Schedule the upgrade during off-peak hours.
- Complete only the necessary steps to upgrade the components to the version you are installing. The installer extracts the data from the earlier version of your configuration and uses this data for upgrading the components during installation.
- Migrate all databases to a supported version of SQL Server.

Be aware that:

- All job engines and services must be stopped, except for RSA Archer Configuration Service.
- The X.509 certificate must be reused.
- The RSA Archer website will not be available during the upgrade.

Important: If you have previously used the Task Management application, ensure that the Status fields are populated in the application before upgrading. For more information, see Changes Made to the Task Management Application.

When you upgrade to release 6.7, users and groups selected in the Application Owner field are now selected in both the Configuration Administrator and Content Administrator fields. New configuration and content administration rights take effect immediately upon upgrade. Original application owners should have the same access to configuration and content that they did prior to the upgrade.

Upgrading All Components

RSA recommends upgrading all components at the same time to ensure that your instance database is also upgraded. Use the Upgrade Installation Worksheet to complete this task.

Important: You must run this upgrade on a Web Server or a server running IIS. Only run this upgrade once for upgrading the instance database. Follow the instructions for upgrading the other components at their respective web or Services Servers. See Upgrading the Web Servers and Upgrading the Services Servers.

Task 1: Prepare the installer package

1. Download the RSA Archer 6.7 installer package from RSA Link.

   https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/

2. Use the Run as Administrator option to extract the installation package on the server to a location that is accessible to other servers.

3. Back up the instance and configuration databases created during the server preparation process. This process ensures that your data is current so that you can recover it if necessary.

Task 2: Stop all RSA Archer Jobs

This task stops processing of new jobs while allowing currently running jobs to process. Jobs in progress and their associated child jobs can finish processing.

1. Run the RSA Archer Control Panel as Administrator. The default RSA Archer Control Panel installation path is C:\Program Files\RSA Archer\Archer Control Panel\ArcherTech.ControlPanel.exe.

2. Go to the Servers tab.

   a. From the Plugins menu, select Job Engine Manager.

   b. Click Servers.

3. Click Discontinue Job Processing.

4. In the Actions pane, click Save.

Task 3: Stop all RSA Archer services except RSA Archer Configuration service

This process ensures that all RSA Archer services are stopped but the RSA Archer Configuration service continues to run.

1. Run Windows Services as Administrator.

2. Scroll until the RSA Services appear.

   a. Right click each Service in turn.

      Note: Do not select RSA Archer Configuration service.

b. Select Stop.

Task 4: Shut down RSA Archer

This process prevents access to the RSA Archer website during the upgrade.

1. Open a command prompt.
2. In the Open field, enter

   ```
   iisreset /STOP
   ```

3. Press Enter.

Task 5: Run the installer as Administrator

Run the installer on all web and services servers.

1. Open the installation folder, and right-click ArcherInstall.exe.
2. Select Run as Administrator.
3. Click OK to run the installer.
4. Select the appropriate language for the installer to use.
5. Read the license agreement, and select I accept the terms in the license agreement.
6. Read the Diagnostics and System Data License.
7. Click Next.

Task 6: Install all components

In addition to installing all components, this installer establishes the connectivity to the instance database that typically resides on a different server.

Begin at the RSA Archer Platform - Installation Options page.

1. Verify that only desired components are selected.

   Note: Make sure to select the same components previously installed before running the upgrade. If running the installer against a specific component is required, ensure that the other components installed on the same server are also selected—otherwise, the installer will uninstall them.

Unselecting the Services component results in all installed services except for the Configuration Service and Advanced Workflow Service being uninstalled. Unselecting the Advanced Workflow Service results in that service being uninstalled.

- Web Application
- Services
- Instance Database
- Advanced Workflow

2. Click Next.

Task 7: Choose the x.509 certificate from store

You must select the same certificate as the one from your original installation of the RSA Archer. For more information, see X.509 Certificates.

Begin at the RSA Archer Platform - Choose Certificate page.

1. Verify that Use Current Certificate is selected.
2. Click Next.

Task 8: Configure Advanced Workflow HTTPS

Begin at the RSA Archer Platform - Specify HTTPS Binding Certificate page.

Note: Advanced workflow requires a dedicated certificate.

1. Enter the port to securely communicate with the Advanced Workflow Service in HTTPS Port.
2. Do one of the following:

   Note: The port numbers for Advanced Workflow REST URL and Advanced Workflow Communication Port cannot be the same when using HTTPS. For example by default, the Advanced Workflow REST URL default port is 8443 and the Advanced Workflow Communication default port is 8000.

   - Use HTTPS
     - Specify where to obtain the X.509, by doing one of the following:
       - If using current certificate, select Use current certificate.

         Note: This option is unavailable, if this is the first installation for your configuration.

        - If selecting from a certificate store, follow these steps:
            a. Select from certificate store.
            b. In Select a certificate from the store, expand the category and select the certificate.
    - Specify the HTTPS Port

      Note: If the system detects the specified port number is in use, you must confirm you wish to replace the certificate bound to the specified port.

- Use HTTP only (Not recommended)

3. Click Next.

Task 9: Set the REST URL and Communication Port for Advanced Workflow service

Begin at the RSA Archer Platform Advanced Workflow Settings page.

1. If using HTTP, click Next.

   Note: During HTTP, the RSA Archer uses default ports and URLs.

2. If using HTTPS, do the following:
   a. Change Advanced Workflow REST URL to the same value specified when configuring Advanced Workflow HTTPS. For example, https://hostName:8000/ where hostName is the fully qualified domain name of the host where the Advanced Workflow Service is installed. If there are multiple Advanced Workflow Service hosts, hostName is the DNS name for the load balancer and the port number refers to the port for which you have configured the load balancer.
   b. Change the Advanced Workflow Communication Port to a different port than you specified when configuring Advanced Workflow HTTPS. (The default value is 8000.)

      Note: If this is a new install, the system populates this field with information from the certificate and HTTPS port used to configure Advanced Workflow HTTPS.

   c. Click Next.

Task 10: Select the language for RSA Archer and content

If you did not check the Instance Database box in Task 6, this task is skipped automatically.

Begin at the RSA Archer Platform Language page.

1. In Select the language for RSA Archer Platform, select the language that you want to use for RSA Archer. By default, the language is US English. The supported languages are English (US), Chinese, French, German, Italian, Japanese, Portuguese (Brazil), and Spanish.
2. Click Next.

Task 11: Set the instance database options

The installer detects whether more than one instance exists so that all Instance Database connections can be upgraded at the same time. If the installer does not detect the Configuration service, it cannot detect whether there are multiple instances.

Begin at the RSA Archer Platform- Instance Database Options page.

Note: Complete step 1 only when multiple instances exist. If the installer does not detect multiple instances, it does not prompt for a database instance selection.

1. Do one of the following:
   - If you want to upgrade each instance individually, go to step 2. By default, the Single Database Instance (Recommended) option is selected. If you select this option, run the installer to upgrade all other instances.
   - If you want to update multiple instances at the same time, select Multiple Database Instances (Advanced). Select the instances that you want to upgrade. The instances you select upgrade one at a time.
2. In SQL Server, enter the server name. If the SQL Server is configured for a custom port, enter [servername],[portID].
3. If you are using integrated security complete the following, otherwise go to step 4.
   a. Select User integrated security.
   b. In Database, enter the instance database.
4. Click Next.
5. Click Yes or Yes to All. If you select Yes, you must confirm each database.

Task 12: Configure the Web Application options

Begin at the RSA Archer Platform - Web Application Options page.

1. In Website, select the destination site for the RSA Archer Web Application.
2. Under Destination directory, verify that destination directory is set to the Web Application installation:
   - Install in the website's default application.
   - Install in an IIS application.
3. Click Next.
4. Click Yes to confirm the destination directory.

Task 13: (Optional) Set the instrumentation database options for message logging

If you are using Message Logging or other event logging, enter the connections to the instrumentation database. RSA recommends using a dedicated database and not the instance or configuration database for this purpose.

Begin at the RSA Archer Platform - Instrumentation Database Options page.

1. Specify the setting for the Not using RSA Archer Instrumentation service option:
   - If you do not want to use the service, select the option (default). Go to step 5.
   - If you want to use the service, clear the option. Go to step 2.
2. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
3. If you are using a SQL Server account, enter the following, otherwise go to step 5.
   - Login name
   - Password
4. If you are using integrated security complete the following, otherwise go to step 5.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
5. Click Next.

Task 14: Set the services and application paths

The installer populates the paths with the applicable path from the existing installation.

Begin at the RSA Archer Platform - Services and Application Files page.

1. In Services, verify the path where the services are installed.
2. In Application Files, verify the path where the application files are installed.
3. In Program Group, verify that Create RSA Archer group for all users is selected, and click Next.

Note: RSA recommends that you do not install Web Application or products in the same virtual directory or Root of Archer. Browsers send Cookies if more than one Web Application resides in same space; this behavior may lead to passing Archer cookies to any other application installed in same Root or Virtual Directory.

Task 15: Set the path for the installer log file

Begin at the RSA Archer Platform - Log Location page.

1. In Log Path, verify the path where the log file is stored, and click Next.
2. Confirm whether to copy the application files. Do one of the following:
   - To copy the application files, click Yes, and select the folder to which you want to copy the application files.
   - To continue without copying the application files, click No.
3. Click OK.

Task 16: Acknowledge configuration changes for installs that include Advanced Workflow

A window may appear in some configuration. The window reads as follows:

The installation process identified a number of places where Advanced Workflows are subject to a configuration change in this release. Certain functionality is no longer delivered using Apply Conditional Layout actions (which are part of DDEs). To see which workflows and actions have been affected, review the DDE log file, which is located in the folder designated in the Log Path field during installation. For instructions on updating affected workflows, see "Reconciling 6.2 Advanced Workflow Apply conditional Layout Action Changes", which is available both as a standalone PDF and as an appendix in the 6.2 Installation and Upgrade Guide. You can download both documents from RSA Archer Community on RSA Link.

Click OK.

Task 17: Perform the installation

Begin at the RSA Archer - Perform Install page.

1. Click Next.
   The installer starts installing the applicable components. A progress bar opens.
2. Wait for the installer to complete installing the applicable components.
3. Click Finish.
   The RSA Archer Control Panel opens.

Task 18: Start IIS on all Web Servers

Begin at a Command prompt on a Web Server.

1. Open a Command Prompt.
2. In the Open field, enter

   ```
   iisreset /START
   ```

3. Click Enter.

Task 19: Verify the instance configuration

Begin in Windows Services.

1. Start all RSA Archer services, except RSA Archer Configuration Services which should already be running.

   Note: If you are using Advanced Workflow, start the RSA Archer Workflow server at the Web Servers.

2. Go to Job Engine Manager in the RSA Archer Control Panel, and start job processing.
   1. Click the Server tab and clear the Discontinue Job Processing checkbox to start processing jobs.
   2. In the Actions pane, click Save.
3. On the Installation Settings tab, verify the Logging and Default Local and Time Zone settings.
4. Double click the default instance to view the instance settings on the right pane and go to each

tab to verify that all information in the configuration is correct.

5. Click Save.
6. Repeat steps 4 and 5 for all other instances.
7. On the dedicated Services Server, start all RSA Archer services.

Upgrading the Services Servers

Upgrading the Services Server consists of installing the Services component. You must upgrade this component on each server for the services role. This upgrade takes a few minutes and occurs simultaneously during the installation of the Instance Database component.

Task 1: Prepare the installer package

1. Download the RSA Archer 6.7 installer package from RSA Link.

   https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/

2. Use the Run as Administrator option to extract the installation package on the server to a location that is accessible to other servers.
3. Back up the instance and configuration databases created during the server preparation process. This process ensures that your data is current so that you can recover it if necessary.

Task 2: Stop all RSA Archer Jobs

This task stops processing of new jobs while allowing currently running jobs to process. Jobs in progress and their associated child jobs can finish processing.

1. Run the RSA Archer Control Panel as Administrator. The default RSA Archer Control Panel installation path is C:\Program Files\RSA Archer\Archer Control Panel\ArcherTech.ControlPanel.exe.
2. Go to the Servers tab.
   a. From the Plugins menu, select Job Engine Manager.
   b. Click Servers.
3. Click Discontinue Job Processing.
4. In the Actions pane, click Save.

Task 3: Stop all RSA Archer services except RSA Archer Configuration service.

This process ensures that all RSA Archer services are stopped but the RSA Archer Configuration service continues to run.

1. Run Windows Services as Administrator.
2. Scroll until the RSA Services appear.
   a. Right click each Service in turn.

      Note: Do not select RSA Archer Configuration service.

   b. Select Stop.

Task 4: Shut down RSA Archer

This process prevents access to the RSA Archer website during the upgrade.

1. Open a command prompt.
2. In the Open field, enter

   ```
   iisreset /STOP
   ```

3. Press Enter.

Task 5: Run the installer as Administrator

Run the installer on all web and services servers.

1. Open the installation folder, and right-click ArcherInstall.exe.
2. Select Run as Administrator.
3. Click OK to run the installer.
4. Select the appropriate language for the installer to use.
5. Read the license agreement, and select I accept the terms in the license agreement.
6. Read the Diagnostics and System Data License.
7. Click Next.

Task 6: Install the services component

Begin at the RSA Archer Platform - Installation Options page.

1. Verify that only desired components are selected.

   Note: When upgrading, options used in past installations are automatically selected.

   - Services Server
2. Click Next.

Task 7: Choose the X.509 certificate from store

You must select the same certificate as the one from your original installation of the RSA Archer. For more information, see X.509 Certificates.

Begin at the RSA Archer Platform - Choose Certificate page.

