



Version 6.10

# Security Configuration Guide

## **Contact Information**

Archer Community at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

## **Trademarks**

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

## **License Agreement.**

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person. No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

## **Third-Party Licenses**

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. 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.

## **Distribution**

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA 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.

© 2020 -2021 RSA Security LLC or its affiliates. All Rights Reserved.

## Contents

---

<b>Preface</b> .....	<b>8</b>
About This Guide .....	8
Archer Documentation .....	8
Support and Service .....	9
<b>Chapter 1: Security Controls Map</b> .....	<b>10</b>
Secure Deployment and Usage Settings .....	10
Web Server Security Configuration .....	18
Disallow IIS Arbitrary File Extensions .....	19
Disallow Arbitrary File Uploads .....	19
Remove IIS and ASP.NET Version Information from HTTP Headers .....	20
Remove AspNet-Version HTTP Header .....	20
Remove X-Powered-By HTTP Header .....	21
Remove IIS Version header .....	21
HTTP Security Settings .....	21
IP Whitelist .....	23
<b>Chapter 2: Authentication</b> .....	<b>24</b>
Configuring LDAP for Managing User Accounts and Groups .....	24
Configuring an Instance for Single Sign-on .....	32
Configuring the Instance Database Connection String and Pooling Options .....	42
Configure the instance database connection string .....	42
Override the pooling options for the instance database .....	43
Changing SysAdmin and Services Account Passwords .....	43
Configuring the Login Page .....	44
Disable the domain field .....	45
Display the login banner .....	45
Database Authentication Methods .....	45
Authentication Configuration Methods .....	46
<b>Chapter 3: Authorization</b> .....	<b>54</b>
User Access Control .....	54

Supporting your users .....	54
Entity permissions .....	57
Default User Accounts .....	57
Adding User Accounts .....	59
New User Accounts .....	59
New User Account with System Administrator Privileges .....	59
Platform User Accounts .....	59
Access Roles .....	65
Adding Access Roles .....	65
Assigning Access Roles to Users or Groups .....	67
Assign an access role to a user .....	68
Assign an access role to a user group .....	68
Unassign an access role from a user account .....	69
Privilege Levels for Archer Services .....	69
Least Privileges Requirement for Archer Database Objects .....	70
<b>Chapter 4: Network Security .....</b>	<b>71</b>
Port Usage .....	71
Network Encryption .....	78
Data Feeds .....	79
Supported Field Types .....	81
Unsupported Field Types .....	82
Archer Web Services Transporter .....	87
HTTP Transporter .....	89
Weak ciphers disabled .....	89
FTP Transporter .....	89
File Transporter .....	90
Web Server Communication .....	92
SQL Server Communication .....	93

Application Programming Interface (API) .....	93
Archer Web Services API .....	93
Archer Web Services .....	94
Proxy Bypass Security Considerations .....	94
Host Hardening .....	95
Recommendations for TLS/SSL cipher hardening .....	95
<b>Chapter 5: Data Security .....</b>	<b>99</b>
Encryption of Data at Rest .....	99
Encrypting Data .....	100
Enable field encryption at the instance level .....	101
Troubleshooting field encryption .....	102
Configuring the Hardware Security Module .....	102
File Repository Path .....	103
Restrict Permissions on Repository Files .....	103
Keyword Index Files .....	104
Company Files Path .....	104
Disabling Metadata Publishing in ASMX Web Services .....	104
Disable ASMX metadata publishing .....	104
Enabling URLs In Saved Records .....	105
Enable URLs in saved records for all instances .....	105
Enable URLs in saved records for an instance .....	105
FIPS Compliant Mode .....	105
Platform Release Supporting FIPS .....	106
FIPS Certificates .....	106
SQL Server FIPS Setup .....	107
LDAP Configuration for FIPS Mode .....	107
Platform FIPS Certification .....	108
<b>Chapter 6: Cryptography .....</b>	<b>110</b>
SSL Certificate Guidance .....	110
Field Encryption certificate requirements .....	110
How to secure a Field Encryption certificate .....	111
SSL Certificate Validation - Redis .....	111
<b>Chapter 7: Auditing and Logging .....</b>	<b>113</b>

Log Description .....	113
Security Events Report .....	113
Archer Error Logs .....	115
Log Directory Permissions .....	115
Windows Event Logs .....	115
<b>Chapter 8: Physical Security .....</b>	<b>116</b>
Physical Security Controls Recommendations .....	116
<b>Chapter 9: Serviceability .....</b>	<b>117</b>
Security Patch Management .....	117
Malware Detection .....	117
Virus Scanning .....	118
Ongoing Monitoring and Auditing .....	118
Securing Credentials .....	118
<b>Chapter 10: Additional Security Considerations .....</b>	<b>119</b>
Creating iViews .....	119
Task 1: Create the iView .....	119
Task 2: Configure the options for your iView type .....	120
Task 3: Determine who can access the iView .....	123
Managing iViews .....	124
Create a folder for a Global iView .....	124
Update an iView display .....	124
Delete a global iView .....	124
Formatting iView Videos .....	125
Embedding From an External Source .....	125
Embedding From an Internal Source .....	125
Adding Objects to the Layout .....	125
Key guidelines for adding objects to the layout .....	126
Add sections .....	126
Add text boxes .....	126
Add placeholders .....	127
Add custom objects .....	127
Add trending charts .....	128
Add report objects .....	128
Adding tab sets .....	129

Offline Access .....	130
Archer features not supported for offline access .....	130
Installing Offline Access .....	131
Preparing for Offline Access Installation .....	131
Install Offline Access .....	132
Elasticsearch Security Considerations .....	133
JavaScript Transporter Security Considerations .....	134
Archer IRM Mobile App Security Considerations .....	134

## Preface

---

About This Guide .....	8
Archer Documentation .....	8
Support and Service .....	9

### About This Guide

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

### Archer Documentation

You can access Archer documentation on the Archer Community:

<https://community.rsa.com/t5/archer-platform-documentation/tkb-p/archer-platform-documentation>.

The following table describes each document.

Document	Description
Platform Planning Guide	Information about how to plan for your Archer installation. This document is intended for system administrators who are responsible for installing and managing Archer.
Platform Installation and Upgrade Guide	Instructions for installing and upgrading to the latest Archer release. This document is intended for system administrators who are responsible for installing and managing Archer.
Online Documentation	Information for using Archer, including how to set up, maintain, and use the Archer Platform, security configuration information, and information on the solution use cases. Available from within Archer.
Archer Control Panel (ACP) Help	Information for using the Archer Control Panel (ACP) module to manage the internal settings of the Platform, such as license keys, global paths and settings. Available from within the ACP module.
Security Configuration Guide	Information about security configuration settings available in the Archer Platform and security best practices for using those settings to help ensure secure operation of Archer.



## Support and Service

Open a Support case via the toll free phone number for your locale, or using the Case Management portal on Archer Community. Step by step instructions for opening a Support case and using the Case Management portal can be found here: <https://community.rsa.com/t5/support-information/how-to-contact-rsa-support/ta-p/563897>.

### Other Resources

Resource	Description
Archer Community	<p>Our public forum, on the Archer Community , brings together customers, partners and analysts to discuss risk and compliance as a practice.</p> <p><a href="https://community.rsa.com/t5/archer/ct-p/archer">https://community.rsa.com/t5/archer/ct-p/archer</a></p>
Archer Customer / Partner Community	<p>Our private community is a powerful governance, risk and compliance online network that promotes collaboration among customers, partners, industry analysts, and product experts.</p> <p><a href="https://community.rsa.com/t5/archer/ct-p/archer">https://community.rsa.com/t5/archer/ct-p/archer</a></p>
Archer Exchange	<p>The Archer Exchange 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.</p> <p><a href="https://community.rsa.com/t5/archer-exchange/ct-p/archer-exchange">https://community.rsa.com/t5/archer-exchange/ct-p/archer-exchange</a></p>

## Chapter 1: Security Controls Map

---

Secure Deployment and Usage Settings .....	10
--	----

### Secure Deployment and Usage Settings

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

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

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

### Security Controls Map

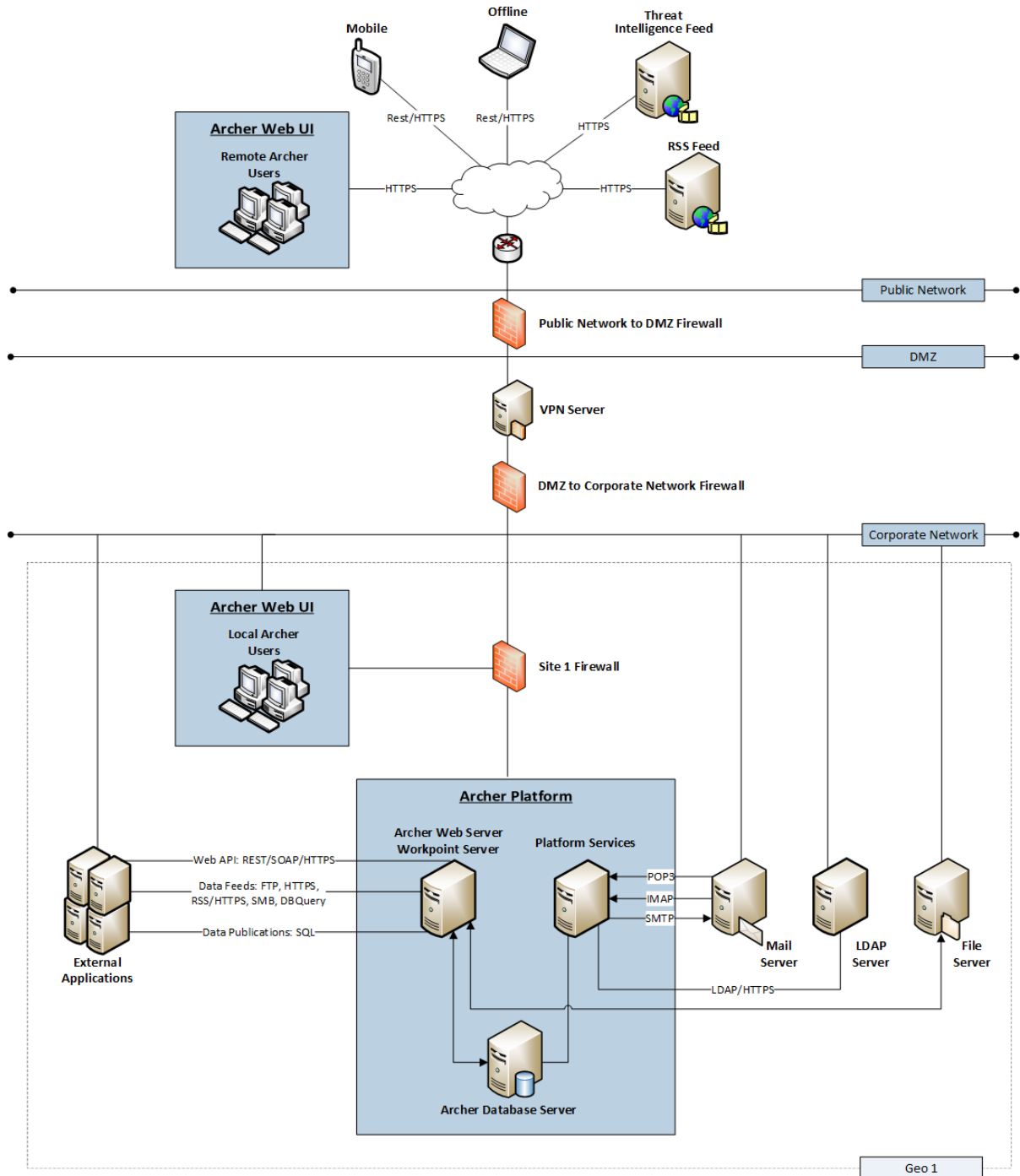
An Archer deployment consists of three physical tiers: a web tier, a services tier, and a database tier. An organization can deploy Archer in a single host configuration or a multi-host configuration. For more information, see the *Archer Platform Installation and Upgrade Guide*.