1. Verify that Use Current Certificate is selected.
2. Click Next.

Task 8: (Optional) Set the instrumentation database options for message logging

If you are using Message Logging or other event logging, enter the connections to the instrumentation database. RSA recommends using a dedicated database and not the instance or configuration database for this purpose.

Begin at the RSA Archer Platform - Instrumentation Database Options page.

1. Specify the setting for the Not using RSA Archer Instrumentation service option:
   - If you do not want to use the service, select the option (default). Go to step 5.
   - If you want to use the service, clear the option. Go to step 2.
2. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
3. If you are using a SQL Server account, enter the following, otherwise go to step 5.
   - Login name
   - Password

4. If you are using integrated security complete the following, otherwise go to step 5.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
5. Click Next.

Task 9: Set the configuration services credentials

Begin at the RSA Archer Platform - Services Credentials page.

1. Verify that Use the specified account to run all services is selected.
2. In User Name, enter the user name in the following format: domain\user.
3. In Password, enter the password for the domain user account.
   If you want to see the password while typing, click Show password.
4. Click Next.

Task 10: Set the services and application paths

The installer populates the paths with the applicable path from the existing installation.

Begin at the RSA Archer Platform - Services and Application Files page.

1. In Services, verify the path where the services are installed.
2. In Application Files, verify the path where the application files are installed.
3. In Program Group, verify that Create RSA Archer group for all users is selected, and click Next.

Note: RSA recommends that you do not install Web Application or products in the same virtual directory or Root of Archer. Browsers send Cookies if more than one Web Application resides in same space; this behavior may lead to passing Archer cookies to any other application installed in same Root or Virtual Directory.

Task 11: Set the path for the installer log file

Begin at the RSA Archer Platform - Log Location page.

1. In Log Path, verify the path where the log file is stored, and click Next.
2. Confirm whether to copy the application files. Do one of the following:
   - To copy the application files, click Yes, and select the folder to which you want to copy the application files.
   - To continue without copying the application files, click No.
3. Click OK.

Task 12: Perform the installation

Begin at the RSA Archer - Perform Install page.

1. Click Next.
   The installer starts installing the applicable components. A progress bar opens.
2. Wait for the installer to complete installing the applicable components.
3. Click Finish.
   The RSA Archer Control Panel opens.

Task 13: Start IIS on all Web Servers

Begin at a Command prompt on a Web Server.

1. Open a Command Prompt.
2. In the Open field, enter
   ```
   iisreset /START
   ```
3. Click Enter.

Task 14: Verify the instance configuration

Begin in Windows Services.

1. Start all RSA Archer services.

   Note: If you are using Advanced Workflow, start the RSA Archer Workflow server at the Web Servers.

2. Go to Job Engine Manager in the RSA Archer Control Panel, and start job processing.
   1. Click the Server tab and clear the Discontinue Job Processing checkbox to start processing jobs.
   2. In the Actions pane, click Save.
3. At the Installation Settings tab, verify the global settings of the RSA Archer. These settings are Logging, and Default Local and Time Zone.
4. Select the default instance and go to each tab and verify that all information in the configuration is correct.
5. Save if you have made changes to the instance configuration.
6. Repeat steps 4 and 5 for all other instances.
7. On the dedicated Services Server, start all RSA Archer services.

Upgrading the Web Servers

Upgrading the web role consists of installing the Web Application and Services components on the dedicated Web Server. You must upgrade these components on each server for the web role. The Web Application component requires the connection to the RSA Archer Configuration service.

This upgrade takes a few minutes and can occur simultaneously during the installation of the Instance Database component, if applicable.

Important: This version of RSA Archer requires Microsoft .NET Framework 4.7.2. For additional information about system requirements, see System Requirements. Be sure to install all required components before running the installer.

Task 1: Prepare the installer package

1. Download the RSA Archer 6.7 installer package from RSA Link.

   https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/

2. Use the Run as Administrator option to extract the installation package on the server to a location that is accessible to other servers.
3. Back up the instance and configuration databases created during the server preparation process. This process ensures that your data is current so that you can recover it if necessary.

Task 2: Stop all RSA Archer Jobs

This task stops processing of new jobs while allowing currently running jobs to process. Jobs in progress and their associated child jobs can finish processing.

1. Run the RSA Archer Control Panel as Administrator. The default RSA Archer Control Panel installation path is C:\Program Files\RSA Archer\Archer Control Panel\ArcherTech.ControlPanel.exe.
2. Go to the Servers tab.
   a. From the Plugins menu, select Job Engine Manager.
   b. Click Servers.
3. Click Discontinue Job Processing.
4. In the Actions pane, click Save.

Task 3: Stop all RSA Archer services except RSA Archer Configuration service

This process ensures that all RSA Archer services are stopped but the RSA Archer Configuration service continues to run.

1. Run Windows Services as Administrator.
2. Scroll until the RSA Services appear.
   a. Right click each Service in turn.

      Note: Do not select RSA Archer Configuration service.

   b. Select Stop.

Task 4: Shut down RSA Archer

This process prevents access to the RSA Archer website during the upgrade.

1. Open a command prompt.
2. In the Open field, enter

   ```
   iisreset /STOP
   ```

3. Press Enter.

Task 5: Run the installer as Administrator

Run the installer on all web and services servers.

1. Open the installation folder, and right-click ArcherInstall.exe.
2. Select Run as Administrator.
3. Click OK to run the installer.
4. Select the appropriate language for the installer to use.
5. Read the license agreement, and select I accept the terms in the license agreement.
6. Read the Diagnostics and System Data License.
7. Click Next.

Task 6: Install the web components

Begin at the RSA Archer Platform - Installation Options page.

1. Verify that only desired components are selected.

   Note: When upgrading, options used in past installations are automatically selected.

   - Web Application
   - Services Server
   - Advanced Workflow
2. Click Next.

Task 7: Choose the X.509 certificate from store

You must select the same certificate as the one from your original installation of the RSA Archer. For more information, see X.509 Certificates.

Begin at the RSA Archer Platform - Choose Certificate page.

1. Verify that Use Current Certificate is selected.
2. Click Next.

Task 8: Configure Advanced Workflow HTTPS

Begin at the RSA Archer Platform - Specify HTTPS Binding Certificate page.

Note: Advanced workflow requires a dedicated certificate.

1. Enter the port to securely communicate with the Advanced Workflow Service in HTTPS Port.
2. Do one of the following:

   Note: The protocol and port numbers for this task must match those given in the following task.

   - Use HTTPS
     - Specify where to obtain the X.509, by doing one of the following:
       - If using current certificate, select Use current certificate.

         Note: This option is unavailable, if this is the first installation for your configuration.

       - If selecting from a certificate store, follow these steps:
         a. Select from certificate store.
         b. In Select a certificate from the store, expand the category and select the certificate.
     - Specify the HTTPS Port

       Note: If the system detects the specified port number is in use, you must confirm you wish to replace the certificate bound to the specified port.

   - Use HTTP only (Not recommended)
3. Click Next.

Task 9: Set the URL for the Advanced Workflow service

Begin at the RSA Archer Platform Advanced Settings page.

1. Change the value to http://hostName:8000/ where hostName is the fully qualified domain name of the host where the Advanced Workflow Service is installed. If there are multiple Advanced Workflow Service hosts, hostName is the DNS name for the load balancer and the port number refers to the port for which you have configured the load balancer.
2. Click Next.

Task 10: Set the REST URL and Communication Port for Advanced Workflow service

Begin at the RSA Archer Platform Advanced Workflow Settings page.

1. If using HTTP, click Next.

   Note: During HTTP, the RSA Archer uses default ports and URLs.

2. If using HTTPS, do the following:

   a. Change Advanced Workflow REST URL to the same value specified when configuring Advanced Workflow HTTPS. For example, https://hostName:8000/ where hostName is the fully qualified domain name of the host where the Advanced Workflow Service is installed. If there are multiple Advanced Workflow Service hosts, hostName is the DNS name for the load balancer and the port number refers to the port for which you have configured the load balancer.

   b. Change the Advanced Workflow Communication Port to a different port than you specified when configuring Advanced Workflow HTTPS. (The default value is 8000.)

      Note: If this is a new install, the system populates this field with information from the certificate and HTTPS port used to configure Advanced Workflow HTTPS.

   c. Click Next.

Task 11: Select the language for RSA Archer and content

If you did not check the Instance Database box in Task 6, this task is skipped automatically.

Begin at the RSA Archer Platform Language page.

1. In Select the language for RSA Archer Platform, select the language that you want to use for RSA Archer. By default, the language is US English. The supported languages are English (US), Chinese, French, German, Italian, Japanese, Portuguese (Brazil), and Spanish.
2. Click Next.

Task 12: Configure the Web Application options

Begin at the RSA Archer Platform - Web Application Options page.

1. In Website, select the destination site for the RSA Archer Web Application.
2. Under Destination directory, verify that destination directory is set to the Web Application installation:
   - Install in the website's default application.
   - Install in an IIS application.
3. Click Next.
4. Click Yes to confirm the destination directory.

Task 13: (Optional) Set the instrumentation database options for message logging

If you are using Message Logging or other event logging, enter the connections to the instrumentation database. RSA recommends using a dedicated database and not the instance or configuration database for this purpose.

Begin at the RSA Archer Platform - Instrumentation Database Options page.

1. Specify the setting for the Not using RSA Archer Instrumentation service option:
   - If you do not want to use the service, select the option (default). Go to step 5.
   - If you want to use the service, clear the option. Go to step 2.
2. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
3. If you are using a SQL Server account, enter the following, otherwise go to step 5.
   - Login name
   - Password
4. If you are using integrated security complete the following, otherwise go to step 5.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
5. Click Next.

Task 14: Set the services credentials

Begin at the RSA Archer Platform - Services Credentials page.

1. Verify that Use the specified account to run all services is selected.
2. In User Name, enter the user name in the following format: domain\user.
3. In Password, enter the password for the domain user account.
   If you want to see the password while typing, click Show password.
4. Click Next.

Task 15: Set the services and application paths

The installer populates the paths with the applicable path from the existing installation.

Begin at the RSA Archer Platform - Services and Application Files page.

1. In Services, verify the path where the services are installed.
2. In Application Files, verify the path where the application files are installed.
3. In Program Group, verify that Create RSA Archer group for all users is selected, and click Next.

Note: RSA recommends that you do not install Web Application or products in the same virtual directory or Root of Archer. Browsers send Cookies if more than one Web Application resides in same space; this behavior may lead to passing Archer cookies to any other application installed in same Root or Virtual Directory.

Task 16: Set the path for the installer log file

Begin at the RSA Archer Platform - Log Location page.

1. In Log Path, verify the path where the log file is stored, and click Next.
2. Confirm whether to copy the application files. Do one of the following:
   - To copy the application files, click Yes, and select the folder to which you want to copy the application files.
   - To continue without copying the application files, click No.
3. Click OK.

Task 17: Perform the installation

Begin at the RSA Archer - Perform Install page.

1. Click Next.
   The installer starts installing the applicable components. A progress bar opens.

2. Wait for the installer to complete installing the applicable components.
3. Click Finish.
   The RSA Archer Control Panel opens.

Task 18: Start IIS on all Web Servers

Begin at a Command prompt on a Web Server.

1. Open a Command Prompt.
2. In the Open field, enter
   ```
   iisreset /START
   ```
3. Click Enter.

Task 19: Verify the instance configuration

Begin in Windows Services.

1. Start all RSA Archer services.

   Note: If you are using Advanced Workflow, start the RSA Archer Workflow server at the Web Servers.

2. Go to Job Engine Manager in the RSA Archer Control Panel, and start job processing.
   a. Click the Server tab and clear the Discontinue Job Processing checkbox to start processing jobs.
   b. In the Actions pane, click Save.
3. At the Installation Settings tab, verify the global settings of the RSA Archer. These settings are Logging, and Default Local and Time Zone.
4. Select the default instance and go to each tab and verify that all information in the configuration is correct.
5. Save if you have made changes to the instance configuration.
6. Repeat steps 4 and 5 for all other instances.
7. On the dedicated Services Server, start all RSA Archer services.

Chapter 4: Activating RSA Archer

This chapter guides you through activating your RSA Archer configuration after a new installation or an upgrade, and configuring Advanced Workflow, if necessary.

- Activation process for a new installation
- Activation process for an upgrade
- Configuring advanced workflow

Use the Post-Installation Worksheet to record your system configuration.

Activating an RSA Archer Installation

After completing a fresh installation of RSA Archer, use this section to configure your environment properly.

Activation Process for an Install

To complete your installation of RSA Archer, configure your environment and activate your servers. Activating servers is the process of ensuring files specific to RSA Archer have the proper permissions and can be accessed by the applicable service.

Activate your RSA Archer installation in the following phases:

Phase	What to do	Reference
1	Use the RSA Archer Control Panel to configure the global settings for RSA Archer in the Installation Setting tab.	*RSA Archer Control Panel Help*: • "Configuring Logging Rules" • "Configuring the Default Locale and Time Zone"
2	Use the RSA Archer Control Panel to do one of the following: • In the case of a vanilla installation, create an RSA Archer instance and set it as the default instance by selecting the "Enable a default instance" checkbox in Installation Settings. • In the case of an upgrade, connect to the existing instance.	*RSA Archer Control Panel Help*: • "Instance Configuration Settings" • "Completing the Default Creation" • "Setting the Default Instance"

Phase	What to do	Reference
3	Activate the Services Server by starting the RSA Archer services and verifying permissions to the domain account and X.509 certificate, for multiple-host installations.	Configuring the Services Server
4	Activate the Web Server by granting permissions to the RSA Archer directories and assigning the application pool to the website.	Configuring the Web Server

Keep the following in mind as you complete the verification process:

- Create your default instance.
- Register your license on your main Web Server.
- Start all RSA Archer services on your main Services Server.
- Start the RSA Archer Configuration service on every Web Server.
- Make sure your Network Share has the appropriate files in it.
- Map Network Share on every server.

Creating the RSA Archer Instance

You create instances in the RSA Archer Control Panel and then designate one of them as the default instance for all users. Each task references the applicable topic from the RSA Archer Control Panel Help to guide you through this process.

Task 1: Start the RSA Archer Queuing service

1. Go to Start > Services to open the Services window.
2. Locate RSA Archer Queuing in the list.
3. Verify RSA Archer Queuing service is running.
   - If the service is running, skip to Task 2.
   - If the service is not running, continue to Step 4.
4. Right-click RSA Archer Queuing.
5. Click Start.

Task 2: Create the default RSA Archer instance

Complete all tasks. See the RSA Archer Control Panel Help on Instance Settings for step-by-step help. Access the RSA Archer Control Panel Help by clicking the question mark icon in the upper right hand corner.

Instance Tab	Required
General	Configuring an Instance for Notifications (Default From Address) Configuring Logging Rules (Override) Configuring the Default Locale and Time Zone (Override) Designating the File Repository Path for an Instance Designating Search Index Path and the Queuing Server for an Instance
Web	Designating the Base and Authentication URLs for the Web Application
Database	Configuring the Instance Database Connection String and Pooling Options
Accounts	Changing SysAdmin and Service Account Passwords

Running the Maintenance SQL Script

Use a SQL script to maintain the RSA Archer database if your organization does not have its own standard process for maintaining Microsoft SQL database indexes and statistics. This script creates the RSA Archer Database Statistics Update job to update statistics and the RSA Archer Database Index Rebuild job to re-index the database.

For best results, schedule these jobs to run during inactive periods. For example, you can schedule the Statistics Update job to run every day at 3:00 AM and the Index Rebuild job to run every Sunday at 2:00 AM.

Note: The SQL Server Agent must be running before you can execute the script.

Run the Maintenance SQL Script

1. Log in as a system administrator to the server that hosts the RSA Archer database.
2. Navigate to the \RSA Archer\Tools\ folder.

3. Double-click jobDeployScript.sql.
4. Select the RSA Archer database as the current database.
5. Execute the script, which creates the Statistics Update and Index Rebuild database jobs.

Configuring the Web Server

Important: Ensure that the configuration files on each server share the same machineKey. This key uses encryption and needs to be the same on each Web Server to ensure proper key generation. For more information, see Configuring a Load Balancer for RSA Archer.

Perform these steps in the Internet Information Services (IIS) manager, unless otherwise specified.

Task 1: Specify the account application pool identity

1. In the IIS Manager, go to the Web Server > Application Pools.
2. Right-click the application pool for RSA Archer, and select Advanced Settings.
3. In Identity under Process Model, click the Ellipsis (...) at ApplicationPoolIdentity.
4. Click Custom Account, and click Set.
5. Enter appropriate values for the following:
   - User Name
   - Password
   - Confirm Password
6. Click OK, and then click OK again.
7. Click OK.

Task 2: Assign the application pool

Note: When assigning the application pool, select the RSA Archer website for your company. The website may reside on a virtual directory. These instructions reflect choosing the Default Web Site.

1. In the IIS Manager, go to Web Server > Sites > Default Web Site > *website*, for example RSA Archer.
2. Right-click on *website* and select Manage Application > Advanced Settings.
3. In General, click Application Pool and the Ellipsis (...) button next to it.
4. In Application pool, select the applicable application pool, and click OK.
5. Click OK.

6. Go to Web Server > Application Pools.
7. Right-click the applicable application pool > Advanced Settings.
8. In the General section, select v4.0 for .NET CLR Version.
9. Click OK.

Task 3: Verify application pool for the API

The API must run under or have the same configuration as the application pool of the website.

1. In the IIS Manager, go to Web Server > Sites > Default Web Site > *website*. For example, RSA Archer.
2. Expand the *website* node and go to the api node.
3. Right-click on the API node and select Manage Application > Advanced Settings.
4. In General, verify that the Application Pool is the same as the *website*.
5. Do one of the following:
   - If the application pool matches the website, go to the Step 6.
   - If the application pool does not match the website, do the following:
     a. In Application Pool, click the Ellipsis (...) button
     b. Select the application pool of the *website*, and click OK.
6. Click OK.

Task 4: Reconfigure the company_files directory as a virtual directory that is mapped to the network share

Complete this task if your configuration has multiple Services Servers.

Configure the virtual directory for the company_files after the initial installation in a multiple-host configuration. You must reconfigure the company_files directory as a virtual directory that is mapped to the network share.

1. On the network share, create the company_files directory and copy all directories from the local company_files folder to the newly created company_files folder. For example, Inetpub\wwwroot\RSAarcher\company_files.
2. Rename the original company_files directory to company_files.old.
3. Set the share properties on the company_files directory to Modify/Change and Read/Write on both Sharing and Security permissions tabs of the domain account.
4. In the IIS Manager, navigate to the Add Virtual Directory dialog box.

   a. Click Web Server >Sites > Default Web Site > RSA Archer.
   b. Right-click on RSA Archer website and select Add Virtual Directory.
5. In Alias, enter company_files.
6. In Physical Path, enter the path of the new created company_files on the network share, and click Connect as.
7. Select Specific user, and click Set.
8. In User name, enter the domain user account.
9. In Password, enter the password of the domain user account.
10. In Confirm password, re-enter the password of the domain user account, and click OK.
11. Click OK.
12. Click OK again.

Task 5: Grant permissions to the RSA Archer directories

Complete this task if your configuration has multiple Services Servers.

Complete this task for all configurations for the Web Application on the network share. Begin at Internet Information Services (IIS) Manager.

Verify that the Identity has Modify privileges for the following folders:

Directory	Path	Notes
Windows\Temp	SYSTEMDRIVE%\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files	
company_files	designated path on the Web Server or network share	For the company_files, Log files, Search Index, and File Repository, use the actual path for your configuration. For example, Inetpub\wwwroot\RSAarcher\company_files
Log Files	designated path on the Web Server or network share	For example, ..\RSAarcher\LogFiles
File Repository	designated path on the Web Server or network share	For example, ..\RSAarcher\FileRepository

Task 6: Reset IIS

1. Go to Start > Run.
2. In the Open field, enter

   ```
   iisreset.exe
   ```

3. Press Enter.

Task 7: Exclude folders from virus scanning (Recommended)

RSA recommends that you routinely run virus scanning software on the deployed servers. However, virus scanning software can interpret data inserted or updated in RSA Archer dependent directories as a virus or malware, for example, as with the RSA Archer Threat Management solution.

1. Disable virus scanning on the folders that contain the following files:
   - Windows\Microsoft.Net\Framework64
   - RSA Archer Company Files
   - RSA Archer Log Files
   - RSA Archer Index
   - RSA Archer File Repository
2. Disable virus scanning on the RSA Archer\Services\Workpoint\ folder in the RSA Archer program files, to prevent server performance degradation with some anti-malware solutions.

For additional information on "Virus Scanning," see the *RSA Archer Security Configuration Guide*.

Configuring the Services Server

On a fresh install, configuring the Services Server requires starting the RSA Archer services.

Task 1: Verify the domain user account has access to network share and company_file directories on the network share

1. Ensure that the log file is on a local drive and not the network share.
2. From RSA Archer Control Panel, verify the path to Logging on the Installation Settings tab. Make certain that the log file is on a local drive and not the network share.
3. In Explorer, verify that the Domain Account has Modify or Read/Write permissions.
4. Navigate to the network share and verify that the following folders have Modify or Read/Write permissions.

- File Repository
- company_files
- Indexes

Task 2: Verify the X.509 certificate permissions

This task ensures that the service account used by the services have Read permissions to the relevant X.509 certificate private key. This certificate was specified during the initial installation. For more information, see X.509 Certificates.

1. Start the Microsoft Management Console (MMC). Do the following:
   a. Click Start and Run.
   b. In Open, enter

      ```
      mmc
      ```
   c. Click OK. The Console Root window opens.
2. Click File > Add/Remove Snap-In.
3. In Available snap-ins, select Certificates and click Add.
4. Select Computer account and click Next. The Select Computer dialog box opens.
5. Select Local computer (the computer this console is running on), and click Finish.
6. Click OK.
7. Expand the Certificates (Local Computer) and the Personal folder, and click Certificates. If the certificate was created during the initial installation, the RSA Archer Configuration certificate is listed.
8. Right-click RSA Archer Configuration or the certificate specified during the installation and click All Tasks > Manage Private Keys.
9. In Group or User Names, do one of the following:
   - If the account is listed, go to the next step.
   - If the account is not listed, do the following:
     a. Click Add. The Select Users, Computers, Service Accounts, or Groups dialog box opens.
     b. In Enter the object names to select, enter the applicable object names, and click OK.
10. In Permissions for [account], do the following:
    a. At Full control, clear the Allow checkbox.
    b. At Read, select the Allow checkbox.

11. Repeat steps 9 and 10 for each account running the RSA Archer Services.
12. Click OK, save and close the Console window.

Task 3: Make the certificate revocation list accessible

Each time a job process starts, it validates the Certificate Revocation List (CRL). If a RSA Archer server does not have direct internet access, making the CRL distribution point inaccessible, a 15-second timeout occurs before the process can to continue. This timeout can introduce a significant delay for each job process that the Job Engine service starts.

To eliminate the 15 second delay, complete one of the following tasks:

Disable the certificate revocation list validation

Complete this task to disable CRL validation for the user account running the Job Engine service. Disabling CRL validation does NOT disable signature verification. The signing certificate still matches against the trusted root store.

1. Open Command Prompt.
2. Type:

   ```
   wmic useraccount get name,sid
   ```
3. Click OK.
4. Find the SID for user account running Job Engine.
   a. At the Command Prompt, type:

      ```
      RegEdit
      ```
   b. Go to HKEY_USERS > [SID of user account running Job Engine] > Software > Microsoft > Windows > CurrentVersion\WinTrust\Trust Providers > Software Publishing.
   c. In the right pane, double-click State.
   d. Change Value data (Hexadecimal) from 23c00 (default, checking enabled) to 23e00 (checking disabled).
5. Click OK.

Set a system-level HTTP proxy

Complete this task to set a system-level HTTP proxy so that any user who logs in to the system has Internet access without having to take another action. This situation may not be desirable behavior.

1. Open Command Prompt.
2. Type:

   ```
   netsh winhttp set proxy proxy-server=”[MyProxyServer:port]” bypass-list=”<local>,”
   ```

where *[MyProxyServer:port]* is populated with an actual proxy server and port number.

3. Press Enter.

Activating an RSA Archer Upgrade

After completing an upgrade of RSA Archer, use this section to configure your environment properly.

Activation Process for an Upgrade

To complete your upgrade of RSA Archer, configure your environment and activate your servers. Activating servers is the process of ensuring files specific to RSA Archer have the proper permissions and can be accessed by the applicable service.

It is accomplished in the following phases.

Phase	What to do	Reference
1	Use the RSA Archer Control Panel to do one of the following: • In the case of an install, create the default RSA Archer instance, including setting the default instance • In the case of an upgrade, connect to the existing instance	*RSA Archer Control Panel Help*: • "Instance Configuration Settings" • "Completing the Default Creation" • "Setting the Default Instance"
2	Create the RSA Archer Database Statistics Update job to update statistics and the RSA Archer Database Index Rebuild job to re-index the database.	Running the Maintenance SQL Script
3	Activate the RSA Archer instance by registering the license, starting the RSA Archer services and rebuilding the search indexes.	Activating the Instance *RSA Archer Control Panel Help:* • "Registering the Instance" • "Rebuilding Search Indexes"

Keep the following in mind as you complete the verification process:

- Register your license on your main Web Server.
- Start all RSA Archer services on your main Services Server.
- Start the RSA Archer Configuration service on every Web Server.

Activating the RSA Archer Instance

Activating the instance requires you to register your RSA Archer license and to rebuild search indexes. The RSA Archer Queuing service must be running to rebuild the search indexes.

Task 1: Use the RSA Archer Control Panel to license your RSA Archer software

Refer to the topic "Registering the Instance" in the *RSA Archer Control Panel Help* for complete instructions.

Task 2: Restart the RSA Archer Queuing Service

This step is required when registering your first instance. Go to the next step for subsequent registrations.

Begin at the Services window.

1. Locate RSA Archer Queuing in the list.
2. Right-click RSA Archer Queuing, and click Restart.

Task 3: Use the RSA Archer Control Panel to initialize the search indexes

See "Rebuilding Search Indexes" in the *RSA Archer Control Panel Help* for complete instructions.

Running the Maintenance SQL Script

Use a SQL script to maintain the RSA Archer database if your organization does not have its own standard process for maintaining Microsoft SQL database indexes and statistics. This script creates the RSA Archer Database Statistics Update job to update statistics and the RSA Archer Database Index Rebuild job to re-index the database.

For best results, schedule these jobs to run during inactive periods. For example, you can schedule the Statistics Update job to run every day at 3:00 AM and the Index Rebuild job to run every Sunday at 2:00 AM.

Note: The SQL Server Agent must be running before you can execute the script.

Run the Maintenance SQL Script

1. Log in as a system administrator to the server that hosts the RSA Archer database.
2. Navigate to the \RSA Archer\Tools\ folder.
3. Double-click jobDeployScript.sql.
4. Select the RSA Archer database as the current database.
5. Execute the script, which creates the Statistics Update and Index Rebuild database jobs.