When deploying Archer on-premise within a corporate network, it is recommended that you do the following:

- Deploy Archer hosts within the corporate network. The DMZ-to-Corporate-Network Firewall intercepts all communication between the single host and the other components in the network.
- Ensure that users are accessing Archer from within the corporate network. If users must access Archer from the internet, it is recommended that they connect to the corporate network through a secure VPN connection.
- Allow only remote access to Archer hosts for secure maintenance using the Remote Desktop Protocol (RDP) through a secure VPN connection.
- Configure firewall rules to ensure secure communication between Archer and other components in the network.

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

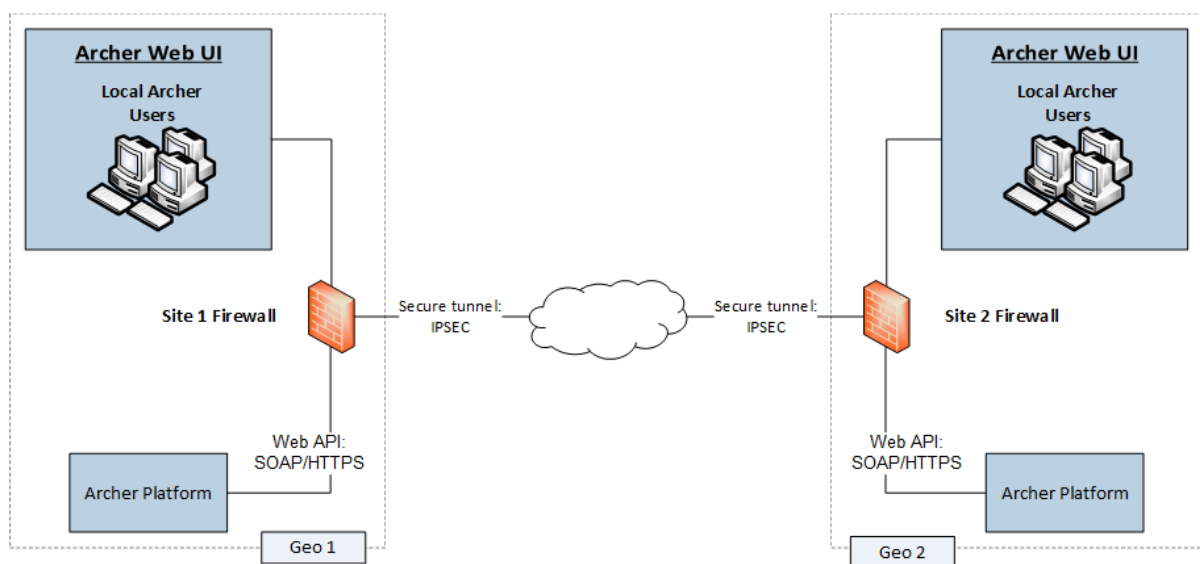
The following figure shows an example of a multi-host configuration.



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

- Deploy Archer web, services, and database servers in the corporate network.
- Deploy data feed servers in the corporate network, except those that provide information using HTTPS, such as, RSS and Threat Intelligence services.
- Deploy a Web Application Firewall between the DMZ and Public network.
- Ensure that all Archer servers in a site are connected to the same sub-network.
- Deploy firewalls at each site to ensure secure transfer of data from an instance of Archer at one site to another instance of the Archer located at a different site.
- Configure firewall rules to intercept all communication between Archer components in the network, as shown in the preceding figure. For more information, see [Firewall Rules](#).

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



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

- Configure firewall rules to intercept all communication between the Archer components in the network and between different sites, as depicted by the firewalls in the preceding figure. For more information, see [Firewall Rules](#).
- Implement data transfer between sites using a secure tunnel as shown in the preceding figure.

## Firewall Rules

Use firewalls to restrict network traffic between Archer and external systems. For graphical depictions of restricting network traffic, see [Security Controls Map](#).

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

- You have a stateful firewall, indicating that only the establishment of TCP ports is considered.
- You specify the direction of communication for the UDP ports because the connections are sessionless.
- The firewall processes the rules top to bottom, finishing with a generic drop of all packets.
- You deploy Archer as shown in one of the figures in [Security Controls Map](#).

It is recommended that you configure firewall rules to ensure secure communication for the following connections:

- [DMZ to Corporate Network](#)
- [Corporate Network to Site Sub-Network](#)
- [Archer-to-Archer Data Feeds](#)

### DMZ to Corporate Network

It is recommended that you do the following:

- Configure trusted communication from the VPN server in the DMZ to the client machines on which the Archer web user interface runs.
- Create firewall rules for all machines from which you intend to remotely access the corporate network through RDP.

### Corporate Network to Site Sub-Network

For corporate network to site sub-network configurations, It is recommended that you do the following:

- Allow firewall access at each site only from designated Archer client machines through a trusted IP address and port.
- Set firewall rules to drop all unless explicitly allowed.

## Single-Host Configuration

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

- TCP 80
- TCP 443

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

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

## Multi-Host Configuration

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

- TCP 80
- TCP 443

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

<b>Purpose</b>	<b>RULE   DIRECTION</b>	<b>Source IP Address → Destination IP Address</b>	<b>Protocol</b>	<b>Port</b>
Client Web Connectivity	ALLOW   INBOUND	ArcherWebUI_IPAddr → ArcherWebServer_IPAddr	TCP	443
	ALLOW   OUTBOUND	ArcherWebServer_IPAddr → ArcherWebUI_IPAddr	TCP	443
RSS Feeds	ALLOW   INBOUND	RSSServer_IPAddr → ArcherWebServer_IPAddr	TCP	443
	ALLOW   OUTBOUND	ArcherWebServer_IPAddr → RSSServer_IPAddr	TCP	443
Threat Feeds	ALLOW   INBOUND	ThreatFeedServer_IPAddr → ArcherWebServer_IPAddr	TCP	443
	ALLOW   OUTBOUND	ArcherWebServer_IPAddr → ThreatFeedServer_IPAddr	TCP	443
<Default>	BLOCK   INBOUND	All_* → All_*	*	*
	BLOCK   OUTBOUND	All_* → All_*	*	*

### Archer-to-Archer Data Feeds

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

For this scenario, It is recommended that you do the following:

- Ensure that the firewall at each end of the data transfer allows communication only through a trusted IP address and port.
- Secure the following default ports to ensure a secure communication between two Archer instances located in different sites:
  - TCP 80
  - TCP 443

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

<b>Purpose</b>	<b>RULE   DIRECTION</b>	<b>Source IP Address → Destination IP Address</b>	<b>Protocol</b>	<b>Port</b>
Archer Data Feed	ALLOW   INBOUND	ArcherDataFeed_IPAddr → ArcherWebServer_IPAddr	TCP	443
<Default>	BLOCK   INBOUND	All_* → All_*	*	*
	BLOCK   OUTBOUND	All_* → All_*	*	*



## Secure Deployment Settings

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

<b>Deployment Settings</b>	<b>Secure Deployment Setting</b>	<b>Pros of Secure Deployment Setting</b>	<b>Cons of Secure Deployment Setting</b>	<b>Instructions on How to Configure Secure Deployment Setting</b>
<p>HTTPS is enabled on a new 6.x installation, by default, between client and server. Remove any existing HTTP bindings (port 80) via IIS Manager.</p>	<p>For best possible security between client and server, enable HTTPS and disable HTTP in Microsoft IIS.</p>	<p>Provides a high level of protection for the communication between client and server by avoiding tampering, spoofing, and man-in-the-middle type of attacks.</p>	<p>Could impact performance.</p>	<p>See "Web Server Communication" in the Archer Online Documentation.</p>
<p>Database Encrypted Communication</p>	<p>Encrypting the communication between the Archer Web Server and the Instance Database increases security.</p>	<p>Provides increased security by implementing secure communication between the Web Server and Instance Database.</p>	<p>Could impact performance.</p>	<p>See "Maintaining Security" in the Archer Security Configuration Guide.</p>
<p>Persistent Session Cookie Configuration</p>	<p>Deleting the cookie holding the session token when the client is closed increases security.</p>	<p>Provides increased security by requiring reauthentication after logout or browser close.</p>	<p>User has to reauthenticate.</p>	<p>See "Enabling Storing the Session Token in a Persistent Cookie" in the Archer Control Panel Help.</p>

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

## Web Server Security Configuration

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

In addition to Microsoft's recommendations, It is recommended that you configure Microsoft IIS to do the following:

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

## Disallow IIS Arbitrary File Extensions

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

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

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

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

## Disallow Arbitrary File Uploads

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

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

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

- .AI
- .BMP
- .CSS
- .CSV
- .DOC
- .DOCM
- .DOCX
- .DOT
- .DOTM
- .EMF
- .EPS
- .EXIF
- .GIF
- .ICO
- .JPEG
- .JPG
- .PDF
- .PNG
- .POT
- .POTM
- .POTX
- .PPA
- .PPAM
- .PPS
- .PPSM
- .PPSX
- .PPT
- .PPTM
- .PPTX
- .PS
- .RTF
- .TIF
- .TIFF
- .TXT
- .WMF
- .XLA
- .XLAM
- .XLS
- .XLSB
- .XLSM
- .XLSX
- .XLT
- .XLTM
- .XLTX
- .XML

## Remove IIS and ASP.NET Version Information from HTTP Headers

To make it more difficult for attackers to identify vulnerabilities in the software that is powering the Web Server, do not disclose the types of applications and their respective version numbers in HTTP headers. While certain HTTP headers are necessary, the HTTP headers that identify the Web Server are not necessary, including the following:

- Server: Microsoft-IIS/<version\_ number>
- X-Powered-By: ASP.NET
- X-AspNet-Version: <version\_ number>

## Remove AspNet-Version HTTP Header

It is recommended that you do the following:

- Remove the HTTP headers that identify the web server.
- Ensure that `<httpRuntime enableVersionHeader="false"/>` is set in the Archer web.config file, located at:
  - IIS\DefaultWebSite\RSAArcher\web.config
  - IIS\DefaultWebSite\RSAArcher\api\web.config

## Remove X-Powered-By HTTP Header

1. Launch the Microsoft IIS Manager.
2. Expand the Sites folder.
3. In the IIS grouping, select the website that you want to modify, and double-click the HTTP Response Headers section.
4. If "X-Powered-By: ASP.NET" is displayed in the Custom Header listbox, click the Remove link in the right-hand column.

**Note:** To ensure that the server header is not automatically added to the outgoing HTTP response by Microsoft IIS, use Microsoft's free UrlScan utility.

## Remove IIS Version header

It is recommended that you ensure that `<requestFiltering removeServerHeader="true"/>` is set in the Archer web.config file, located at:

- IIS\DefaultWebSite\RSAArcher\web.config
- IIS\DefaultWebSite\RSAArcher\api\web.config

1. Open the web.config file.
2. In the web.config system.webServer node, use the following settings to configure requestFiltering.

```
<security>  
<requestFiltering removeServerHeader="true"/>  
</security>
```

3. Save the file.

## HTTP Security Settings

A fundamental part of website security includes configuring the HTTP Security Settings. These settings protect against attacks including XSS, code injection, and clickjacking, that are most likely to impact your website.