Update the Task Management Application

After upgrading from RSA Archer 6.1 or earlier to RSA Archer 6.2 or later, you must update record permissions to allow tasks assigned to a group to be displayed on the task-driven landing screen.

1. Login to RSA Archer with administrative access.
2. Click Administration > Application Builder > Applications.
3. In the Applications list, click Task Management.
4. Click the Fields tab.
5. From the Fields list, click Assigned To.
6. Click the Options tab.
7. In the Field Population section, click Lookup.
8. From the Groups list, click All Groups, and click OK.
9. In the Field Population section, ensure that All Groups has both Read and Update rights.
10. From the Manage Field: Assigned To page, click Save.
11. From the Manage Application: Task Management page, click Save.

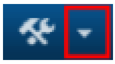
    Tasks assigned to groups now display on the Task Driven Landing screen for members of the assigned group.

Install the Admin Dashboard Package

When upgrading, it is necessary to install the Admin Dashboard Package. For more information, see "Admin Dashboard" in the RSA Archer Online Documentation.

To enable all features and iViews of the Admin Dashboard, you must import and install the Admin Dashboard package.

Import and map the Admin Dashboard package

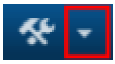
1. On RSA Link, download the Admin Dashboard package file.
2. Go to the Install Packages page.
    a. From the menu bar, click .
    b. Under Application Builder, click Install Packages.
3. In the Available Packages section, click Import.
4. Click Add New, then locate and select the Admin Dashboard package file.
5. Click OK.

    The package file is displayed in the Available Packages section and is ready for installation.

Note: Only the package file has been imported; you must map and install the package file to migrate the components to your instance of RSA Archer.

6. Map objects from the package.

Install the Admin Dashboard package

1. Go to the Install Packages page.
   1. From the menu bar, click .
   2. Under Application Builder, click Install Packages.
2. In the Available Packages section, select the Admin Dashboard package, and click Install.
3. In the Configuration section, select the components of the package that you want to install.
   - To select all components, select the top-level checkbox.
   - To install only specific global reports in an already installed application, select the checkbox associated with each report that you want to install.

   Note: Items in the package that do not match an existing item in the target instance are selected by default.
4. In the Configuration section, in the Install Method and Install Option fields, select one of the following options for each selected component.
   - Create New and Update
   - Override Layout(s)
   - Full Install
   - Override Permission(s)
5. Click Install.
6. Click OK.
7. Review the Package Installation Log.

Configuring Advanced Workflow

If you plan to use the Advanced Workflow feature, you may have to perform additional configuration activation, depending on your environment. Review the following tasks and complete any that are applicable to your environment.

Task 1: Open HTTP on localhost for communication between the Advanced Workflow service and RSA Archer

HTTP communication is used between the RSA Archer middle tier and the RSA Archer Advanced Workflow Service. If you have currently disabled HTTP communication, and want to use the Advanced Workflow feature, on the server running the RSA Archer Advanced Workflow Service, add exceptions for TCP port 8000 in your local firewall or other tools.

Task 2: Run the Advanced Workflow service with a non-admin account

By default, the Advanced Workflow service runs as administrator. However, if you do not want to run the service with admin or local system privileges, you can run the service under a different account that has the following permissions:

Directory	Access Required
C:\Program Files\RSA Archer\Services\Workpoint	Read/Write
C:\ArcherFiles\Logging	Write
The directory that the %TMP% or %TEMP% environment variables point to for the account.	Read/Write

To change the service account, do the following:

1. Open the Services Control Manager.
2. Right-click the Advanced Workflow service, and select Properties.
3. Click the Log On tab, and select This account.
4. Select the user you want to use, enter the credentials, and click OK.

Task 3: (Optional) Enable Advanced Workflow in a load balanced environment

If you are running RSA Archer with a load balancer, ensure that all of the internal servers running IIS and the Advanced Workflow service can communicate through port 8000.

This is set in the Archer Control Panel.

Additionally, you may force the RSA Archer Advanced Workflow service to honor currently configured proxy settings.

Task 4: Ensure Windows host registry key is valid

1. Open Regedit.exe
2. Confirm the following registry key stores the Advanced Workflow configuration information:

   HKEY_LOCAL_MACHINE\SOFTWARE\Workpoint LLC\Workpoint\x.x

   where *x.x* is the Workpoint version number installed in your environment.
3. Confirm the ServerAddress stores the hostname for the server.

Important: If the Windows host is renamed, Advanced Workflow does not synchronize correctly until the property is updated.

Enabling Elasticsearch

Elasticsearch improves how quickly data gets indexed.

Enable Elasticsearch

1. Open the RSA Archer Control Panel, and go to the Installation Settings tab.
2. On the General tab, go to the Elasticsearch section.
3. In the Elasticsearch field, select Enable Elasticsearch.
4. In the Elasticsearch Cluster field, click Add.
5. In the Cluster Name field, enter the cluster name and click OK.
6. Next to the Elasticsearch Node IP Configuration field, click Add New.
7. In the Enter URL field, enter the complete URL for the Elasticsearch Node IP and click OK. By default, Elasticsearch listens to port 9200. This port can be configured in the configuration file of Elasticsearch. For a secure connection to Elasticsearch, you must use 'https' (for example, https://1.1.1.1:9200).
8. To test the availability of the IPs, select the desired URL from the Elasticsearch Node IP Configuration field and click the Test Availability link below. Enter the username and password to authenticate and click Submit.
   The values for the user name and password entered are used by the system to authenticate and are not stored in a database. If you want to store these values, see "Store authentication information for instances" below.
9. On the toolbar, click Save.

Store authentication information for instances

Enabling authentication allows you to store authentication information used to connect with the selected Elasticsearch cluster for the particular instance.

1. Go to the Search Index section for the instance.
   a. From the Instance Management list, double-click the instance for which you want to enable authentication.
   b. On the General tab, go to the Search Index section.
2. In the Elasticsearch field, select Check this flag to use Elasticsearch as search data source.
3. From the Cluster Name drop-down list, select the cluster.
4. Select Enable Authentication and enter the user name and password that are used to connect RSA Archer with Elasticsearch for this instance.
5. On the toolbar, click Save.

Chapter 5: Validating RSA Archer

This chapter guides you through validating the components of your RSA Archer configuration. Use this with the Validation Checklist in Appendix D.

Platform System Validation

The validation process ensures that you have properly configured and activated system components for RSA Archer and that key elements of the RSA Archer function for your business operations.

The information in this chapter enables you to validate basic functionality. RSA recommends developing a more robust test plan to meet your specific business practices. Test any other features that you are using. For example, if notifications are a major part of your workflow, test this functionality. For additional information about getting your system operational, see the RSA Archer Online Documentation.

Validating RSA Archer Elements

Validate the RSA Archer elements to ensure that you have configured your instance correctly, including the search indexes, file repository, and company_files.

As part of this validation, you must add a new application, enter records, test a keyword search, and attach a file to a record. If you plan to use advanced workflow functionality, you will also create a test workflow in your application. Each task references the applicable topics from RSA Archer Online Documentation to guide you through this process.

Task 1: Open RSA Archer and log in as system administrator

Step	Action	Results
1	Start the browser, for example IE, and enter the Base URL to the RSA Archer.	This URL is established in the Web settings in the RSA Archer Control Panel.
2	Log in to the RSA Archer as system administrator: a. In User Name, enter sysadmin. b. In Company, enter the instance name. c. In Password, enter the password.	

Step	Action	Results
3	Click Login.	The RSA Archer page opens. If you do not see the Login page, see Troubleshooting System Components.

Task 2: Add and test a new application using Application Builder

Step	Action	Results
1	Create a new application from scratch. For information on creating new applications, see the topic "Adding Applications" in the Online Documentation and *RSA Archer Administrator's Guide*.	
2	Add the following field types: • Text with Search Results enabled • Attachment • Values List with three or more values For information on adding field types, see the topics "Adding a Text Field", "Adding an Attachment Field", and "Adding a Values List Field" in the Online Documentation and *RSA Archer Administrator's Guide*.	Each added field is listed on the Manage Fields page.
3	Add the newly created fields to the layout. For information on adding fields to a layout, see the topic "Adding Fields to the Layout" in the Online Documentation and *RSA Archer Administrator's Guide*.	

Step	Action	Results
4	(Optional) Build and activate a simple advanced workflow with the following settings: • Nodes: Start, Stop, and Update Content. Set the Update Content node to update a value in a field. (Creating a test record enables you to determine if the workflow you have built is valid). • Enrollment option: New. **Important:** Make sure that you activate the workflow. Workflows are created as inactive by default. For information on building and activating advanced workflows, see the topic "Building Advanced Workflows" in the Online Documentation and *RSA Archer Administrator's Guide*. **Note:** You only need to complete this step if you plan to use the advanced workflow functionality.	
5	Save the application.	The newly created application is listed on the Manage Applications page.
6	Go to your home page and open the application that you created. For information on working with records, see the topics called "Working with Records" in the Online Documentation and *RSA Archer Administrator's Guide*.	The Search Results page opens for that application.
7	Add two new records to the application and save.	The new records appear in the Search Results page of the application. If you created an advanced workflow, fields in the record are updated according to your design.

Task 3: Test keyword indexes by performing a keyword search

Step	Action	Results
1	Go to the Search Results page for the application you created.	The Search Results page opens for that application.
2	Run a Keyword Search using text entered in one of the records created in the test application.	Records found from the search are listed on the Search Results page.

For information on keyword searches, see "Running Searches in Applications and Questionnaires" and "Search Options: Keywords and Phrases" in the Online Documentation and *RSA Archer Administrator's Guide*.

Task 4: Validate the path to the File Repository folder by adding an attachment to a record

Step	Action	Results
1	Locate a file that you can attach to a record.	
2	Go to the Search Results page for the application you created.	
3	Navigate to the Attachment section, and click Add New.	
4	Attach the file to the record.	The newly attached file is a link on the record.
5	Click the link to the attachment.	The attachment file opens.

For information on working with attachments, see "Working with Records" and "Data Entry" in the Online Documentation and *RSA Archer Administrator's Guide*.

Task 5: (Optional) Test Advanced Workflow

Step	Action	Results
1	Log in to the RSA Archer as system administrator: a. In User Name, enter sysadmin. b. In Company, enter the instance name. c. In Password, enter the password.	
2	Go to the Application Builder.	
3	Open an application that has Advanced Workflow.	The application has advanced workflow tab.
4	Build an Advanced Workflow.	The nodes and transitions can be added properly.
5	Run the Advanced Workflow	The workflow functions as expected.

For information on working with advanced workflow, see "Building Advanced Workflows" in the Online Documentation and *RSA Archer Administrator's Guide*.

Troubleshooting System Components

If you cannot access RSA Archer at the login page, use the following tasks to troubleshoot the system components.

Validating Server Settings

Task 1: Validate IIS settings

The procedures for validating these settings depends on the version of IIS installed in your environment. The RSA Archer supports Microsoft Internet Information Services (IIS) 8.5 or 10.

Step	Action	Results
1	Verify that the ASP.NET 4.x is set to Allowed.	ISAPI and CGI Restrictions
2	Verify that only one authentication option is set for the default web site.	Sites > Default Web Site > RSAarcher > Authentication

Task 2: Validate Web Server folder access

This test verifies that Network Service user account has access to the logging folder, the file repository folder, and the company_files folder. The paths to the file repository and logging folders are set in the General tab of the instance in the RSA Archer Control Panel. The path to the company_files folder was set during the installation of the RSA Archer Platform component.

1. Open a Microsoft Explorer window.
2. Navigate to the logging folder. The default path is:

   C:\Program Files\RSA Archer\Logfiles
3. Right-click the logging folder and click Properties.
4. Click the Security tab.
5. Select the Network Service or domain service account and verify that Modify is selected in the Permissions box.
6. Click OK.
7. Repeat steps 1 – 6 for the file repository folder. The default path is:

   C:\Program Files\RSA Archer\FileRepository
8. Repeat steps 1 – 6 for the company_files folder. The path to this folder was set during the installation process. The default path is:

   C:\Inetpub\wwwroot\RSA Archer\company_files

Validating Client Settings

Task 1: Validate the Silverlight version

This task applies to computers running either Windows or Mac (MacOS) operating system.

Complete the task for your operating system:

Windows Operating System	MacOS
1. In Control Panel, open the Programs and Features. 2. Locate the Microsoft Silverlight row. 3. In the Version column, verify the version.	1. In Finder, display /Library/Internet Plug-Ins. 2. Press control and click the Silverlight.plugin, then select Show package contents. 3. Display the Contents/Resources folder and double-click Silverlight.Preferences.app. 4. Verify the version.

Task 2: Validate browser settings

Ensure your browser security settings allow downloads and pop-ups for RSA Archer.

For more information, review your browser's documentation and consult to your IT department.

Important: If you do not enable downloads and popups in your browser, the Export feature may not function properly. A security message may display when using the Export feature.

Troubleshooting RSA Archer Advanced Workflow

This section assumes that you selected advanced workflow as part of your installation.

If you cannot access the advanced workflow functionality in the Application Builder or your test workflow fails, use the following tasks to troubleshoot the Advanced Workflow service installation and configuration.

Note: Most of these tasks require access to the server on which RSA Archer Advanced Workflow service was installed. If you do not have access, contact your system administrator.

Advanced workflow installation overview

Advanced workflow runs as a Windows service with other services on a Web Server. Alternatively, you can dedicate a Web Server to advanced workflow.