In addition to the three security settings mentioned below, for more HTTP Security Settings, see the following two topics:

- [Configure IIS for HTTPS/SSL protocol](#)
- [Configure Platform web.config file for HTTPS/SSL protocol](#)

### **Content-Security-Policy HTTP Header**

Archer uses the Content-Security-Policy HTTP header, with the `frame-ancestors` attribute set to `self`, to prevent cross frame scripting attacks. This header prevents hosts outside of the Archer server from framing Archer pages, similar to the X-Frame-Options header. However, Internet Explorer does not support the Content-Security-Policy header.

You can remove the Content-Security-Policy HTTP header and add custom HTTP headers into IIS. If you remove the Custom-Security-Policy HTTP header and install a newer version of Archer, the installer adds the header back into IIS.

Archer also uses the X-Frame-Options HTTP header. Major browsers including Google Chrome, Mozilla Firefox, and Internet Explorer support this header. Set the value of this header in the list in IIS to `sameorigin` to prevent users from loading an Archer host within an `iframe` of another host.

### **X-Content-Type-Options Header**

Archer uses the X-Content-Type-Options header, set to `nosniff`, to prevent MIME sniffing attacks. This header prevents browsers from reconfiguring the MIME types in Archer hosts. `nosniff` prevents browsers from assuming the page content type and renders pages with the correct MIME type.

You can remove the X-Content-Type-Options header and add custom HTTP headers into IIS. If you remove the X-Content-Type-Options header and install a newer version of Archer, the installer adds the header back into IIS.

The following major browsers support this header: Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer, and Opera. Safari does not support this header.

### **Access-Control-Allow-Origin Header**

Archer uses the Access-Control-Allow-Origin header to configure which hosts can access responses sent from the Archer API. The default value of this header is `*`, which allows any host to access the API responses.

To restrict access to API responses only to the request origin host, set `<add key="RestrictCORSDomains" value = "true"/>` in the Archer `web.config` file, located at `IIS\DefaultWebSite\RSAArcher\api\web.config`.

Major browsers including Google Chrome, Mozilla Firefox, and Internet Explorer support this header.

## **IP Whitelist**

The IP Whitelist allows for the ability to define a range of IP addresses that can access Archer. The IP Whitelist restricts incoming connections only, and should include the following items:

- Web Application servers
- Services servers
- Client machines accessing the Web Application

Optionally, the following items can also be included:

- Data Feed source servers
- LDAP servers

It is recommended that you implement the IP Whitelist to limit the availability of the Platform as a potential attack vector.

## Chapter 2: Authentication

---

Configuring LDAP for Managing User Accounts and Groups .....	24
Configuring an Instance for Single Sign-on .....	32
Configuring the Instance Database Connection String and Pooling Options .....	42
Changing SysAdmin and Services Account Passwords .....	43
Configuring the Login Page .....	44
Database Authentication Methods .....	45
Authentication Configuration Methods .....	46

### Configuring LDAP for Managing User Accounts and Groups

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

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

**Important:** Before you configure LDAP synchronization for your Archer SaaS environment, you must first contact Archer Customer Support for assistance connecting your organization's LDAP server to the Archer cloud environment. You must provide the IP address or address range for your LDAP server.

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



**Note:** It is recommended that you require a domain for LDAP synchronizations and SSO. If domains are not used, disable the display of the Domain field in the Archer Control Panel.



The following fields change during mapping:

- A user profile field that is mapped to an LDAP attribute is populated for new accounts. The value is retained for existing accounts.
- A user profile field that is mapped to an LDAP attribute that does not have a value is not populated for new accounts. The value is retained for accounts that were previously created.
- When the Email Address or Phone field in the user profile is mapped to an LDAP value, the LDAP value is inserted in the first email or phone number field in the user profile for new user accounts. For existing accounts, the LDAP value replaces the value in the first email or phone number field in the user profile. If a user has modified the email address or phone number through the Platform, the modification is overwritten by LDAP synchronization unless the LDAP value is null.
- The Time Zone field in the user profile cannot be mapped to an LDAP attribute.

### Task 1: Set up your LDAP server

1. Go to the Manage LDAP Configurations page.
  - a. From the menu bar, click .
  - b. Under Access Control, click LDAP Configurations.
2. Click .
3. In the General Information section, enter the name and description.

4. Click the Configuration tab, and do the following:

- a. In the LDAP / Active Directory Server section, enter the LDAP / Active Directory Server Domain, Name / IP Address, and connection or binding preferences.

The following table describes each field.

Field	Description
User's Domain	The domain to which user accounts from this LDAP server belong. The name must be unique for all LDAP configurations. If you are using Windows Authentication, ensure that the User Domain field matches the Windows domain name. If these values do not match, single sign-on (SSO) fails. These domain names are not case sensitive.
Name/IP Address	The fully qualified name or IP address of your LDAP or Active Directory server. Selecting this option ensures that your server assumes responsibility for directing Archer to the appropriate domain controller. If the previously contacted domain controller is unavailable, a secondary domain controller is identified and used instead. For example, if your primary LDAP server is down for maintenance, Archer is directed to the secondary server to begin LDAP synchronization.

**Note:** You can bind the LDAP connection to a default domain controller without specifying the name of a default server. Microsoft recommends the use of serverless binding for fault tolerance. If you select Use Serverless Binding, you do not need to enter a value in the Name/IP Address field.

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

The following table describes each field.


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

Field	Description
User Identifier	<p>Identifies the object as a user object.</p> <ul style="list-style-type: none"> <li>• For new LDAP configurations, the default value is user.</li> <li>• For Active Directory servers, the default value is user.</li> <li>• For other LDAP servers, the default value is inetOrgPerson.</li> </ul> <p>To obtain the actual default values for your organization, contact your LDAP Administrator.</p>
Group Identifier	<p>Identifies the object as a group object.</p> <ul style="list-style-type: none"> <li>• For new LDAP configurations, the default value is group.</li> <li>• For Active Directory servers, the default value is group.</li> <li>• For other LDAP servers, the default value is groupOfUniqueNames.</li> </ul> <p>To obtain the actual default values for your organization, contact your LDAP Administrator.</p>
Additional Attributes	<p>Provides additional attributes that must be retrieved from the LDAP source during search. For example, if you are using filters, enter those filters into this field.</p>
User's Group Identifier	<p>Identifies the groups to which the user belongs.</p> <ul style="list-style-type: none"> <li>• For new LDAP configurations, the default value is memberOf.</li> <li>• For Active Directory servers, the default value is memberOf.</li> <li>• For other LDAP servers, the default value is uniqueMember.</li> </ul> <p>To obtain the actual default values for your organization, see your LDAP Administrator.</p>
Users and Groups	<p>Sets the User/Group association.</p> <ul style="list-style-type: none"> <li>• Users contain groups. Specifies that the user-group association is defined in the user object of the Active Directory server.</li> <li>• Groups contain users. Specifies that the user-group association is defined in the group object of the LDAP server.</li> </ul>

Field	Description
Connection Timeout	Inputs the timeout value in seconds for the LDAP query. <b>Important:</b> This value must be a whole number greater than 0. For new LDAP configurations, the default value is 60.

5. Click Save or Save and Close.
  - To apply the changes and continue working, click Save.
  - To save and exit, click Save and Close.

### Task 2: Map LDAP attributes to your user profiles


1. Go to the Configuration tab of the LDAP Configuration.
  - a. From the menu bar, click  .
  - b. Under Access Control, click LDAP Configurations.
  - c. Click the Configuration tab.
2. Go to the User Field Mapping section.
3. In the Base DN field, enter the domain name.
4. (Optional) In the Filter field, enter the criteria for filtering the LDAP directory.
5. Click Get Attributes to populate the field mapping.
6. In the User Field Mapping section, select the attributes for each field in the user profile that you are synchronizing with the LDAP directory.  
 The following table describes each field.

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

Field	Description
Filter	<p>Filters the LDAP information available for mapping to user profile fields. Filters are entered using the following format: objectClass=class name.</p> <p>Example</p> <p>You want to map only LDAP values associated with the User class. Enter objectClass=user as the filter. This entry makes the values associated with this class available for mapping.</p>
Get Attributes	<p>Populates the Attribute lists in the Field Mapping section.</p> <p><b>Note:</b> Archer supports creation of custom attributes for users in their LDAP server. Only custom attributes designated as human-readable with their object identifiers (OIDs) defined in RFC 2252 are available for mapping under LDAP configuration in the User Field Mapping section.</p>
Field Mapping	<p>Maps the attributes from the LDAP directory to the fields in the user profile. You must map all required fields in the user profile to an attribute.</p>
Test Connection	<p>Tests the connection of an LDAP Configuration between the Archer database and the LDAP server or active directory server.</p> <p>If an error message is displayed when the number of records returned exceeds the configured size limit for the active directory, contact your LDAP administrator to request a configuration change.</p>

7. Click Save or Save and Close.
  - To apply the changes and continue working, click Save.
  - To save and exit, click Save and Close.

### Task 3: Set rules for managing user accounts and groups

1. Go to the Data Sync tab of the LDAP Configuration.
  - a. From the menu bar, click .
  - b. Under Access Control, click LDAP Configurations.
  - c. Click the Data Sync tab.
2. In the User Account Management section, define the rules for updating, creating, deactivating, and reactivating accounts.

The following table describes each section.

Field	Description
Updating	<p>Specifies the rules for updating the user profile.</p> <ul style="list-style-type: none"> <li>• Update all user accounts on each sync: Updates all user accounts based on the information contained in your LDAP server</li> <li>• Update only user accounts where the LDAP attribute meets the following criteria: Updates user accounts based on a specific LDAP attribute and the specified criteria.</li> </ul> <p>Example: You want to update only user accounts from your New York office. Select Office from the Attribute list, select Equals as the operator, and enter New York in the Value field from the Operator list.</p>
Creating	<p>Creates or updates a user account if the account does not exist in Archer. The name for the new user account is assigned the value of the LDAP attribute mapped to the User Name (Login) field.</p>
Clear User DNs	<p>Clears the distinguished names of all users just before the LDAP synchronization starts. The synchronization then repopulates the database with the most up-to-date list of distinguished names. If users have changed their login names, moved location, or are in a new part of the company, for example, the old distinguished names are no longer valid. Consequently, these users would not be able to log into Archer.</p> <p><b>Note:</b> It is strongly recommended that you enable this option.</p>

Field	Description
Deactivation	<p>Deactivates user accounts.</p> <ul style="list-style-type: none"> <li>Deactivate all user accounts that do not have a matching LDAP user. Deactivates user accounts for which no matching LDAP account is found during data synchronization.</li> <li>Deactivate those user accounts where LDAP attribute meets the following criteria and then enter the LDAP criteria. Deactivate user accounts based on a specific LDAP attribute.</li> </ul> <p>Example: You want to deactivate user accounts where the employment status for the matching LDAP user account is set to inactive. Select Employment Status from the Attribute list, select Equals as the operator, and enter Inactive in the Value field from the Operator list.</p>
Reactivation	<p>Reactivates user accounts based on specific LDAP attribute criteria.</p> <p>Example: You want to reactivate inactive user accounts where the employment status in the matching LDAP user account is set to active. You would select Employment Status from the Attribute list, select Equals and enter Active in the Values field from the Operator list.</p>
Send Notification	<p>Sends a notification to each user that is created to alert the user of a new password. The Default Email Address in the user account must be present to send notifications. When you select this option, a notification message is sent to all users that are being created.</p> <p>It is recommended to disable this option when synchronizing a large number of records because uploading a large number of users can cause the email server to exceed its capacity for sending email messages.</p>

- (Optional) In the Group Management section, select whether to enable the Group sync as part of the sync process.

The following table describes each field.