In a new installation, the following occurs:

1. The Advanced Workflow service is installed.
2. The service communicates with the Configuration service to get instance settings and updates the workflow server configuration with the settings.
   Advanced workflow is ready to communicate with the Web Application.

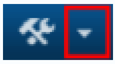
Advanced workflow suggested settings

Advanced workflow runs as a Windows service with other services on a Web Server or Services Server. Alternatively, you can dedicate Services Server to advanced workflow. The process occurs during install. In a new installation, the following Application Request Routing cache settings populate in the IIS:

Field	Value
Enable Proxy	Selected
HTTP Version	Pass through
Keep alive	Selected

Field	Value
Time-out (seconds)	120
Reverse rewrite host in response headers	Selected
Preserve client IP in the following header	X-Forwarded-For
Include TCP port from Client IP	Selected
Memory Cache duration (seconds)	60
Enable disk cache	Selected
Query string support	Ignore query string

Troubleshooting process overview

Step	Question to answer	How to find out	Result	Action
1	Can Microsoft Internet Information Services (IIS) communicate with the Advanced Workflow service?	a. Log in to RSA Archer. b. From the menu bar, click . c. Under Advanced Workflow, select Job Troubleshooting.	If the page loads, the test passed.	Go to step 2.
			If the page does not load or renders an error page, the test failed.	Go to Troubleshoot communication.

Step	Question to answer	How to find out	Result	Action
2	Is the Advanced Workflow service running?	Open the Windows service Control Manager and see if the RSA Archer Advanced Workflow service is running.	The service is running.	Go to Troubleshoot the Advanced Workflow application server deployment.
			The service exists, but is not running.	Start the service.
			The service does not exist.	Go to Troubleshoot the Advanced Workflow service.

Troubleshoot the communication between IIS and the Advanced Workflow service

1. Open IIS Manager and, at the global server level, verify that the Application Request Routing module exists. If the module does not exist, do the following:
   a. Reboot your system. See if the module now exists.
   b. If that does not work, repeat the installation. On the RSA Archer Platform - Installation Options page, verify that only Advanced Workflow Service is selected.
2. Open the Application Request Routing module.
3. In the Cache Setting section, verify that Enable Disk Cache is selected. If not, select it and click Apply.
4. In IIS, verify that the WebDAV feature is disabled for your Archer site. If it is enabled, disable it. RSA Archer does not support the WebDAV feature.
5. Open Archer Control Panel. Navigate to the Install Settings page and the Advanced Workflow frame. Ensure the Workflow Host or Load Balancer URL match the values used for Advanced Workflow REST URL and Advanced Workflow Communication Port during the installation process.
6. If you are encrypting advanced workflow, verify that a dedicated certificate was imported properly into the local machine's personal store. See Preparing Encryption for RSA Archer Advanced Workflow for more information.

Troubleshoot the Advanced Workflow Service

1. Verify that the Advanced Workflow service was created:

   C:\Program Files\RSA Archer\Services\ArcherTech.Services.WorkflowService.exe
2. Verify that the following directory was created:

C:\Program Files\RSA Archer\Services\Workpoint

3. If any of the above were not created, repeat the installation.

Troubleshoot the Advanced Workflow application server deployment

1. In the Task Manager, verify that the following are running:
   - WpAsyncMonitor.exe
   - WpEventMonitor.exe
   - WpGeneralMonitor.exe
   - WpJobMonitor.exe
   - WpServiceHost.exe
2. Check the service wrapper log file for errors in the file C:\ArcherFiles\Logging\Archer.ArcherTech.Services.WorkflowService.*date*.xml.
3. If you have enabled logging in the RSA Archer Control Panel, open C:\ArcherFiles\Logging and check whether or not the ArcherAdvancedWorkflow.xml file exists. If it does not, contact Support.

Note: C:\ArcherFiles is a configurable field in the ACP. For more information see the ACP documentation.

Troubleshoot high-availability or load-balanced environment

While using a high-availablity or load-balanced environment, one of the servers running advanced workflow fails, all calls in progress are interrupted and rerouted to another available host. In addition, new calls go through the new host. This protects users.

If a failure occurs, while running a data feed, check the data logs for any lost information. View the data feed results log, Archer.ArcherTech.DataFeed.log in the directory set during installation.

Sometimes the Job Framework response time is too fast for the load balancer. To extend that time, alter the ArcherTech.JobFramework.exe.config or web.config files according to the error listed in following chart:

Error Encountered	Setting	Description
Advanced workflow HTTP request error, attempt X. The operation will be retried in X milliseconds.	wpRetryAttemptsOnFailure	The number of times to retry a failed connection to the Workpoint API before stopping (default is 5).

Error Encountered	Setting	Description
Advanced workflow HTTP request error.	wpRetryDelayMillisec	How many milliseconds to wait between attempts at API calls to Workpoint (default is 2000).

Troubleshooting Cache

When working with Cache, it is important to understand the following:

File or Process	Description
ArcherTech.JobFramework.Cache.exe	This service minimizes the number of database calls that the job engine makes to the SQL server. **Note:** While this service has cache in the name, it is not involved with the caching process. Do not enable or disable this service as part of your caching set up process.

Appendix A: Additional Configuration Options

Time Zones

During the initial installation, you must establish the default time zone for RSA Archer. This time zone becomes the default time zone for all instances and users unless you override it. You can override the default time zone in any instance (in the RSA Archer Control Panel) or for any user (in the User Profile of RSA Archer).

The default time zone is stored in RSA Archer as Coordinated Universal Time (UTC). RSA Archer uses this time standard for converting time and dates based on the instance or user locale. All time is stored as UTC and converted based on the time zone of the user.

Each user account has a time zone associated with it. RSA Archer uses this time zone to standardize dates and times entered by a user. When a date field includes the time component, it uses the time zone to store the date and time in the database as UTC and displays it to other users based on the time zone associated with the User Profile of the other user.

All values for date fields entered in RSA Archer reside in the database as UTC. However, the Display Control type determines how RSA Archer handles time.

- For Date only, RSA Archer truncates the time.
- For Date and Time, RSA Archer converts the time based on the time zone associated with the user profile.

Example: Date only

The following table describes the example scenario, action, and result.

Scenario	User 1 is in time zone (UTC-6:00) Central Time (US & Canada). User 2 is in time zone (UTC+5:30) Chennai, Kolkata, Mumbai, New Delhi.
Action	User 1 enters the date 11/14/2017 in record A. The date is stored in the database as 11/14/2017 00:00:00 UTC.
Result	User 2 accesses record A and sees 11/14/2017 as the date. Because the field is Date only, the time is truncated and is shown to the user as the date stored without time.

Example 2: Date and time

The following table describes the example scenario, action, and result.

Scenario	User 1 is in time zone (UTC-6:00) Central Time (US & Canada). User 2 is in time zone (UTC+5:30) Chennai, Kolkata, Mumbai, New Delhi.

Action	User 1 enters the date 11/14/2017 and the time 10:13 P.M. in record A. The date and time are converted based on the time zone of user 1. As a result the date and time are stored in the database as 11/15/2017 04:13:00 UTC.
Result	User 2 accesses record A and sees 11/15/2017 9:43:00 A.M. Because the field is Date and Time, the date and time are converted from UTC to the time zone of user 2.

Data feeds and calculated fields use UTC. Consider a calculated field with the DATEFORMAT function with Example 2, the date and time is displayed as 8/15/2012 04:13:00 UTC for all users regardless of their time zone. The date and time are stored in a text field. When the date and time is stored in a text field, the data is not converted because RSA Archer recognizes the date as text only.

The DATEFORMAT(NOW(),"yyyy-MM-dd hh:mm tt") function displays the current date and time in UTC in the format you want. If you want to store it in a Date Field with time enabled, convert the literal to a date time serial value.

DATETIMEVALUE(DATEFORMAT(NOW(),”yyyy-MM-dd hh:mm tt”)) displays the current date and time converted from UTC to the current time zone of the user because the data is being displayed in a Date field with time enabled.

A time zone is required when creating schedules to run processes like data feeds and scheduled recalculations. If the time zone is not specified, the default time zone for the instance is used. This time zone is set up in RSA Archer Control Panel during the initial installation. For more information, see the RSA Archer Control Panel Help.

X.509 Certificates

The installation process requires an X.509 certificate. RSA Archer uses this certificate for authentication between the Web Application and Archer services.

You can create a new certificate during the initial installation of RSA Archer. The certificate is named RSA Archer Configuration and saved in the Personal area of the certificate store. Export this certificate for use in future installations. You must always use the same certificate in subsequent installations.

You can change the certificate later. To change the certificate after installation, rerun the installer, select only Web Application and Services, and then select the Use a different certificate option.

If you already have an X.509 certificate, determine its location and provide that information when requested during the installation.

Installation Options

During a new installation, RSA Archer prompts you to either create an X.509 certificate, import an existing certificate, or select an existing certificate already in the certificate store. RSA recommends creating a new X.509 certificate for all new installations unless you have an existing certificate.

Create a certificate

Create the RSA Archer Configuration certificate and save it in the Personal store of the certificate store. If you choose to create a new certificate, the new certificate does not interfere with other certificates in IIS, such as an SSL certificate. Make a note of this certificate so that you can use it during the installation. The new X.509 certificate has the following parameters:

Parameter	Value

Issuer	CN = RSA Archer Configuration
	O = RSA Archer

Subject	CN = RSA Archer Configuration
	O = RSA Archer

Valid to	December 31, 2039
Signature algorithm	sha512RSA
Private key	RSA (1024-bit)

Select from disk

Designates an existing certificate not yet imported into the certificate store. If you select to import a certificate, you must select the file in which the certificate is located and provide the password to the private key.

Select from certificate store

Designates an existing certificate from the certificate store.

Configuration Service Authentication

The RSA Archer Control Panel and Archer Web Services authenticate to the Archer Configuration Service using the X.509 certificate. During installation, RSA Archer allows you to do the following:

- Use an existing X.509 certificate, for example, one issued and signed by your Root CA. RSA recommends that you use a domain certificate or a certificate signed by an external CA and generated in accordance to industry best practices.
- Have the installer generate an X.509 certificate for you. In this case, the installer generates a self-signed certificate.

The X.509 certificate used for authentication to the RSA Archer Configuration service does not interfere with other certificates used within IIS, such as your SSL certificate.

Export the X.509 Certificate

Complete this task to export the initial certificate for use in future installations. The same X.509 certificate must be used for all subsequent installations.

Begin at the server where the certificate was created.

1. Click Start > Run > MMC.
2. Select File > Add/Remove Snap-ins.
3. From the Available Snap-ins list, select Certificates and click Add.
4. Select Computer Account and click Next.
5. Select Local Computer and click Finish.
6. Click OK.
7. Expand Certificates > Personal folder. Right-click RSA Archer Configuration and select All Tasks > Export. The Certificate Export Wizard starts.
8. Select Yes, export the private key and click Next.
9. Select Personal Information Exchange - PKCS #12 (PFX) format.
10. Select Export all extended properties and click Next.

11. Designate a password to protect the private key, and select a local directory in which to export the certificate.

Configuring a Load Balancer for RSA Archer

This section describes the process for installing and configuring RSA Archer in a high-availability, multiple-server configuration using a load balancer to distribute load based on server availability. The target audience is RSA Archer administrators installing RSA Archer and anyone responsible for managing and configuring RSA Archer servers.

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers increase capacity for concurrent users and reliability of applications.

Because session state and ViewState information needs to be shared between the Web Servers, a mechanism must also be provided to ensure this information can be processed by any web farm server. The server is configured through the Machine Key option of the RSA Archer site, which is added to the web.config file in the Web Application directory of each Web Server.

Alternatively, the global machine.config file can be modified.

Requirements for a load-balanced installation

- An Active Directory domain account to configure access shared file server resources.
- A file share that hosts common RSA Archer files and access to the domain account set to Modify Access.
- All web servers are configured to use the same X.509 certificate.
- All services are configured to use the same account with the installer to configure the correct permissions.
- All servers containing IIS and Advanced Workflow Services must be able to communicate through port 8000.

Note: The permissions on the X.509 Certificate used by the web and application servers grant the Active Directory domain account read access to the private key.

Installation process

1. Plan for installation.
2. Install the RSA Archer.
3. Update the web.config file on Web Servers.
4. Configure load balanced URL on software or hardware load balancer.
5. Verify RSA Archer can be accessed via the load balanced URL.
6. Test the installation.

Task 1: Preparation

Before configuring the Web Servers for load balancing, complete the following:

1. Verify that load balancer, application, and database servers are located on the same local area network.
2. Verify that you have the Platform installation package.
3. Verify that you have administrative access for all applications and Web Servers that will host the GRC Platform.
4. Create an X.509 Certificate to be used for authenticating to the configuration service from the Web Application and RSA Archer Services. The certificate may be a new or existing organizational X.509 Certificate, or you may elect to self-generate it as part of the installation process.
5. Generate a common Machine Key to be used by IIS on all web farm servers.
6. Set up an Active Directory domain account for impersonation purposes, and configure a UNC-accessible SMB file share accessible by all servers running RSA Archer application code. These servers are used to host common files such as search indexes, file repository, and company files.
7. Configure least-privilege permissions on a file system and shared directory structures, which will host common files and verify that the Active Directory domain account has appropriate access to the network share.
8. Modify the identity of the application pool used by the RSA Archer web and application services for the Active Directory domain account configured above.

Task 2: Install RSA Archer

Complete the installation process as described in Chapter 4: "Installing RSA Archer".