Field	Description
Group Sync	<p>Replicates your LDAP group structure in Archer when synchronized. The common name (CN) of the group on your LDAP server is used as the group name in Archer. If a group in Archer is created before synchronizing with your LDAP server, and there is a group with a matching name in your LDAP directory, the group in Archer is not synchronized with the LDAP group. Instead, a new group with the same name is created and is flagged with the Synchronization icon.</p> <p>Selecting the Group Sync option makes your LDAP server the authoritative system for Archer group management.</p> <ul style="list-style-type: none"> <li>• Any groups that you delete from your LDAP server also are deleted from Archer</li> <li>• Any changes made to your groups in the LDAP directory are reflected in Archer.</li> </ul> <p>You cannot edit or delete groups in Archer that were created through LDAP synchronization. You can create additional groups in Archer that are not included in your LDAP group structure, and can fully manage these groups in Archer.</p>
Group Base DN	<p>Specifies the Base Distinguished Name (DN) for your LDAP group structure. If you selected Group Sync and you do not specify a DN for your group structure, the group sync query defaults to the Base DN specified in the LDAP configuration.</p>

4. Click Save or Save and Close.

- To apply the changes and continue working, click Save.
- To save and exit, click Save and Close.

## Configuring an Instance for Single Sign-on

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



Archer supports two basic authentication mechanisms:

- Username/password login scheme (default)
- SSO configuration, which facilitates user login in corporate computing environments and supports most popular web authentication products.

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

**Important:** Before you configure LDAP synchronization for your Archer SaaS environment, you must first contact Archer Customer Support for assistance connecting your organization's LDAP server to the Archer cloud environment. You must provide the IP address or address range for your LDAP server.

### Single Sign-on properties

The following table describes the SSO properties.

Option	Description
Single Sign-on Mode	<p>Specifies the user login method. By default, the method is Disabled. When you have enabled this option, the system grants the user access if the user exists in Archer. If the user does not exist, an LDAP query retrieves the user profile information and creates an account.</p> <p>The other options are:</p> <ul style="list-style-type: none"> <li>• HTTP Header. This method requires an HTTP header parameter that identifies the user attempting to access the application.</li> <li>• Request Parameter. This method requires a request form or query string parameter that identifies the user attempting to access the application.</li> <li>• Windows Integrated uses the “Integrated Windows Authentication” built into Internet Information Services (IIS) that uses the user credentials using NTLM/Active Directory.</li> <li>• Federation. This method allows Archer to process Windows Federated claims from Active Directory Federation Services (ADFS). Use Federation to process claims generated from ADFS directly. You can also set up ADFS as a service provider to a SAML 2.0 identity provider (IDP) and convert the SAML 2.0 assertions to Federated claims.</li> <li>• SAML. This method allows you to set up a SAML 2.0 capable provider to work with Archer and authenticate based on SAML assertions of IDPs.</li> </ul> <p>Use ADFS as the service provider for the Federation option.</p>

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

### Authentication options

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

### Configuration procedure

#### Task 1: Enable authentication for Single Sign-on

1. Go to Internet Information Services (IIS) Manager.
  2. Enable authentication for the following SSO modes for the current server desktop connection:
    - For HTTP Header, enable Anonymous Authentication.
    - For Request Parameter, enable Anonymous Authentication.
    - For Windows Integrated, enable Windows Authentication.
    - For Federation, enable Anonymous Authentication.
    - For SAML, enable Anonymous Authentication.
- Note:** Archer requires that only one authentication type be enabled at a time.
3. In the Archer Control Panel, specify and then enable the instance for which you are configuring SSO.

## Task 2: Configure Single Sign-on

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

1. Click the Single Sign-on tab of the instance you want to configure.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click the instance.
2. In the Single Sign-on Mode field, select one of the following:
  - HTTP Header
  - Request Parameter
  - Windows Integrated
  - Federation
  - SAML
3. Do one of the following:
  - If you selected Request Parameter or HTTP Header methods, go to the next step.
  - If you selected Windows Integrated method, go to step 6.
  - If you selected Federation, go to step 7.
  - If you selected SAML, go to Configuring SAML Single Sign-on Mode.
4. In the Username Parameter field, enter the name of the user logon.
5. In the Domain Parameter field, enter the domain to which the user can log in.
6. Do one of the following:
  - To enable manual login to, click Allow Manual bypass, and then go to step 14.
  - To force SSO regardless of the user, go to step 14.
7. Configure the following options in the Single Sign-on section:
  - a. Select Override Federation metadata to ignore Federation metadata at the installation level, which enables instances to use a different ADFS service provider.


**Note:** Any change of the entity name or change of any certificates in ADFS requires that you reimport metadata into Archer.
  - b. If you selected Override Federation Metadata, you can click Select to go to a different metadata .xml file, and then select the file.

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

- c. In the Relying Party Identifier field, enter the replying party identifier, which is provided in ADFS for this instance.
- d. In the Home Realm Parameter field, enter the name that you created to identify your realm. This name is the identifier that is used in the vanity URL. The syntax for this string is:  
`https://{servername}/../Default.aspx?<HomeRealmIdentifier>=<IdpRealmName>`

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

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

8. Configure the following options in the Identity Providers section:
  - a. In the Decision Page Header field, enter the text that you want to appear as the heading at the top of the Decision Page.
  - b. In the Dropdown Label field, enter the text that you want to appear on the Decision Page as the label for the drop-down that lists all identity providers.
  - c. In the Identity Provider field, select an existing IDP. You can complete the following three fields to add an IDP. (See the Claim Names for the Federation table at the end of this procedure for Archer supported claim names.):
    - In the Realm field, enter the realm name for the new identity provider.  
You can link to the following website to learn how to set up the claim provider and relying party in ADFS:  
[https://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides(v=ws.10).aspx)
    - In the Identifier field, enter the appropriate claim provider identifier which is provided in ADFS for a given identity provider. For a complete list of the claims that Archer supports, see the table below.
    - In the Display Name field, enter the display name for the new identifier, which then displays in the drop-down list of the Decision Page.
- To add more providers, click , and then complete the same three fields for each provider.
9. (Optional) In the On Login Error field, enter the URL for the page you have created. The user is redirected here if there is a login failure.
10. (Optional) In the On User Not Found field, enter the URL for the page you have created. The user is redirected here if the username cannot be found in Archer.

11. (Optional) In the On Provisioning Failure field, enter the URL for the page you have created. The user is redirected here if there is a provisioning failure. For example, if you have exceeded the maximum number of users for your instance.
12. Select the Provisioning Settings for the selected IDP as appropriate.
13. Enter the default First Name, Last Name, and User Role that Archer uses if no name and user roles were specified at the time of provisioning. You can, later, edit these values for the new user.
14. On the toolbar, click Save.

### Claim names for the Federation Option

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

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

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

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

### Task 3: Set authentication for Single Sign-on

1. Enable LDAP synchronization enabled in Microsoft Internet Information System (IIS).
2. Specify and enable the instance for which you are configuring SSO.
3. Configure SSO for the instance.
4. Modify the web.config file for your authentication method.

### Configuring SAML Single-Sign-on mode

1. Allow manual bypass.
  - Enabled allows you to bypass SSO mode and log in using Archer credentials.
  - Disabled allows you to only use SSO through configured identity providers (IDPs).
2. Provide the Instance Entity ID (required).
  - The identifier for this instance acts as a SAML service provider when issuing authentication requests.
  - Entity IDs must be unique across Archer instances using the same IDP and limited to 1024 characters in URL format.
3. Provide a certificate thumbprint.
  - An x.509 certificate is required to allow signing SAML requests and encryption of SAML assertions. Archer signs requests when the IDP requires. The IDP uses the same certificate


when encrypting assertions.

- Provide a thumbprint for the x.509 certificate in the Windows Local Machine Certificate Store.
  - The IIS Application pool identity running the Archer application requires Private Key-Read permission.
  - If you use multiple web servers, import the same certificate to all Local Machine Certificate Stores.
4. The service provider metadata exports Archer service provider metadata XML for use when configuring Archer as a client with your IDP. Metadata includes:
- Instance Entity ID
  - Redirection URL to Archer assertion consumer service
  - Required Name ID preference
  - Public key of signing and encryption certificate
  - Preference for signed assertions from the IDP

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

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

### Identity Providers

1. Complete the following fields to add an IDP or select an existing IDP from the list to edit. If adding a second or multiple IDPs, click the  icon then complete the following (required):
  - a. In the Display Name field, enter the display name for the new identifier. The identifier displays in the drop-down list on the Single Sign-on Decision Page. The display name is shown when the instance URL is provided without the IDP parameter.
  - b. In the Realm field, enter the Realm name for the new IDP. The Realm field value, instance URL, and parameter name IDP can be used to skip the Single Sign-on Decision Page.

Example:

- Instance URL: <https://archer.domain.com> Realm: CorpIDP
- Going to <https://archer.domain.com/default.aspx?IDP=CorpIDP> skips the Decision Page and immediately redirects you to CorpIDP for authentication.

2. Import identity provider SAML metadata (required).

- a. Click import, and go to metadata .xml file.
- b. Click OK to finish the import.

The IDP Metadata field shows value of EntityID contained in the entity descriptor from the metadata.

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

3. Select the appropriate Provisioning Settings for the selected IDP (Optional):

- Enable User Provisioning. If an account does not exist, a new account is created based on the username.
- Enable User Update. Profile information including email address, street address, First Name, Last Name, updates each time that a user successfully authenticates through SSO.
- Enable Group Update. Group membership is updated on each SSO.
- Enable Role Update. Role assignment is updated on each SSO.

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

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

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

### Archer Supported Attribute Mapping for SAML

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

Archer Field Name	Archer Supported Attribute Mapping
<b>User Identity Information</b>	
User Name*	NameID*
User Domain	UserDomain
First Name	FirstName



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

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

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

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

**Note:** For a list of all supported time zone ID values, see "Supported Time Zone ID Values" in the Archer Control Panel Help.

## Configuring the Instance Database Connection String and Pooling Options

You can configure the database connection string for either Windows Integrated Security or SQL Server encryption 2017, 2017 on Linux (Ubuntu), or 2019. It is recommended that you configure authentication with this database based on Microsoft's recommended best practices for secure authentication to a database. Archer supports using Integrated Security for connecting to the database.

- If using Windows Integrated Security, this option uses the current Windows identity established on the operating system thread to access the instance database. Selecting this option disables Login name and Password. Do not select this option if you are using SQL Server Authentication.
- If using SQL Server encryption, you must install separate certificates on each server (web application, services, and database) and you must enable encryption on the SQL server. Otherwise the connection will fail.
- If your application connects to an AlwaysOn availability group (AG) on different subnets, selecting the Multi-Subnet Failover option provides faster detection of and connection to the active server

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

### Configure the instance database connection string

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

1. On the instance you are configuring, go to the Connection Properties section.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click the instance.
  - c. Go to the Database tab, and then go to the Connection Properties section.
2. In the SQL Server field, select the database server for the instance.

3. Select the authentication method for connecting to the database server.  
Do one of the following:
  - If using Windows Integrated Security, select Use integrated security and skip to step 6.
  - If using SQL Server encryption, select Use encryption and continue at the next step.
  - If your application connects to an AlwaysOn availability group (AG) on different subnets, select the Multi-Subnet Failover option, and then continue at the next step. Enabling this option adds the following expression to the SQL connection string for the Instance database:  
`MultiSubnetFailover=True`
4. In the Login name field, enter the name of the SQL Server Authentication account.
5. In the Password field, enter the login password for the SQL Server Authentication account.
6. In the Database field, enter the instance database name.
7. Click Test Connection to test the connection string.
8. (Optional) In the Connection Timeout field, change the default duration of time for the connection timeout.
9. Designate the file repository path.

## Override the pooling options for the instance database

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

1. Click the Database tab, and then go to the Pooling section.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click to expand the Instances list.
  - c. Double-click the instance in the list that you want to configure.
2. In the Pooling field, click Override connection pool size.
3. In the Min pool size field, enter the minimum pool size.
4. In the Max pool size field, enter the maximum pool size.
5. On the toolbar, click Save.

## Changing SysAdmin and Services Account Passwords

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

The password expiration settings are not enforced for both the SysAdmin Account and the Services Account. However, after installing Archer, it is recommended that you change both passwords at least every 90 days using the Archer Control Panel. The new passwords must meet the security parameter configuration for the accounts. You can deactivate the sysadmin account, but cannot delete or rename it. Users cannot log into Archer with a Services Account.

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

### Change the SysAdmin password

1. On the Accounts tab, go to the SysAdmin Account section of the instance you want to update.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click the instance.
2. In the New Password field, enter the password for the SysAdmin account.
3. (Optional) Select Show Password to show the password as you enter it. If this option is not selected, the password is masked with substituted characters for the actual text.

### Change the Services Account password

1. On the Accounts tab, go to the Services Account section of the instance you want to update.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click the instance.
2. In the New Password field, enter the password for the Services account.
3. (Optional) Select Show Password to show the password as you enter it. If this option is not selected, the password is masked with substituted characters for the actual text.
4. Complete the Default Instance Creation.

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

## Configuring the Login Page

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

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

## Disable the domain field

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

## Display the login banner

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

## Database Authentication Methods

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

- SQL Server Authentication. Archer connects to each database using a SQL account created on the SQL Server instance. You provide the account information during the installation process.
- SQL Server databases. Archer connects to SQL Server 2017, 2017 on Linux (Ubuntu), or SQL Server 2019 databases for data storage. Restrict authorization to these databases to only the accounts that need access to the database.

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

- Data Read rights (member of db\_datareader)
- Data Writer rights (member of db\_datawriter)
- Execute permissions on all stored procedures and scalar functions
- Select permissions on all views, table-valued functions, and in-line functions
- Execute permissions on the system-stored procedure sp\_procedure\_params\_100\_managed

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

- **Integrated Security.** 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 Archer. This domain user account has DB Owner (DBO) access to the instance database that serves as the process identity for applications assigned to the application pool. DBO access is only required during the installation.

It is recommended that you create a custom domain services account dedicated to Archer for the IIS Application Pool Identity, and then provide it access to the necessary resources. In addition, be prepared to provide the same account credentials for the Archer Services account during the installation process.

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

## Authentication Configuration Methods

User authentication settings control the process of verifying an identity claimed by a user for accessing Archer.

A new installation of Archer is secure by Default (HTTPS protocol enabled) with anonymous authentication. Anonymous authentication is sufficient for most environments. For those environments where it is not sufficient, more sophisticated authentication methods are necessary. Configuring authentication methods requires changes to multiple server-side components, some of which are outside the scope of Archer.

**Important:** Before making any of the authentication configuration changes below, be sure to back up the Archer web.config file, the Configuration database, and the IIS settings.

**Note:** An incorrectly configured authentication method can prevent the entire Archer from being accessible.

The following are supported protocol methods.

### HTTPS/SSL protocol

The certificate for SSL must be available in the Server Certificates component (Machine Name > Server Certificates) within IIS. When the certificate is available, an https Binding which uses the SSL certificate must be added for the RSA web site.

Use the following tasks to configure IIS, the web.config files, and the Archer Control Panel for HTTPS/SSL.

**Note:** If you need to restore HTTP after configuring for HTTPS/SSL protocol, implement the process by undoing all the HTTPS/SSL steps.

## Configure IIS for HTTPS/SSL protocol

1. Select the Platform web site in the Connections pane.
2. In the Actions pane, click Bindings.
3. Click Add.
4. In the Type list, select the https option.
5. In the SSL certification list, select the applicable certificate.
6. Click OK.
7. Do one of the following:
  - To continue without removing the HTTP Site Binding, go to the next step.
  - To remove the HTTP Site Binding, do the following:
    - a. Select the HTTP Site Binding.
    - b. Click Remove.
    - c. Click Yes.
8. Click Close.
9. Perform an IIS reset.

## Configure Platform web.config file for HTTPS/SSL protocol

Archer must be configured to run either in HTTP or HTTPS, not both. Edit the Archer web.config in the base Archer web site directory.

1. Find the expression `<!-- for HTTPS`, and then do each of the following:
  - Replace `httpGetEnabled` with `httpsGetEnabled="false"`.
  - Uncomment the line `<security mode="Transport" />`.
  - Replace the `httpTransport` attribute with `httpsTransport`.
2. Find the expression `<customHeaders>`, and then add each of the following configurations in a separate new line within the custom headers section:
  - `<add name="Strict-Transport-Security" value="max-age=31536000; includeSubDomains" />`
  - `<add name="X-Content-Security-Policy" value="default-src 'self';" />`
  - `<add name="X-XSS-Protection" value="1; mode=block"/>`
3. Click Save.
4. Perform an IIS reset.

## Configure REST API web.config file for HTTPS/SSL protocol

The REST API child API IIS application inherits properties from the parent Archer application. Similar to the Platform web.config, Archer must be configured to run either in HTTP or HTTPS, not both. Edit the REST API web.config in the api directory within the base Archer web site directory.

1. Find the expression `<!-- for HTTPS`.
2. Replace `httpGetEnabled` with `httpsGetEnabled="false"`.
3. Uncomment the line `<security mode="Transport" />`.
4. Replace the `httpTransport` attribute with `httpsTransport`.
5. Click Save.
6. Perform an IIS reset.

## Configure Archer Control Panel for HTTPS/SSL

All URLs in the Archer Control Panel must include HTTPS.

1. Open the Archer Control Panel.
2. In Instance Management, double-click the instance you want to configure.
3. Click the Web tab.
4. Change all applicable Platform Web site URLs to include HTTPS.
5. Repeat steps 2 – 4 for all other instances.
6. Click Save All.

## Windows Authentication

The authentication mode must be set to Windows Authentication in IIS; if Windows Authentication is not available for selection, it must be installed. All other authentication modes must be disabled.

**Important:** The REST API does not support Windows Authentication. Windows Authentication must be disabled for the child API IIS application, and Anonymous Authentication enabled again.

Use the following tasks to configure IIS and the web.config file for Windows HTTP or HTTPS protocols.

## Configure IIS for Windows Authentication

1. Select the Platform Web site in the Connections pane.
2. Select the Authentication feature.



3. Set Windows Authentication to Enabled.
4. Disable all other authentication modes, for example, Anonymous.
5. Perform an IIS reset.

### **Configure Platform web.config file for Windows Authentication - HTTP**

Edit the Archer web.config file in the base Archer web site directory.

1. Find the expression `<!-- For Windows Authentication, change mode to 'Windows'.`
2. Replace `<authentication mode="None" />` with `<authentication mode="Windows" />`.
3. Find the expression `<!-- For Windows Authentication, and uncomment the lines.`
4. Uncomment the lines related to `<authorization><allow users="*" /></authorization>`.
5. Find the expression `<!-- For Basic Authentication (without SSL), and uncomment the lines.`
6. Uncomment the lines related to security mode.
7. Find the expression `<!-- for Windows Integrated Authentication, and add authenticationScheme="Negotiate".`
8. As instructed, add `authenticationScheme="Negotiate" />` to `httpTransport` or `httpsTransport`.
9. Click Save.
10. Perform an IIS reset.

### **Configure Platform web.config file for Windows Authentication - HTTPS**

Edit the Archer web.config in the base Archer web site directory.

1. Open the web.config file in a text editor.
2. Locate the `<authentication mode>` tag and change the authentication mode from None to Windows.
3. Locate the `<authorization>` and `<allow users>` tags and remove the comments.
4. Locate the `<serviceMetaData>` tab and change the HTTP identifier to HTTPS.
5. Locate the `<webHttpBinding>` section.
6. Remove the comments in the `<security mode>` and `<transport>` tabs identified for Windows Authentication and change the security mode as follows:

```
<security mode="Transport">  
<transport clientCredentialType="Windows" />  
</security>
```

7. Locate the <httpTransport> tag for the binaryHttpBinding.

8. Add the authenticationScheme="Negotiate" attribute to the tag and the HTTPS identifier.

```
<httpTransport maxReceivedMessageSize="1024000000" maxBufferSize="1024000000"  
authenticationScheme="Negotiate" />
```

9. Locate the <httpTransport> tag for the binaryHttpBindingStreaming binding.

10. Add the authenticationScheme="Negotiate" attribute to the tag and the HTTPS identifier.

```
<httpsTransport transferMode="StreamedRequest"  
maxReceivedMessageSize="1024000000" maxbufferSize="1024000000"  
authenticationScheme="Negotiate" />
```

11. Locate the <location> tag and remove the comments.

12. Save the web.config file

13. Perform an IIS reset.

## Single Sign-on for Windows integrated authentication

Use the following tasks to configure Single Sign-On for Windows integrated authentication.

### Configure Platform web.config file for Single Sign-On

Edit the Archer web.config file in the base Archer web site directory.

1. Find the expression `</configuration>`.
2. On a preceding blank line, insert `<location path="default.aspx"><system.web><authorization><deny users="?"></authorization></system.web></location>`.
3. Click Save.
4. Perform an IIS reset.

### Configure Archer Control Panel for Single Sign-On - Single Instance

1. Open the Archer Control Panel.
2. In Instance Management, double-click the instance you want to configure.
3. Click the Single Sign-On tab.
4. Select Windows Integrated as the single sign-on mode.
5. Click the Installation Settings tab.
6. Select the Default Instance box.
7. Click the arrow in the Instance list, and then select the instance.
8. Click Save All.

### Configure Archer Control Panel for Single Sign-On - Multiple Instances

1. Open the Archer Control Panel.
2. In Instance Management, double-click the instance you want to configure.
3. Click the Single Sign-On tab.
4. Select Windows Integrated as the single sign-on mode.
5. Click the Web tab.
6. Enter a unique Instance URL.  
**Note:** If a matching DNS entry does not exist for the Instance URL, it does not resolve.
7. Click Save.

## Enabling Kerberos Authentication

Use the following tasks to configure Windows authentication for single and multiple web hosts.

### Configure Windows Authentication for Single Host

If it does not already exist, an HTTP service principal name (SPN) must first be registered with the domain by a domain administrator. The following is the command to do so:

```
Setspn -S HTTP/{ArcherURL} {App Pool Identity}
```

For example, `Setspn -S HTTP/all.archer.local archer.local\Administrator` is the command to inject a SPN add into the domain if the following were true:

- Archer is installed into Default Web Site.
- The Archer URL is `https://all.archer.local`.
- The Archer Application Pool identity is: `archer.local\Administrator`.

If Archer is installed into the RSAArcher site—located inside of Default Web Site—the command to inject is `Setspn -S HTTP/all.archer.local archer.local\Administrator`.

1. Open Microsoft IIS.
2. Select the Archer site (default or otherwise).
3. Select Authentication.
4. Enable Windows Authentication.
5. Select Advanced Settings.
6. Unselect Enable Kernel-mode authentication and click OK.
7. Select Providers.
8. Select Negotiate: Kerberos from the Available Providers drop-down.
9. Click Add.
10. Move Negotiate Kerberos to the desired order under Enabled Providers and click OK.  
Ensure that these steps have been completed for at least the Archer site. These steps may also need to be performed to the Default Web Site and Server level components in IIS depending on your own needs.
11. Perform an IIS reset.

## Configure Windows Authentication for Multiple Web Hosts in Load-Balanced Environment

When IIS is run in clustered or load-balanced environments, applications are accessed using the cluster name rather than a node name. This scenario includes network load balancing. In cluster technology, a node refers to one computer that is a member of the cluster.