Task 3: Generate the machineKey

The format of the Machine Key setting appears as follows:

```
<machineKey

validationKey="some long hexadecimal value"

decryptionKey="another long hexadecimal value"

validation="SHA256"/>
```

1. Start IIS manager on one of the Web Servers being configured for load balancing.
2. From the Sites node, select the RSA Archer site, and double-click the Machine Key applet.
3. On the Machine Key page, do the following:
    a. Set the values of the following parameters. For information on the values see https://technet.microsoft.com/en-us/library/hh831711(v=ws.11).aspx.

- Encryption Method
- Decryption Method

b. In the Validation Key and Decryption Key sections, clear any selected options.

c. In the actions panel, select Generate Keys.

4. In the Actions panel, click Apply to save the generated keys to the web.config file.

   The generated keys appear in the Validation key and Decryption key sections.

5. For all subsequent Web Servers, do the following:

   a. Copy the generated key values from the Validation key and Decryption key sections.

   b. At the other Web Servers, repeat steps 1 - 3b to generate the machineKey.

   c. Paste the values from the generated machineKey into the respective Validation key and Decryption key boxes on the Machine Key page.

   d. In the Actions panel, click Apply.

Task 4: Test the load balanced URL

1. Verify whether you can access RSA Archer through the load balanced URL.
   Common problems that may occur post-configuration include dashboards not displaying correctly or file-repository access failing. If either condition occurs, access each Web Server individually from your browser instead of using the load-balanced URL to identify which systems may be having issues.

2. Verify the following:

   - The IIS application pool is configured to run under the correct Active Directory domain account credentials.
   - The Machine Key setting in the web.config file matches the applicable Validation key and Decryption key values.

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.

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
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

Application Pool Requirements

An application pool is required for administrating the RSA Archer Web Application. The application pool defines the set of Web Applications that share one or more worker processes, which are Windows processes that run Web Applications.

Required values for configuring the application pool

Property	Value
Application Pool Name	[user defined]
.NET CLR version	.NET CLR 4.0
Start application pool immediately	Select this checkbox

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

Component	Location
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 "Configuring the Web Server".

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

Cloud and Hosting Support

RSA Archer supports hosting in Microsoft Azure® and Amazon Web Services® (AWS) cloud environments. This section provides information to assess and plan for an installation using cloud environments.

When using Cloud vendors, RSA only supports using virtual machines to run your RSA Archer environment.

Use the same process for a cloud or hosted environment as outlined in the *RSA Archer Platform Planning Guide* to determine your environment size. Choose a product from your cloud provider that most closely matches your configuration requirements.

For example, consider the specifications for a small environment given in *RSA Archer Platform Planning Guide*. As of this publication, the details in this table are accurate based on current vendor specifications.

Element	Small Environment	AWS (m4.xlarge)	Azure (Standard_ DS3 package)
Processor	Four cores	Four cores	Four cores
Memory	16 GB	16 GB	14 GB
Disk Space	50 GB HDD	100 GB SSD (Using Elastic Block Store)	100 GB HDD

Note: This table describes hardware requirements only. To understand all requirements for your configuration, see "Sizing Guidelines" in the *RSA Archer Platform Planning Guide*.

There are some factors to consider when preparing your cloud based configuration:

- Input/Output per second (IOPS) directly affects your RSA Archer performance. If you find your performance is slow, consider choosing a vendor product with more IOPS per disk.
- Communication between your on-premises systems and your cloud vendor is key. Contact your vendor to select a method that works best for your environment.

For more information about the different vendor products offered, review the Azure and AWS documentation:

- For Azure, see https://docs.microsoft.com/en-us/azure/.
- For AWS, see https://aws.amazon.com/.

Search Plug-In for Elasticsearch

If Elasticsearch is used as a search provider, then keyword and global search will return results only if the RSA Archer-provided search plug-in is installed in all nodes of the Elasticsearch cluster. The provided plug-in can be found in the installed tools directory of your RSA Archer system in the following location: <BuildName>\support\Tools\join-search-plugin.0.0.1\.

To install the plug-in on an Elasticsearch node, use the following command:

```
elasticsearch-plugin install "file:///<FILEPATH>"
```

For example, elasticsearch-plugin install "file:///C:\join-search-plugin-0.0.1.zip"

To remove the plug-in, use the following command:

```
elasticsearch-plugin remove join-search-plugin
```

For more information about configuring Elasticsearch, see "Enabling Elasticsearch" in the RSA Archer Control Panel Help.

Geocoding

If your environment uses geocoding, configure geocoding for RSA Archer. Three geocode keys are included in the Web Configuration file.

The following table describes each geocode key.

Geocode Key	Description
numberOfParellelGeocodingThreads	The number of parallel threads created to keep geocoding running. By default, the value is 10.
GeoCodeChunkSize	The number added to the payload size for the network traffic from the RSA Archer Client and the RSA Archer Server. When the value is high, each requested geocode payload size is high. When the value is low, each requested geocode payload size is low. The number of the geocodes that must be added. By default, the GeoCodeChunkSize value is 100.

Geocode Key	Description
numberOfGeoCodingTrials	The number of attempts you allow RSA Archer to geocode addresses. By default, the value is 3.

Task 1: Configure the Web Configuration file

1. Open the web.config file from the following folder:

   \inetpub\wwwRoot\IIS_App_Name

   Note: The default name is RSAarcher.

2. Verify the geocode key values.
3. If you updated geocode values, reset IIS.
   a. Go to Start > Run.
   b. In the Open field, enter the following:

      iisreset.exe

   c. Press Enter.

Task 2: Configure geocoding proxy in the RSA Archer Control Panel

In the RSA Archer Control Panel, add the port and address of the proxy server that allows traffic from the following URLs:

- http://dev.virtualearth.net/REST/v1/
- https://dev.virtualearth.net/REST/v1/

For more information about configuring Maps, see "Registering Your Bing Maps Account for Whitelisting IP Addresses for an Instance" in the RSA Archer Control Panel help.

Task 3: Configure geocoding on the Web Server

Verify that the web server has one or both of the following:

- Internet connection
- Geocoding proxy

Appendix B: Test Environment

Test Environment Configuration Requirements

RSA recommends the latest version of the software listed for running RSA Archer in a single-server configuration. All components except the database run on a dedicated Web Server. RSA recommends using this configuration only for running a test environment of RSA Archer.

A test environment configuration does not require a high-performance or high-availability solution.

Component	Recommended Software
Operating System	Microsoft Windows Server 2012 R2 or 2016 Standard or Datacenter editions
Database	Microsoft SQL Server 2016 SP 1 (64-bit) or 2016 Enterprise Edition (64-bit) or 2017 (64-bit) SQL Express is not supported
Web and Services	Microsoft Internet Information Services (included in Microsoft Windows Server 2012 R2 or 2016 Microsoft Office 2010 or 2013 Filter Packs (to enable indexing of MS Office files) Requires Microsoft Filter Pack 2.0 or later. Microsoft Sync Framework 2.1 (for offline access)

For instructions on installing RSA Archer on a single server, see Installing All Components on a Single Server. The following figure illustrates a single-server configuration.

Server	File Server	Database Server
• Web Application • Services	• Company_files • File repository • Services	• Instance databases • Configuration database

Installing All Components for a Test Environment

You can install RSA Archer in a single-server configuration. This configuration is only suitable for an environment that does not require a high-performance or high-availability solution, for example, a test environment.

Task 1: Prepare the installer package

1. Download the RSA Archer 6.7 installer package from RSA Link.

   https://community.rsa.com/community/products/archer-grc/archer-customer-partnercommunity/

2. Use the Run as Administrator option to extract the installation package on the server to a location that is accessible to other servers.
3. Back up the instance and configuration databases created during the server preparation process. This process ensures that your data is current so that you can recover it if necessary.

Task 2: Run the installer

Run the installer on all web and services servers.

1. Open the installation folder, and right-click ArcherInstall.exe.
2. Select Run as Administrator.
3. Click OK to run the installer.
4. Select the appropriate language for the installer to use.
5. Read the license agreement, and select I accept the terms in the license agreement.
6. Read the Diagnostics and System Data License.
7. Click Next.

Task 3: Install all components

In addition to installing all components, this installer establishes the connectivity to the instance database that typically resides on a different server.

Begin at the RSA Archer Platform - Installation Options page.

1. Verify that only desired components are selected.

   Note: Make sure to select the same components previously installed before running the upgrade. If running the installer against a specific component is required, ensure that the other components installed on the same server are also selected—otherwise, the installer will uninstall them.

   Unselecting the Services component results in all installed services except for the Configuration Service and Advanced Workflow Service being uninstalled. Unselecting the Advanced Workflow Service results in that service being uninstalled.

   - Web Application
   - Services
   - Instance Database
   - Advanced Workflow

2. Click Next.

Task 4: Specify the X.509 certificate

Important: You must use the same X.509 certificate during installations on all types of servers. For more information, see X.509 Certificates.

Begin at the RSA Archer Platform - Specify Certificate page.

1. In Specify where to obtain the X.509 certificate, do one of the following:
   - Select Create a certificate to create a new certificate.
   - Select an existing certificate from a disk or a certificate store.
     - If selecting from a disk, follow these steps:
       a. Choose Select from disk.
       b. In Specify the file to import into the certificate store, click ... to display a Windows Explorer Open File window, and then navigate to the location of the certificate file.
       c. Select the file, and click OK.
       d. In Type the password for the private key, enter the applicable certificate password.
     - If selecting from a certificate store, follow these steps:
       a. Choose Select from certificate store.
       b. In Select a certificate from the store, expand the category and select the certificate.
2. Click Next.

Task 5: Set the configuration database options

Complete this task only if prompted during the installation process. If the installer detects the RSA Archer Configuration service, the RSA Archer Platform - Configuration Database Options page does not display.

Begin at the RSA Archer Platform - Configuration Databases Options page.

1. In SQL Server, enter the SQL Server that hosts the Configuration Database.
2. If you are using a SQL Server account, enter the following, otherwise go to step 4.
   - Login name
   - Password
3. If you are using integrated security complete the following, otherwise go to step 4.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
4. In Database, enter the Configuration Database.
5. Click Next.

Task 6: Configure Advanced Workflow HTTPS

Begin at the RSA Archer Platform - Specify HTTPS Binding Certificate page.

Note: Advanced workflow requires a dedicated certificate.

1. Enter the port to securely communicate with the Advanced Workflow Service in HTTPS Port.
2. Do one of the following:

   Note: The port numbers for Advanced Workflow REST URL and Advanced Workflow Communication Port cannot be the same when using HTTPS. For example by default, the Advanced Workflow REST URL default port is 8443 and the Advanced Workflow Communication default port is 8000.

   - Use HTTPS
     - Specify where to obtain the X.509, by doing one of the following:
       - If using current certificate, select Use current certificate.

         Note: This option is unavailable, if this is the first installation for your configuration.
       - If selecting from a certificate store, follow these steps:
         a. Select from certificate store.
         b. In Select a certificate from the store, expand the category and select the certificate.
     - Specify the HTTPS Port

       Note: If the system detects the specified port number is in use, you must confirm you wish to replace the certificate bound to the specified port.

- Use HTTP only (Not recommended)

3. Click Next.

Task 7: Set the REST URL and Communication Port for Advanced Workflow service

Begin at the RSA Archer Platform Advanced Workflow Settings page.

1. If using HTTP, click Next.

   Note: During HTTP, the RSA Archer uses default ports and URLs.

2. If using HTTPS, do the following:

   a. Change Advanced Workflow REST URL to the same value specified when configuring Advanced Workflow HTTPS. For example, https://hostName:8000/ where hostName is the fully qualified domain name of the host where the Advanced Workflow Service is installed. If there are multiple Advanced Workflow Service hosts, hostName is the DNS name for the load balancer and the port number refers to the port for which you have configured the load balancer.

   b. Change the Advanced Workflow Communication Port to a different port than you specified when configuring Advanced Workflow HTTPS. (The default value is 8000.)

      Note: If this is a new install, the system populates this field with information from the certificate and HTTPS port used to configure Advanced Workflow HTTPS.

   c. Click Next.

Task 8: Select the RSA Archer language

If you did not check the Instance Database box in Task 6, this task is skipped automatically.

Begin at the RSA Archer Platform Language page.

1. In Select the language for RSA Archer Platform, select the language that you want to use for RSA Archer. By default, the language is US English. The supported languages are English (US), Chinese, French, German, Italian, Japanese, Portuguese (Brazil), and Spanish.
2. Click Next.

Task 9: Set the instance database options

Begin at the RSA Archer Platform - Instance Database Options page.

1. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
2. If you are using a SQL Server account, enter the following, otherwise go to step 4.
   - Login name
   - Password
3. If you are using integrated security complete the following, otherwise go to step 4.
   a. Select User integrated security.
   b. In Database, enter the instance database.
4. Click Next.

Task 10: Set the default time zone

This time zone for the configuration database applies to all instances unless you override it for a specific instance in the RSA Archer Control Panel.

Note: If the installer detects a time zone, it does not prompt you to set the default time zone, and the Web Application Options page opens; skip this task.

Begin at the RSA Archer Platform - Time Zone page.

1. In Time Zone, select the default time zone for RSA Archer.
2. Click Next.

Task 11: Configure the Web Application options

Begin at the RSA Archer Platform - Web Application Options page.

1. In Website, select the destination site for the RSA Archer Web Application.
2. Under Destination directory, verify that destination directory is set to the Web Application installation:
   - Install in the website's default application.
   - Install in an IIS application.

3. Click Next.
4. Click Yes to confirm the destination directory.

Task 12: Enable HTTPS automatically for communication between Web Servers and web traffic

If prompted, begin at the RSA Archer Platform - Specify HTTPS Binding Certificate page.