To use Kerberos as the authentication protocol, the application pool identity on each IIS node must be configured to use the same domain user account. To configure each IIS node to use the same domain user account, use the following command:

```
Setspn -A HTTP/CLUSTER_NAME domain\username
```

For example, the command may resemble the following:

```
Setspn -A HTTP/www.myIISCluster.com mydomain\appPool1
```

1. Open Microsoft IIS.
2. Select the Archer site (default or otherwise).
3. Select Authentication.
4. Enable Windows Authentication.
5. Select Advanced Settings.
6. Unselect Enable Kernel-mode authentication and click OK.
7. Select Providers.
8. Select Negotiate: Kerberos from the Available Providers drop-down.
9. Click Add.
10. Move Negotiate Kerberos to the desired order under Enabled Providers and click OK.  
Ensure that these steps have been completed for at least the Archer site. These steps may also need to be performed to the Default Web Site and Server level components in IIS depending on your own needs.
11. Perform an IIS reset.

## Chapter 3: Authorization

---

User Access Control .....	54
---------------------------	----

### User Access Control

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

- User accounts allow users to log on to Archer.
- User groups provide a means of grouping users based on organizational structure or geographic locations.
- Access roles are collections of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete).
- Security parameters are rules for controlling user access to Archer and its individual pages.
- LDAP synchronization streamlines the administration of users and groups by allowing updates and changes that were made in the LDAP server to be reflected automatically in Archer.

### Supporting your users

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

## Preventing social engineering attacks

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

- If Help Desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call the Help Desk back at a well-known Help Desk telephone number to ensure that the original request is legitimate.
- The Help Desk telephone number should be well known to all users.
- Help Desk administrators should only ask for user name of the user over the phone when they call the Help Desk. Help Desk administrators should never ask for user passwords.
- Help Desk administrators should authenticate the user's identity before performing any administrative action on a user's behalf. It is recommended that you verify user identity using the following methods:
  - Call the user back on a phone owned by the organization and on a number that is already stored in the system.
    - Important:** Be careful when using mobile phones for identity confirmation, even if they are owned by the company because mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.
  - Send an email to the user at a company email address. If possible, use encrypted email.
  - Work with the manager of the employee to verify the user identity.
  - Verify the identity in person.
  - Use multiple open-ended questions from employee records. For example: "Name one person in your group." or "What is your badge number?" Avoid yes or no questions.

### Confirming user identities

It is critical that your Help Desk administrators verify each end-user identity before performing any Help Desk operations. It is recommended that you verify user identities using the following methods:

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

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

- Send an email to the user at a company email address. If possible, use encrypted email.
- Work with the employee's manager to verify the user's identity.
- Verify the identity in person.
- Use multiple open-ended questions from employee records. For example: "Name one person in your group." or "What is your badge number?" Avoid yes or no questions.

### Advice for your users

It is recommended that you instruct your users to do the following:

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

**Note:** It is recommended that you conduct regular training to communicate this guidance to users.



## Entity permissions

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

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

Component	Permissions Explanation
Workspaces, Dashboards, Global iViews	Configured from the Access tab in a workspace or dashboard. It is recommended that you configure these components to be private.
Global Reports	Configured when you save a report. It is recommended that you set the Permissions field to Global Report.
Record Permissions	Configured in a Record Permissions field in an application or questionnaire.
Field Permissions	Configured in the Access tab in a field in an application or questionnaire. It is recommended that you configure fields to be private.
Configuration Administrators	Configuration administrators have rights to the configuration aspects (for example, fields, layout, data-driven events, notifications) of an application, questionnaire or sub-form. Configuration administrators have read rights to the content page for the application or questionnaires.
Content Administrators	Configured in applications and questionnaires. Inherently grants CRUD rights to all content within the application or questionnaire regardless of record permissions.
Global Report Administrators	Configured in Application Builder for the assigned report owners in a specific application or questionnaire.

## Default User Accounts

- When you create a new instance, you must enter a password for the sysadmin and service accounts.
- Standard users cannot log on to any of the default user accounts.

- Only the System Administrator can log on to the sysadmin account. You cannot delete or rename any of the default user accounts.

The following table describes the default Archer user accounts of a System Administration (sysadmin) account and several Archer services accounts.

User Account	Account type	Account used for	General Information
sysadmin	system administrator	Archer	Can be disabled, but cannot be deleted or renamed.
userArcherAssetServer	service	Asset service	Can only be used by Archer services.
userArcherAsyncService	service	Job management	Can only be used by Archer services.
userArcherCalculationAccount	service	Calculations	Can only be used by Archer services.
userArcherDataFeedService	service	Data feeds	Can only be used by Archer services.
userArcherLdapService	service	LDAP synchronization	Can only be used by Archer services.
userArcherNotificationService	service	Notifications	Can only be used by Archer services.
userMigrationUser	service	Migration	Can only be used by the installer.
userOfflineService	service	Offline access	Can only be used by Archer services.

## Adding User Accounts

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

### Configuring new accounts

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

### New User Accounts

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

- The system administrator assigns the password manually. It is strongly recommended that you enable the Force Password Change with the Next Sign-In option in Archer for all new user accounts. Configuring this option requires the user to change the password after the first successful logon attempt.
- If the single sign-on feature is in place on your system, Archer automatically creates a random password for each new user.

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

### New User Account with System Administrator Privileges

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

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

### Platform User Accounts

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

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

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

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


It is recommended that you treat these settings as the minimum requirement for enforcing strong passwords and secure sessions in Archer.

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

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

**Important:** If you activate the Account Lockout Message option in the Archer Control Panel, the message displayed to the user indicates a locked Archer account. Deactivate this option to prevent unauthenticated users from accessing status information about Archer user accounts.

### Add a user account

1. Go to the Manage Users page.
  - a. From the menu bar, click  .
  - b. Under Access Control, click Users.
2. Click Add New.
3. In the General Information section, enter the name of the user, the user name for log on, and the domain.

The following table describes each property.

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

4. (Optional) In the Contact Information section, enter the default email address and any other pertinent information for contacting the user.

The following table describes each property.

Property	Description
Address	The complete address of the user.
Company	The company name.
Title	The title of the user.

Property	Description
Email	<p>The following user email types are available:</p> <ul style="list-style-type: none"> <li>• Business</li> <li>• Business 2</li> <li>• Home</li> <li>• Home 2</li> <li>• Mobile</li> <li>• Mobile 2</li> <li>• Other</li> <li>• Other 2</li> <li>• Pager</li> </ul>
Phone	<p>The following user telephone number types are available:</p> <ul style="list-style-type: none"> <li>• Assistant</li> <li>• Business</li> <li>• Business 2</li> <li>• Business Fax</li> <li>• Home</li> <li>• Home 2</li> <li>• Home Fax</li> <li>• ISDN</li> <li>• Mobile</li> <li>• Mobile 2</li> <li>• Other</li> <li>• Other 2</li> <li>• Other Fax</li> <li>• Pager</li> </ul>

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

The following table describes the options.

Option	Description
Time Zone	The time zone for the location of the user. Time is based on Coordinated Universal Time (UTC). All time is stored as UTC and converted based on the time zone of the user.
Locale	The physical location of the user.
Manually select a language	Overrides the default language set for the instance. When you select this option, you must specify the language.

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

The following table describes each property.

Property	Description
Status	The current status of the user account. The options are Active, Inactive, or Locked.
Password	<p>For new user accounts, the password must be entered and confirmed. These entries must match exactly. The password must conform to the default security parameter password rules.</p> <p>For existing user accounts, use the Change Password link to change the password manually.</p> <p>The Send user a notification with password information option enables Archer administrators to notify new users that the user account has been setup with a temporary password and may require a password change.</p>
Force Password Change	Determines whether the user is forced to change the password the next time the user logs in.
Security Parameter	The security parameter assigned to the user. A user can only have one security parameter assigned at a time.
Notifications, Subscriptions	Enables users to select the records and applications for which they want to receive notifications when an update occurs.
Default Home Page	<p>Sets a user's default home page to use either a task-driven landing page or a dashboard based on group, role, or user profile. If the user belongs to multiple roles or groups, the home page is based on the most recently assigned role or group. Once the user logs in, the selected home page becomes default and any changes to the home page of the role or the group do not affect the user's default home page.</p> <p><b>Note:</b> If the user's permission to access the dashboard assigned to the home page is revoked, a message appears upon log in allowing them to select a new home page.</p> <p><b>Important:</b> If the administrator sets the default home page while the user is logged in, the user must click the Home button to refresh the home page setting. If the user changes the default home page selection, the change is applied upon clicking Save.</p>
Default Home Dashboard	Sets which dashboard displays on the default home page.

Property	Description
Enable Advanced Workflow Actions by Email for this user	<p>Allows this user to complete simple advanced workflow actions from their email.</p> <p><b>Important:</b> To use Advanced Workflow Actions by Email you must:</p> <ul style="list-style-type: none"> <li>• Have a user account with Actions by Email enabled. For more information, see "Adding User Accounts" or "Updating User Accounts" in the Archer Online Documentation.</li> <li>• Enable Actions by Email in all applicable applications, questionnaires, notification templates, and advanced workflows.</li> <li>• Configure the Archer Control Panel to enable Actions by Email for on-premises deployments. This step is not required for SaaS deployments. For more information, see "Configuring Advanced Workflow Actions by Email" in the Archer Control Panel Help.</li> <li>• Configure your email service to use the Transport Layer Security (TLS) encryption protocol, which is enforced by the Amazon Web Services (AWS) mail service for SaaS deployments. This step is not required for on-premises deployments.</li> </ul> <p><b>Note:</b> Advanced Workflow Actions by Email is not supported for SaaS deployments in the APJ region. This feature relies on native services provided by AWS which are not currently available in APJ.</p>

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

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

8. (Optional) In the Notes section, record any additional information about the user account, for example, list hours of availability or preferences for how the user should be contacted. Account notes appear when users click a linked user name in Archer to view the user profile.
9. Click Save or Save and Close.
  - To apply the changes and continue working, click Save.
  - To save and exit, click Save and Close.



## Access Roles

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

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

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

For instructions on assigning permissions through group membership, see [Assigning Access Roles to Users and Groups](#).

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

### Importing access roles

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

## Adding Access Roles

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

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




### Page-level rights

The following table describes page-level rights.

Rights	Description
Create	Create new page content, such as records, fields, notification templates, and content review stages.

Rights	Description
Read	Read page content.
Update	Modify existing page content.
Delete	Delete page content.

### Add an access role

1. Go to the Manage Access Role page.
  - a. From the menu bar, click .
  - b. Under Access Control, click Access Roles.
2. Do one of the following:
  - If you want to create a new access role, click .
  - If you want to create a new access role from an existing access role, click  from the Actions area of the Access Role you want to copy.
3. In the General Information section, enter a name and description for the access role.
4. (Optional) To enter an Alias, click Save, and then enter an Alias name in the General Information section.
5. (Optional) To set access role as the default for all users and groups, in the Default Home Page field of the General Information section, click Assign as Default.
6. (Optional) In the Group Assignments section, assign groups to the access role.
7. Click Save.
8. On the Rights tab, and select the Create, Read, Update, and Delete (CRUD) checkboxes that correspond to the appropriate rights for each page type.
  - User or group access to the Manage Global Values Lists page provides access to all global values lists in Archer. If you want a user to have access to specific global values lists and not all lists, select the appropriate CRUD access for the individual global values list.
  - If you grant access rights to import data, you must also grant rights to the content record that data will be imported into. For example, users can import data into the Policies application only if they have access to Integration: Data Imports; Create, Read, and Update rights to Policies: Content Record; and Policies: Data Import.

9. Click Save or Save and Close.

- To apply the changes and continue working, click Save.
- To save and exit, click Save and Close.