1. Do one of the following:
    - Use Existing Binding
    - Create New Binding
        - Specify where to obtain the X.509, by doing one of the following:
            - If selecting from a disk, follow these steps:
                a. Select from disk.
                b. In Specify the file to import into the certificate store, click ... to display a Windows Explorer Open File window, and then navigate to the location of the certificate file.
                c. Select the file, and then click Open.
                d. In Type the password for the private key, enter the applicable certificate password.
            - If selecting from a certificate store, follow these steps:
                a. Select from certificate store.
                b. In Select a certificate from the store, expand the category and select the certificate.
2. Click Next.

Important: RSA recommends removing any existing HTTP binding from IIS to ensure secure configuration.

Task 13: (Optional) Set the instrumentation service database options

If you are using Message Logging or other event logging, enter the connections to the instrumentation database. RSA recommends using a dedicated database and not the instance or configuration database for this purpose.

Begin at the RSA Archer Platform - Instrumentation Database Options page.

1. Specify the setting for the Not using RSA Archer Instrumentation service option:
   - If you do not want to use the service, select the option (default). Go to step 5.
   - If you want to use the service, clear the option. Go to step 2.
2. In SQL Server, enter the server name.
   If the SQL Server is configured for a custom port, enter [servername],[portID].
3. If you are using a SQL Server account, enter the following, otherwise go to step 5.
   - Login name
   - Password
4. If you are using integrated security complete the following, otherwise go to step 5.
   a. Select User integrated security.
   b. In Database, enter the Instance Database.
5. Click Next.

Task 14: Configure the service credentials

Begin at the RSA Archer Platform - Services Credentials page.

1. Select
   - Use the Local System account to run all services.
   - Use the specified account to run all services and provide Account Credentials.
2. Click Next.

Note: To allow correct RSA Archer Services installation, ensure that Log on as a Service is enabled for the Window Services Account.

Task 15: Set the services and application file paths

Begin at the RSA Archer Platform - Services and Application Files page.

1. In Services, enter the path where the services are installed.
   By default, the path is C:\Program Files\RSA Archer\Services.
2. In Application Files, enter the path where the application files are installed.
   By default, the path is C:\Program Files\RSA Archer.

> **Note:** RSA recommends that you do not install Web Application or products in the same virtual directory or Root of Archer. Browsers send Cookies if more than one Web Application resides in same space; this behavior may lead to passing Archer cookies to any other application installed in same Root or Virtual Directory.

3. In Program Group, select one of the following options, and click Next.
   - Create RSA Archer program group for the current user only
   - Create RSA Archer group for all users (Recommended)
   - Do not create RSA Archer program group
4. Click Next.
5. Click Yes to confirm the newly created directories and program group.

Task 16: Set the log file path

Begin at the RSA Archer Platform - Log Location page.

1. In Log Path, enter the folder in which you want to store the log files. All servers in the RSA Archer environment use this path for logging events. When setting this path, use the same path for all web and services servers.
2. Click Next.

Task 17: Perform the installation

Begin at the RSA Archer - Perform Install page.

1. Click Next.
   The installer starts installing the applicable components. A progress bar opens.
2. Wait for the installer to complete installing the applicable components.
3. Click Finish.
   The RSA Archer Control Panel opens.

Appendix C: Qualified and Supported Environments

RSA recommends the latest qualified versions of specific software for running RSA Archer in the recommended configuration. For more information, see RSA Archer 6.6 and Later - Qualified and Supported Environments.

Appendix D: Checklists and Worksheets

Preparation Checklist

This checklist is for a new installation and is provided for your convenience.

Prepare the Database Servers			
See Preparing the Database Server for information on completing each task.			
❑	Task 1: Verify Database Requirements		
❑	Task 2: Choose Authentication Method		

Prepare the Web Servers			
See Preparing the Web Servers for information on completing each task.			
❑	Task 1: Verify Web Server Requirements		
❑	Task 2: Configure IIS		
❑	Task 3: Verify Application Pool Requirements		
❑	Task 4: Confirm User Account		

Prepare the Services Servers			
See Preparing the Services Server for information on completing each task.			
❑	Task 1: Verify Services Server Requirements		
❑	Task 2: Configure Network Share		
❑	Task 3: (Optional) Configure Keyword Indexing for Attachments		
❑	Task 4: Configure Message Logging		

Installation Checklist

You must perform all new installations on the designated servers for the web and services roles. If you are upgrading RSA Archer from an earlier version, please see Upgrading RSA Archer.

Run this installation on each web and Services Server. See Installing the Web Application and Services Components for more details.

Install the Web Application and Services Components			
□	Task 1: Prepare the installer package		
□	Task 2: Run the installer on all Web servers and Services servers		
□	Task 3: Install the Web Application, and services		
□	Task 4: Specify the X.509 certificate		
□	Task 5: Set the configuration database options (if prompted)		
□	Task 6: Configure Advanced Workflow HTTPS		
□	Task 7: Set the REST URL and Communication Port for Advanced Workflow service		
□	Task 8: Select the language for RSA Archer and content (if prompted)		
□	Task 9: Set the instance database		
□	Task 10: Set the default time zone for the configuration database		
□	Task 11: Configure the Web Application options		
□	Task 12: Enable HTTPS automatically for communication between Web Servers and web traffic		
□	Task 13: (Optional) Set the instrumentation database options for message logging		
□	Task 14: Configure the service credentials		
□	Task 15: Set the services and application file paths		
□	Task 16: Set the path for the installer log file		
□	Task 17: Perform the installation		

Install the Web Application and Services Components			
❑	Task 18: In the RSA Archer Control Panel, set the instance database options		
❑	Task 19: Stop all RSA Archer services except RSA Archer Configuration service		

Run this installation on each Services Server. See Installing the Services for more details.

Install the Services Component			
❑	Task 1: Prepare the installer package		
❑	Task 2: Run the installer as administrator		
❑	Task 3: Install the Services component		
❑	Task 4: Specify the X.509 certificate		
❑	Task 5: Set the configuration database options		
❑	Task 6: Set the default time zone for the configuration database		
❑	Task 7: (Optional) Set the instrumentation database options for message logging		
❑	Task 8: Configure the service credentials		
❑	Task 9: Set the services and application file paths		
❑	Task 10: Set the path for the installer log file		
❑	Task 11: Perform the installation		

Upgrade Installation Checklist

This checklist is for a upgrade installation and is provided for your convenience.

You may perform upgrades on all components at once or on individual components separately. If you are installing RSA Archer on a fresh system, please see Installing RSA Archer.

Run the upgrade on all web and Services Servers. Refer to Upgrading All Components for details.

Upgrade all Components			
❑	Task 1: Prepare the installer package		
❑	Task 2: Stop all RSA Archer Jobs		
❑	Task 3: Stop all RSA Archer services except RSA Archer Configuration service		
❑	Task 4: Shut down RSA Archer		
❑	Task 5: Run the installer as Administrator		
❑	Task 6: Install all components		
❑	Task 7: Choose the x.509 certificate from store		
❑	Task 8: Configure Advanced Workflow HTTPS		
❑	Task 9: Set the REST URL and Communication Port for Advanced Workflow service		
❑	Task 10: Select the language for RSA Archer and content		
❑	Task 11: Set the instance database options		
❑	Task 12: Configure the Web Application options		
❑	Task 13: (Optional) Set the instrumentation database options for message logging		
❑	Task 14: Set the configuration services credentials		
❑	Task 15: Set the services and application paths		
❑	Task 16: Set the path for the installer log file		
❑	Task 17: Acknowledge configuration changes for installs that include Advanced Workflow		
❑	Task 18: Perform the installation		
❑	Task 19: Start IIS on all Web Servers		
❑	Task 20: Verify the instance configuration		

Run the upgrade on Services Servers only. Refer to Upgrading the Services Servers for details.

Upgrade Services Servers only			
❑	Task 1: Prepare the installer package		

Upgrade Services Servers only			
❑	Task 2: Stop all RSA Archer Jobs		
❑	Task 3: Stop all RSA Archer services except RSA Archer Configuration service		
❑	Task 4: Shut down RSA Archer		
❑	Task 5: Run the installer as Administrator		
❑	Task 6: Install the services component		
❑	Task 7: Choose the x.509 certificate from store		
❑	Task 8: (Optional) Set the instrumentation database options for message logging		
❑	Task 9: Set the configuration services credentials		
❑	Task 10: Set the services and application paths		
❑	Task 11: Set the path for the installer log file		
❑	Task 12: Perform the installation		
❑	Task 13: Start IIS on all Web Servers		
❑	Task 14: Verify the instance configuration		

Run the upgrade on all Web Servers only. Refer to Upgrading the Web Servers for details.

Upgrade Web Servers only			
❑	Task 1: Prepare the installer package		
❑	Task 2: Stop all RSA Archer Jobs		
❑	Task 3: Stop all RSA Archer services except RSA Archer Configuration service		
❑	Task 4: Shut down RSA Archer		
❑	Task 5: Run the installer as Administrator		
❑	Task 6: Install the web components		
❑	Task 7: Choose the x.509 certificate from store		

Upgrade Web Servers only			
□	Task 8: Configure Advanced Workflow HTTPS		
□	Task 9: Set the URL for the Advanced Workflow service		
□	Task 10: Set the REST URL and Communication Port for the Advanced Workflow service		
□	Task 11: Select the language for RSA Archer and content		
□	Task 12: Configure the Web Application options		
□	Task 13: (Optional) Set the instrumentation database options for message logging		
□	Task 14: Set the services credentials		
□	Task 15: Set the services and application paths		
□	Task 16: Set the path for the installer log file		
□	Task 17: Perform the installation		
□	Task 18: Start IIS on all Web Servers		
□	Task 19: Verify the instance configuration		

Activation Checklist

This checklist is for configuring your servers after an installation or upgrade and is provided for your convenience. If you choose to document your installation, including passwords, secure the document so you can protect passwords and configuration settings by keeping them confidential.

See Configuring the Web Server for more details. These steps are performed in the Internet Information Services (IIS) manager, unless otherwise specified.

Configure the Web Server			
□	Task 1: Specify the account application pool identity		
□	Task 2: Assign the application pool		
□	Task 3: Verify application pool for the API		

Configure the Web Server			
❑	Task 4: Reconfigure the company_files directory as a virtual directory that is mapped to the network share		
❑	Task 5: Grant permissions to the RSA Archer directories		
❑	Task 6: At the command prompt, reset IIS		
❑	Task 7: Exclude folders from virus scanning		
❑	Task 8: Start the RSA Archer Configuration service		

See Configuring the Services Server for more details.

Configure the Services Server			
❑	Task 1: Verify the domain user account has access to network share and company_file directories on the network share		
❑	Task 2: Verify the X.509 certificate permissions		
❑	Task 3: Make the certificate revocation list accessible		
❑	Task 4: Start the RSA Archer services		

See Update the Task Management Application for more details.

Update the Task Management Application			
❑	Task 1: Login to RSA Archer with administrative access		
❑	Task 2: Update the permissions for the Assigned To field in the Task Management application.		

If you use Advanced Workflow, configure it accordingly. Review the following tasks and complete any that are applicable to your environment. See Configuring Advanced Workflow for more details.

(Optional) Configure Advanced Workflow			
❑	Task 1: Open HTTP on localhost for communication between the Advanced Workflow service and RSA Archer		
❑	Task 2: Run the Advanced Workflow service with a non-admin account		
❑	Task 3: (Optional) Enable Advanced Workflow in a load balanced environment		

(Optional) Configure Advanced Workflow			
❑	Task 4: Ensure Windows host registry key is valid		

Validation Checklist

Use this checklist to ensure that RSA Archer is operational and that you have validated key functionality. As with any system implementation, testing is vital. While this checklist helps you ensure basic functionality, RSA recommends developing a more robust test plan to meet your specific business practices.

This checklist is for verifying an installation or upgrade. It is provided for your convenience. If you choose to document your installation, including passwords, secure the document so you can protect passwords and configuration settings by keeping them confidential.

See Validating RSA Archer as a companion to this checklist.

RSA Archer Testing			
See Testing RSA Archer Elements for information.			
❑	Task 1: Open RSA Archer and log in		
❑	Task 2: Add and test a new application		
❑	Task 3: Test a keyword search		
❑	Task 4: Attach a file to a record	File Attachment	
❑	Task 5: (Optional) Test Advanced Workflow		
❑	Task 6: (Optional) If you had custom links in custom iViews before upgrading, test the links. If any links do not work, manually relink them.		

If the RSA Archer Login page does not open, use the following section to troubleshoot system components.

Validate Server Settings			
See Troubleshooting System Components for information.			
❑	Task 1: Validate IIS settings		
❑	Task 2: Validate Web Server folder access		

If the RSA Archer Login page does not open, use the following section to troubleshoot system components.

Validate Client Settings			
See Troubleshooting System Components for information.			
❑	Task 1: Validate the Silverlight version		
❑	Task 2: Validate browser settings		

Preparation Worksheet

This worksheet is for a new installation and is provided for your convenience.

Important: If you choose to document your installation, including passwords, secure the document so you can protect passwords and configuration settings by keeping them confidential.

For more information, see Preparing RSA Archer for Installation as a companion to the worksheet.

Details for Database Authentication			
❑	Credentials for Instance Database	Username: Password:	
❑	Credentials for Configuration Database	Username: Password:	
❑	(Optional) Credentials for Logging Database	Username: Password:	

Details for Windows Authentication			
❑	Credentials for Windows Server Administration	Username: Password:	

Activation Worksheet

This worksheet is for configuring your servers after an installation or upgrade and is provided for your convenience. If you choose to document your installation, including passwords, secure the document so you can protect passwords and configuration settings by keeping them confidential.

For more information, see Activation Process as a companion to the worksheet.

Verification Worksheet

Use this worksheet to track details throughout the verification process. Remember to secure your documents to protect passwords and configuration details.

❑	Default Instance name.	Instance name:	
❑	Instance database credentials	SQL Server: Login name: Password: Database:	
❑	File Repository path. This should be mapped to the network share.	Path:	
❑	Search Index path and Queuing server.	Search Index path: Queuing server:	
❑	Default From Address.	Email From address:	
❑	Base and authentication URLs.	Base URL: Authentication URL:	
❑	SysAdmin and Service Account passwords.	SysAdmin: Service Account:	
❑	Instance Serial Number ❑ Company information. ❑ Activation method	Serial Number: First name: Last name: Company: Automated Manual	
❑	Services account application pool credentials	User name: Password:	

Appendix E: User Requirements

Client Computers

The following list is the recommendations for users accessing RSA Archer on client computers.

Component	Description
Browser	Internet Explorer 11; Firefox 60ESR or 62; Safari 11
Miscellaneous	Microsoft Silverlight 5.1.3 (required for Administration.

For a list of supported third-party components in RSA Archer, see "RSA Archer Qualified and Supported Environments" in the RSA Archer Online Documentation.

Offline Access Requirements for the RSA Archer Audit Management Solution

To use offline access for the RSA Archer Audit Management solution, the client computers must meet the following recommendations:

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

RSA recommends that your client computers have dual CPU processors. The recommended disk space is conditional upon the amount of data you download to the client computer.

For installation instructions, see Installing Offline Access.

Appendix F: Uninstalling RSA Archer

This process removes RSA Archer and its associated data. It removes only the directories or files added by RSA Archer installer. However, it does not remove files added during configuration, such as repository files, keyword index files, and log files.

If you have installed the components on multiple servers, perform this task on each server.

Important: Do not perform this task if you are upgrading to a later version of RSA Archer. Run the installer to upgrade the RSA Archer components. Make certain that the ArcherInstall.exe file is in the same location it was when you installed RSA Archer. The unistall program needs to find this file and uses its original path. If the file is no longer there, the uninstall will not work.

Uninstall RSA Archer

1. From the Windows Control Panel, do one of the following based on the version of Windows you are running:
   - Click Add or Remove/Programs.
   - Click Programs and Features.
2. Do one of the following based on the version of Windows you are running:
   - Select either RSA Archer and click Change/Remove.
   - Right-click RSA Archer Platform and click Uninstall/Change.

   The Uninstall process starts and the Select Language dialog box opens.
3. Select the language for the installer. Click OK to continue. The Uninstall Options page opens.
4. Select the objects that you want to uninstall and click Next. The Perform UnInstall page opens.
5. Click Next to continue. The File Progress box opens while the uninstall is performed.
6. Wait a few minutes for the process to complete.
7. Click Finish. All selected objects are removed.
8. Delete the SQL databases from the database server.

Appendix G: Reconciling Advanced Workflow Apply Conditional Layout Action Changes

When upgrading from 6.0 and 6.1 to 6.2 or later, you must reconcile some changes made to advanced workflow. The following explains the process.

Reconciling Apply Conditional Layout Data-Driven Events

The 6.2 release affected advanced workflow action and user-initiated enrollment buttons. In previous releases, these buttons were layout objects, you could use Apply Conditional Layout (ACL) data-driven events (DDEs) to control when and to whom buttons were available. Starting in 6.2, you determine during configuration when a transition can be taken and who should have access to these buttons directly from the Advanced Workflow Process Designer.

Changes to each button type:

- Action buttons (transitions out of a User Action node): In release 6.2 and later, these buttons are always hidden unless actual permissions are granted through the transition. Permissions are determined when the record is loaded, which is consistent with how other objects in the system are permissioned. Rules never hide or disable buttons. Rules are evaluated when the button is clicked, and if the rule is not met, the transition is not taken and the content remains on the current node.
- User-initiated enrollment buttons: User-initiated buttons are still hidden to users who do not have permissions. Like action buttons, rules never hide or disable the button. Rules are evaluated when the button is clicked, and if the rule is not met, the content is not enrolled.
  - If only the New Records enrollment option is selected, the user-initiated button does not display for new records (that is, records that have not yet been saved). The button only appears for previously saved unenrolled records.
  - If only the Updated Records enrollment option is selected, the user-initiated button only displays on the edit page when the record has never been saved. The button never displays for previously saved unenrolled records.
  - If both the New Records and Updated Records enrollment options are selected, you cannot enable a User-Initiated button to enroll content.
  - If neither the New Records or Updated Records enrollment options are selected, the User-Initiated button will always display on the edit page for users who have permission to the button.

The button changes provide the following advantages:

- You can now reuse layouts
- Because transitions are versioned with the workflow, you can add or remove transitions from a User Action node without breaking existing jobs.
- Permission logic is now enforced at the middle tier, which means that other RSA Archer features, such as data feeds and APIs, must follow the permission logic set for workflow buttons.

When you install 6.2 or later, the system identifies those DDEs in your instance that are associated with advanced workflow layout objects, removes the layout objects, and writes the results to the DDE log file. After installing 6.2 or later, you must review the log file to determine the DDEs that are affected by the changes and add permissions or rules to action buttons and user-initiated buttons to that advanced workflows function as you intend.

Important: There is no automatic migration. You must manually convert any affected DDEs to transition and/or user-initiated permissions and rules after upgrading to release 6.2 or later. The log file also only returns results for applications and questionnaires that you have licensed at the time of the upgrade. If you update your license key after installing release 6.2 or later, and that license key provides access to additional applications that you did not previously have, the log file will not identify any affected DDEs in the newly-licensed applications. To update core applications, you can apply the appropriate 6.2 or later use case packages. These packages will update the advanced workflows with new permissions and rules for action buttons and user-initiated buttons.

Reconcile DDEs

1. Open the DDE log file, which is located in the folder designated in the Log Path field during Platform installation.
   The log file contains two sections that list the affected DDEs in your system and what action was set in the DDE prior to upgrade. One section lists DDEs that affect user-initiated buttons and the other section lists DDEs that affect transition buttons.

   User-initiated buttons:

Column	Description
Module Name	The name of the application or questionnaire.
Level Name	The name of the application or questionnaire level.
Event Action Name	The name of the affected DDE action.
User Initiated Button Text	The name of the user-initiated button.
Action Type	The action configured against the button.
Process ID	The Advanced Workflow Process ID.

   Action buttons:

Column	Description
Module Name	The name of the application or questionnaire.
Level Name	The name of the application or questionnaire level.
Node Name	The node name associated with the outgoing transition.
Layout Name	The layout associated to the node which also contains the affected DDE action.
Event Action Name	The name of the affected DDE action.
Button Name	The name of the button/transition.
Action Type	The action configured against the button.
Proc Node ID	The system id of the node.
Proc Node DB	The system proc node db.

2. For each affected action, look at the rule associated with that action and determine which of the following scenarios applies:

Scenario	Intent of rule	Users/groups applied to	Convert to
A	Intended to always evaluate to true	Specific users or groups	Advanced workflow permission
B	Intended to evaluate to true only when certain conditions were met	Everyone	Advanced workflow rule

Scenario A example

In release 6.1, say that you have the following transitions out of a User Action node and an associated DDE:

User Action transitions	Associated DDE rule	Associated DDE action
Submit to Business Unit Manager Submit to Risk Specialist	Record Status Equals New or Updated	Disable both buttons for everyone except the Risk Manager

Because this action only applies to specific users and the rule always evaluates to true, this DDE was likely intended to determine who could follow this transition. In release 6.2, you would replace this DDE by configuring permissions on the transition itself:

User Action transitions	Transition permissions
Submit to Business Unit Manager Submit to Risk Specialist	On each transition, create a permission and select the Risk Manager

Scenario B example

In release 6.1, say that you have the following transition out of a User Action node and an associated DDE:

User Action transition	Associated DDE rule	Associated DDE action
Submit to Risk Specialist	Risk Specialist Equals No Selection	Disable the Submit to Risk Specialist button for all users

Because this action applies to all users and the rule only evaluates to true under certain conditions, this DDE was likely intended to determine when the transition could be followed. In release 6.2, you would replace this DDE by configuring a rule on the transition itself:

User Action transition	Transition rule
Submit to Risk Specialist	Risk Specialist Does Not Equal No Selection Criteria: • Field to Evaluate: Risk Specialist • Operator: Does Not Equal • Value(s): No Selection

3. Convert each affected DDE to rules and/or permissions. For detailed steps on configuring rules and permissions, see "Building Workflows" in the Online Documentation.

Appendix H: Preparing Encryption for RSA Archer Advanced Workflow

You can optionally set up certificate-based encryption for the RSA Archer Advanced Workflow service. There are two tasks involved in this, one completed prior to installing RSA Archer, and one completed after the installation.

Complete the following procedure prior to installation.

1. Copy the certificate to the server that hosts the Advanced Workflow service.
2. Open the Certificate Manager.
   a. Click Start.
   b. Type:

      ```
      certmgr.msc
      ```

   c. Select Certificate Manager.
3. From the Certificate Manager, right click on Certificate, hover over All Tasks, and click Import.
4. From the Certificate Import Wizard, in File to Import, select the certificate to import, then click Next
5. In Certificate Store, select Place all certificates in the following store.
6. Click Finish.

Post-installation, complete the following task.

1. Run Windows Services as Administrator.
2. Scroll until the RSA Services appear.
   a. Right click RSA Archer Workflow service.
   b. Select Stop.
3. Close Windows Services.
4. Make a copy of the following file:

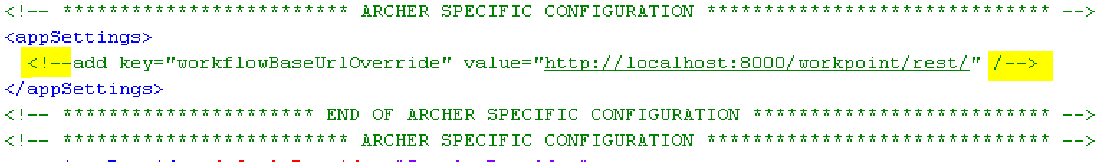
   ```
   <Installdirectory>\Services\Workpoint\conf\templates\WpServiceHost.exe.config
   ```

   Note: The install directory is usually Program Files/RSA Archer.

5. Edit the following file:

   ```
   <Installdirectory>\Services\Workpoint\conf\templates\WpServiceHost.exe.config
   ```

6. In appsettings, apply comment code to workflowBaseUrlOverride. For example:



```
<!-- ************************* ARCHER SPECIFIC CONFIGURATION ****************************** -->
<appSettings>
  <!--add key="workflowBaseUrlOverride" value="http://localhost:8000/workpoint/rest/" /-->
</appSettings>
<!-- ********************** END OF ARCHER SPECIFIC CONFIGURATION ************************** -->
<!-- ************************* ARCHER SPECIFIC CONFIGURATION ****************************** -->
```

7. Save WpServiceHost.exe.
8. Run Windows Services as Administrator.
9. Scroll until the RSA Services appear.
   a. Right click RSA Archer Workflow service.
   b. Select Start.
10. Close Windows Services.

Appendix I: Changes Made to the Task Management Application

When updating from RSA Archer 5 to 6.0 or later, be aware that the Task Management application has been updated. It is a system application and may be modified in future releases to support core platform features. These changes are made automatically by the installer to support the use of the Tasks widget on the Task-Driven Landing Screen and the creation of workflow tasks. If you use the Task Management application, ensure that it is thoroughly vetted in development and test environments before moving to production.

Renamed and New Fields

To better reflect what the fields actually represented, the old Subject and Priority fields were renamed to Type and Rating, respectively. This allowed for the addition of two new fields using the old field names, Subject and Priority, that better fit the names to the uses.

Renamed Fields

The following table lists the fields that were renamed in RSA Archer 6.0 or later.

Old Field Name	New Field Name	Field Type	Required	Locked
Subject	Type	Values List	No	Yes
Priority	Rating	Values List	No	Yes

New Fields

The following fields were added to the application in RSA Archer 6.0 or later.

Field Name	Field Type	Required	Locked
Subject	Text	Yes	Yes
Priority	Values List	Yes	Yes

Important: These are new Subject and Priority fields, not the renamed fields mentioned previously.

Updated Fields

The following fields were not previously required to include data in them, but now must contain data for core 6.1 functionality:

- Subject (New)
- Priority (New)
- Status

Important: If you have previously used the Task Management application, ensure that the Status fields are populated in the application before upgrading.

Appendix J: Importing RSA Security LLC Certificate into Trusted Root CA Store

The RSA Security LLC certificate is not present on every machine’s root store by default. It is required by users who are simultaneously enforcing the signature check option and utilizing an RSA provided JavaScript Transporter feed. The certificate must be imported once on each server in an environment.

1. Right-click the .JS file and click Properties.
2. Click the Digital Signatures tab.
3. On the Signature list, select the RSA Security LLC signer.
4. Click Details.
5. Click View Certificate.
6. Click Install Certificate.
7. Select Local Machine and click Next.
8. Select Place all certificates in the following store and click Browse.
9. Select Trusted Root Certification Authorities and click OK.
10. Click Next.
11. Click Finish.
12. Click OK to dismiss the successful import window.
13. Launch Certmgr from the Start menu.
14. Under Certificates – Local Computer, select Trusted Root Certification Authorities.
15. Select Certificates and verify there is a new RSA Security LLC certificate listed.
16. Export/Import this certificate to all servers in the Archer instance.
17. Whitelist the certificate's thumbprint in the ACP.

    For more information, see "Configuring the IP Whitelist" in the RSA Archer Control Panel Help.