## Assigning Access Roles to Users or Groups

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

Immediately after installation, it is recommended that you configure access roles as follows:

- Create a new access role with no rights and make it the default role. Grant additional roles to users as needed for appropriate access in Archer.
- Create read-only roles that can be used by an auditor. It is recommended that these roles only have permissions to view reports, configurations, and logs.
- Create a new Security Administrator role that has full rights to Access Control. Grant the Security Administrator role access rights to managing roles.
- Configure access roles to grant non-administrative users only the rights they need for each task based on their role in the organization. You can grant multiple access roles to each user. It is recommended that these roles do not have permission to view or modify security configuration.

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

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


For example, one access role grants create, read, and update privileges in the Policies applications and another access role grants only delete privileges. A user who is assigned both access roles has create, read, update, and delete (CRUD) privileges in the Policies applications.


### Role Assignment by Group or User

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

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

### Assign an access role to a user


1. Open the user account to which you want to assign an access role.
  - a. From the menu bar, click .
  - b. Under Access Control, click Users.
  - c. Select the user account.
2. Click the Roles tab.
3. Click Lookup.
4. In the Available list, expand the Roles tree, and click the access role to assign.

**Note:** To search for a specific role, enter the role name in the Find field and, if applicable, select the type from the adjacent list. Click . The results of your search appear in the Available list in the Search Results node.
5. Click OK.
6. Click Save or Save and Close.
  - To apply the changes and continue working, click Save.
  - To save and exit, click Save and Close.

### Assign an access role to a user group

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



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

1. Open the access role to which you want to assign a user group.
  - a. From the menu bar, click .
  - b. Under Access Control, click Access Roles.
  - c. Select the access role.
2. In the Group Assignments section, click Assign to Group.
3. From the Available list, expand Groups, and select the group or groups to which you want to assign the access role. You can also use the Search field to search for a specific group.

4. Click Save or Save and Close.
  - To apply the changes and continue working, click Save.
  - To save and exit, click Save and Close.

### Unassign an access role from a user account

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

1. Open the user account from which you want to unassign an access role.
  - a. From the menu bar, click .
  - b. Under Access Control, click Users.
  - c. Select the user account.
2. Click the Roles tab.
3. From the Selected list, click  to remove the applicable access role from the user.
4. Click Save or Save and Close.
  - To apply the changes and continue working, click Save.
  - To save and exit, click Save and Close.

## Privilege Levels for Archer Services

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

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

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

## Least Privileges Requirement for Archer Database Objects

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

- Data Reader Rights (member of the db\_datareader).
- Data Writer Rights (member of the db\_datawriter).
- Execute permissions on all stored procedures and scalar functions.
- Select permissions on all views, table-valued functions, and in-line functions.
- Execute permissions on the system stored procedure sp\_procedure\_params\_100\_managed of the parent database.
- Execute permissions on the user-defined table type content\_date\_Table\_Type of the Platform Instance database.
- Reference permissions on the user-defined table type content\_date\_Table\_Type of the Platform Instance database.
- Execute permissions on the \_BulkType user-defined table types of the Platform Instance database, if provisioned for Offline Access.
- Reference permissions on the \_BulkType user-defined table types of the Platform Instance database, if provisioned for Offline Access.

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

When installing or upgrading Archer, use an account with a membership to the db\_owner.

## Chapter 4: Network Security

Port Usage .....	71
Network Encryption .....	78
Host Hardening .....	95

### Port Usage

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

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

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

You can modify the following ports:

- Configure the port used for SQL in SQL Server.
- Configure the port used for HTTPS in Microsoft IIS.

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

<b>Purpose</b>	<b>Source</b>	<b>Destination</b>	<b>Protocol</b>	<b>Port (Default)</b>	<b>Mandatory or Optional</b>
Client Web Connectivity	Platform Web UI	Web Server (IIS) or Load Balancer	HTTP(S)	80/TCP, 443/TCP	Mandatory
	See <a href="#">Web Server Communication</a> . The destination is a Load Balancer if the Platform is deployed with a web server cluster or farm. It is recommended that you rely only on HTTPS.				

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



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

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
LDAP Queries	LDAP Synchronization Service	[LDAP Server]	LDAP(S)	389/TCP (LDAP), 636/TCP (LDAPS over SSL), 3268/TCP (LDAP), 3269/TCP (LDAP to GC over SSL)	Optional
<p>Only required if performing LDAP synchronization. You can change the default port for use by your application.</p> <p><b>Note:</b> If you have more than 1000 users, it is recommended that you use a Global Catalog (GC) connection. For more information, see the Knowledge Base article, "LDAP Sync Unable to Create More Than 1000 Users in Archer," at <a href="https://community.rsa.com/t5/archer-knowledge-base/ldap-sync-unable-to-create-more-than-1000-users-in-rsa-archer/ta-p/5281">https://community.rsa.com/t5/archer-knowledge-base/ldap-sync-unable-to-create-more-than-1000-users-in-rsa-archer/ta-p/5281</a>.</p>					
Audit Logging	Web Server (IIS)	[Remote Host]	TCP/UDP	Varies	Optional
<p>Only required if Audit Logging is enabled.</p>					
Email Notifications	Job Engine Service	[SMTP Server]	SMTP(S)	25/TCP (SMTP), 465 (SMTPS)	Optional
<p>Only required if using email notifications. You can change the default port for use by your application.</p>					
Mail Monitor	Job Engine Service	[POP3 or IMAP Server]	POP3(S), IMAP(S)	110/TCP (POP3), 995/TCP (POP3S), 143 (IMAP), 993/TCP (IMAPS)	Optional

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	Only required if leveraging Mail Monitor functionality.				
Read Receipts	Job Engine Service	[POP3 or IMAP Server]	POP3, IMAP	110/TCP (POP3), 143 (IMAP)	Optional
	Only required if leveraging Read Receipt functionality.				
Configuration Data	All clients of the Configuration Service	Configuration Service REST API		13200/TCP	Mandatory
	Required for communication between clients and the Configuration Service using REST API.				
	All clients of the Configuration Service	Configuration Service	WCF	13201/TCP	Mandatory
	<p>Required for communication between clients and the Configuration Service using WCF.</p> <p>In a multiple server Archer deployment, the Configuration Data Retrieval ports do not need to be open between servers. Configure each server to have its Web Service communicate with the Configuration Service on the same server.</p>				
	LDAP Synchronization Service	Configuration Service	WCF	13201/TCP	Optional
	Only required if using LDAP synchronization.				
	Configuration Service	Web Server (IIS)	WCF	13202, 13300-13304/TCP	Mandatory
	<p>Required to push configuration data updates to the web servers.</p> <p>In a multiple server Archer deployment, configure any Configuration Service to communicate with any Web Servers using the Configuration Data ports.</p>				

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	Configuration Service	Job Engine Service, Queuing Service	WCF	13305-13350/TCP	Mandatory
<p>Required to push configuration data updates to Archer services.</p> <p>In a multiple server Archer deployment, configure any Configuration Service to communicate with any destination service that runs on other servers, using the Configuration Data ports.</p>					
	Configuration Service	LDAP Synchronization Service	WCF	13305-13350/TCP	Optional
<p>Only required if using LDAP synchronization.</p> <p>In a multiple server Archer deployment, configure any Configuration Service to communicate with the LDAP Synchronization Service on any server using the Configuration Data ports.</p>					
	Configuration Service	Content API	WCF	13351-13355/TCP	Optional
<p>Only required if using the Content API.</p> <p>In a multiple server Archer deployment, configure any Configuration Service to communicate with the Content API on any server using the Configuration Data ports.</p>					
	Configuration Service	Mobile API	WCF	13356-13360/TCP	Optional
<p>Only required if using the Mobile API.</p> <p>In a multiple server Archer deployment, configure any Configuration Service to communicate with the Mobile API on any server using the Configuration Data ports.</p>					
SSO Authentication	Web Server (IIS)	[Remote Host]	Varies	Varies	Optional

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

Purpose	Source	Destination	Protocol	Port (Default)	Mandatory or Optional
	<p>Only required if using the Advanced Workflow feature.</p> <p>You can change the default port for use by your application. Be sure that the support port number is available for use.</p> <p>The services server communicates when a new record is enrolled in an advanced workflow.</p> <p>The Advanced Workflow service requires dedicated port on the configured servers to communicate with Archer.</p>				
Elasticsearch	Indexing Service, Web Server	[Elasticsearch Cluster Node]	HTTP(S)	9200 to 9300	Mandatory
	<p>Only required if using the Elasticsearch feature. You can change the default port for use by your application.</p>				
Other Data Feeds	Job Engine Service	[Remote Host (s)]	Varies	Varies	Optional
	<p>Only required if using Archer to pull data from other systems using transfer protocols, for example, FTP, SMB, and SQL. The destinations, ports, and protocols vary based on your implementation. You can change the default port for use by your application.</p>				

## Network Encryption

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

- [Data Feeds](#)
- [Web Server Communication](#)
- [SSL Certificate Guidance](#)
- [SQL Server Communication](#)
- [Archer Web Services API](#)

## Data Feeds

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

- Configure multiple, dynamic data feeds, and manage those feeds without relying on programming resources.
- Build and configure dynamic integrations with external enterprise systems and files. From Data Feed Manager, you can build a transport path between Archer and an external source and then map the data from that source to an existing target application or questionnaire in Archer.
- Configure the data feed to run on a schedule. After the initial configuration, the data feed executes automatically with no need for you to intervene.

You can integrate data using Data Feed Manager for:

- Network and asset discovery data
- Vulnerability scan results
- Performance scorecards
- Incident reports
- Audit results and recommendations

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

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

### Data feed types

**Important:** To avoid potential conflicts with other data feeds, it is recommended that you use a different service user for each data feed. For more information, see [Data Feed Service Account](#).

Data Feed Manager supports standard and transport data feeds.

The following table describes each type of data feed.

Feed Type	Description
Standard	<p>Brings data from an external source into an application or questionnaire. This data feed type requires that you:</p> <ul style="list-style-type: none"> <li>• Define the fields and data format.</li> <li>• Map the fields in the source file to the target.</li> <li>• Configure a transport type that successfully imports the source data into another application or questionnaire. For example, perform a report-based search for an application or questionnaire that contains the source data that you want to import into another application or questionnaire.</li> <li>• Select a <a href="#">Data Feed Service Account</a>.</li> </ul> <p>You can specify the following:</p> <ul style="list-style-type: none"> <li>• Whether to send subscription notifications to specified users or groups when records are modified.</li> <li>• Whether to send a notification to specified users or groups when a data feed job completes, identifying a successful or failed completion.</li> <li>• The locale format of your source data. For example, different characters might be used to indicate a decimal place.</li> </ul>
Transport Only	<p>Creates the specified data file that subsequent, standard data feeds can use as input and that can be reviewed to understand the data structure that a transport configuration returns. For example, to review the configuration of the output file that an HTTP data feed returns, run the data feed as a Transport Only feed. The output allows you to determine how to configure the XSLT to generate source fields to use for data mapping.</p> <ul style="list-style-type: none"> <li>• Ensure that a user account for the data feed and a target path for the separate data file exist, but no additional data configuration.</li> </ul>

### Data feed transporter types

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

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

Transporter	Description
Archer Web Services	Accesses the Web Services API and retrieves data from an instance of Archer This transporter is used in Archer-to Archer data feeds.
Database Query	Returns results using an SQL query



<b>Transporter</b>	<b>Description</b>
File	Retrieves delimited data files, including support for multi-file manifests
FTP	Retrieves data files using the FTP protocol
HTTP	Runs a GET or POST to retrieve data from an HTTP or HTTPS site.
JavaScript	Runs a user-provided JavaScript file If the result of that run is a data set, it is transformed and processed into the platform as normal.
Mail Monitor	Retrieves content from monitored email accounts
RSS	Retrieves records from a configured RSS feed

### **Supported and unsupported field types for data mapping**

#### **Supported Field Types**

- Attachment
- CAST Detail
- Cross-Reference
- Date
- External Links
- Image
- IP Address
- Matrix
- Numeric
- Record Permissions
- Related Records
- Sub-Form
- Text
- Tracking ID
- User/Groups List
- Values List

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

### Unsupported Field Types

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

### Schema sources

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

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

Source	Description
Execute Search	Runs the search in Archer and detects the source schema from the results Recommended approach for an Archer-to-Archer data feed. Loads the source fields directly from the report. When using this scheme, complete all required information on the Transport and Navigation tabs.
Execute Query	Runs the query specified on the Transport tab and detects the source schema from the resulting record set Using this option may trigger actions in the database associated with this query.

Source	Description
Sample File	<p>Uses a skeleton of your actual source data file. For example, if you are importing data from a .csv file, the source data file is a .csv file that includes the column names from your source data. If you are importing data from an .XML file, the source data file includes the structure of your .XML without the actual field values.</p> <p>When you select the sample file, the Source Fields section populates with the fields specified in the sample data file.</p> <p>For the Archer Web Services Transporter, select a file from an external location that contains the data in the same format as the report format.</p>
Load URL	<p>Loads the contents at the target URL and detects the source schema from the contents</p> <p>Using this option may trigger actions associated with accessing the target URL.</p>
Standard Schema	Uses the standard mail schema

### Updating locked records

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

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

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

### Key Fields

You can use key fields from the source data to identify matching records in a target application or questionnaire. Keys defined within Data Feed Manager are different from keys defined within the Application Builder.

The following table lists the valid key field types from a target application or questionnaire.

Text-Based Field Types	List-Based Field Types
Text	Values Lists
Numeric	Record Permissions

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

The following restrictions apply to key fields:

- You can only use the Tracking ID as a key field if you configure the field as System ID. If you configure the field as Application ID, then you cannot use Tracking ID as a key field.
- If you map a source field for a sub-form and that source field value is blank, then the data feed will not process the sub-form record.

#### Simple keys and combination keys

Simple keys include only one field. Each key has a different order number, and the data feed processes the keys in the specified order. The data feed updates existing records from the source data in the target application or questionnaire using a simple key.

For example, each person has a unique Individual Taxpayer Identification Number (ITIN) or Social Security Number (SSN). Simple keys that consist of either the ITIN or SSN fields can identify records based on only those fields.

Combination keys allow you to select multiple fields to create a single key. By establishing a combination key, the order of each field within the key matches.

For example, first name and last name are two simple keys. By combining both the first name and last name fields into a combination key, the data feed uses the combination key as a single key to identify records.

#### Use of multiple keys

Archer allows users to define multiple keys and define the order of processing to identify matching records. After you set the order number of each key, the data feed scans the source data for matches to each key in the specified order. If a key is a combination key, all fields in the key from the source data must match the corresponding fields in the target record. The data feed continues the following process until it finds a match or until it processes all keys.

- If the first key from the source data matches the corresponding field in the target record, the source data updates the target record data.
- If the data feed does not find a match for the first key, it attempts to find a match using each consecutive key.

- If the data feed does not find a match or no keys are left to scan, then it creates a new application or questionnaire record.

For example, you can configure keys in the following order: ITIN, first name, and last name.

- If the data feed identifies a matching record using the ITIN, a key unique to each user, it stops processing the records.
- If the data feed cannot find matching records based on the first key, ITIN, it uses the second key, first name, to find a match.
- If the data feed cannot find matching records based on the second key, first name, it uses the third and last key, last name, to find a match.
- If there are still no matching records, the data feed creates a new application or questionnaire record using the source data.

#### Matching criteria for list-based field types

The following table describes the matching criteria for list-based field types.

Option	Description
MatchExact	<p>Specifies that the values in the target record field and the values in the source data field must match to update the target record. If the match is not exact, the data feed creates a new record.</p> <p>For example, a field in the target application record contains a list with the values Red, Blue, and Green, and the source data field contains a list with the values Blue, Green, and Red. Since the list in the target application record matches the exact values in the source data list, then the data feed updates the target record.</p>
MatchAny	<p>Specifies that at least one value in the source data field must match at least one value in the target record field for the data feed to update the target record. If no values match between both fields, the data feed creates a new record.</p> <p>For example, if a target application record has the values Blue and Green selected in the key field, and the mapped field in the source data includes only the value Blue, the data feed updates the record because at least one of the values matches.</p>

Option	Description
MatchAll	<p>Specifies that all values in the target record field must contain all values included in the source data field for the data feed to update the target record. If the target record field does not include all source data values, the data feed creates a new record.</p> <p>For example, if the target application record has the values Red, Blue, and Green selected in the key field, and the mapped field in the source data includes the values Red and Green, the data feed updates the record. However, if the target record source data has the values Red, Blue, and Yellow, the data feed does not update the record.</p>

### Data Feed Service Account

A data feed Service Account is an account that the system specifically uses to run a data feed. The Service Account user also creates and updates content in a data feed. When configuring a data feed, users can either choose an existing Service Account or create a new Service Account. Users can use the same Service Account to run every data feed, but for troubleshooting purposes, set up different Service Accounts for each data feed. Users cannot log into Archer with a data feed Service Account. History Log fields display field changes made by data feed Service users. Associating a unique data feed Service Account to each feed clarifies which data feed applied the update.

### Data feed communication

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

To strengthen data feed security, it is recommended that the Data Feed Manager require data feed paths to be specified as relative paths.

**Note:** Relative path entry is set up as the default.

### BatchContentSave data feed token

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

### Archer-to-Archer Data Feeds

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

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

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

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

### Archer Web Services Transporter

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

#### Guidelines for designating the security credentials

- If IIS is configured for Anonymous authentication, use the Anonymous/Service Account User option. When IIS is set to Anonymous authentication, the user account credentials are not sent with the data feed request.
- If IIS is configured for Windows Integrated authentication, use either Anonymous/Service Account User or Specific.
  - If credentials are set to Anonymous/Service Account User, the service account running the asynchronous job is sent with the data feed request.
  - If credentials are set to Specific, the specified Windows account credentials are sent with the data feed request.

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

Search Type	Description
Report ID	Retrieves data using the search report GUID or ID, which is provided in the search results for the report.

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

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

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

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

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

### RSS Data Feeds

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

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

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

Use the following tasks to add an RSS data feed:

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

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

### HTTP Data Feeds

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

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



## HTTP Transporter

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

It is recommended that you disable the HTTP Transporter if a business need does not require its use. If you must use the HTTP Transporter, it is recommended that you use HTTPS, select Zip File as the File Type, and use encryption by selecting an Encryption Type.

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

## Weak ciphers disabled

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

For more information about disabling weak ciphers, see [Host Hardening](#).

Use the following tasks to add an HTTP data feed:

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

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

## FTP Data Feeds

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

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

## FTP Transporter

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

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

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

Use the following tasks to add an FTP data feed:

### **File Data Feeds**

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

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

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

### **File Transporter**

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

It is recommended that you disable the File Transporter if a business need does not require its use. If the File Transporter must be used, it is recommended that you set the Zip File as the File Type and use encryption by selecting an Encryption Type.

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

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

Use the following tasks to add a file data feed:

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

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

### **Mail Monitor Data Feeds**

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

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

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

**Note:** It is recommended that you configure an SSL connection to connect with the email server.

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

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

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

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

### Database Query Data Feeds

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

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

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

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

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

- Adding Standard Database Query data feeds
- Adding Transport Only Database Query data feeds

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

## Web Server Communication

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

- HTTP using default port 80
- HTTPS using default port 443

These web clients include:

- Archer web user interface
- Third-party web applications, which are applications provided by the customer that use Archer web APIs (SOAP and REST)
- Certain data feeds, for example, RSS and Threat Intelligence

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

- IIS
- Archer web.config
- Archer Control Panel

For more information, see [Appendix A: Authentication Configuration](#).

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

- Redirecting connections from an unsecured HTTP port to a secured HTTPS port can cause your application to be vulnerable to these types of attack. Redirecting connections is not a complete disablement of the HTTP port.
- Disabling HTTP without ensuring that the SSL certificate is in the trusted certificate store displays an error message.
- Disabling HTTP causes the SOAP API forms to become non-functional. These forms only accept HTTP Post.

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

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

## SQL Server Communication

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

The Configuration database accepts secure or encrypted connections. It is recommended that you follow the guidance in [SSL Certificate Guidance](#) when issuing an SSL certificate to communicate with SQL Server.

### (Optional) Use encryption

Select the Use Encryption option in the Archer Control Panel to encrypt communication between the Archer servers and SQL Server.

**Note:** If you deactivate the Use Encryption option in the Archer Control Panel, but if Force Encryption is activated on SQL Server, then SQL Server will not accept the unencrypted data.

### (Optional) Force Encryption

Configure the Force Encryption option in SQL Server to only accept encrypted data sent from the Archer servers to SQL Server. For more information, see the [Microsoft SQL documentation](#).

After configuring the encryption, restart the services and reset IIS on the Archer Web Servers. Verify that there is an encrypted connection between SQL Server and the Archer servers.

## Application Programming Interface (API)

Archer provides three types of APIs for your use.

- [Web Services API](#)
- RESTful API
- Content API

With general API usage, it is recommended that you log and regularly audit the source, time, and summary data submitted and received by APIs.

For more information on the Application Programming Interface, see the Archer Online Documentation.

## Archer Web Services API

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

## Archer Web Services

It is recommended that you rely on HTTPS for secure communications between the Archer web server and the following:

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

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

The following table lists web services that are available.

<b>Available Web Services</b>	
Access Control	The Access Control class provides programmatic access to the Access Control feature, such as creating users and managing security parameters.
Access Role	The Access Role class provides programmatic access to options relating to managing access roles.
Field	The Field class allows you to manage and configure the values lists used in the applications, questionnaires, and sub-forms.
General	The General class allows you to create and terminate Web Services API user sessions.
Module	The Module class provides programmatic access to module information.
Record	The Record class allows you to create and manipulate content records in content applications.
Search	The Search class allows programmatic access to the Platform's search features.

## Proxy Bypass Security Considerations

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

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

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

- Only bypass external systems which have SSL/TLS protection enabled to allow communication with internal systems.
- Only bypass external systems with strong authentication systems in place.
- Only bypass URLs/IPs approved by your IT department.

## Host Hardening

To ensure secure operation of Archer, the underlying components of the host must be hardened so that the server will function properly and opportunities for vulnerabilities are removed.

Archer recommends hardening the host system under it to only allow TLS 1.2 on all Archer supported clients and servers.

- Make sure that SQL servers, Web Services, and clients have the latest service packs using TLS 1.2.
- Make sure that all security updates are applied before additional hardening is performed on all underlying components, including, but not limited to, the Operating System, SQL, and IIS.

## Recommendations for TLS/SSL cipher hardening

Once all underlying components are up-to-date, TLS/SSL cipher hardening can be applied. A cipher suite is a set of algorithms that help secure a network connection using Transport Layer Security (TLS). Cipher hardening will prevent known cipher attacks in TLS/SSL (for example, Sweet32, BEAST, POODLE).

### Disabling SSL 2.0 and SSL 3.0

Disable the SSL 2.0 and SSL 3.0 protocols due to issues including the POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability.

### Disabling TLS 1.0 and 1.1

Unless your environment requires supporting legacy browsers, disable TLS 1.0 and 1.1.

### Disabling weak ciphers

Web server communication over HTTP relies on the SSL/TLS ciphers and key lengths provided by the version of IIS on which Archer is installed. Ensure that IIS is configured for cryptographic support, which cannot be easily defeated. It is recommended that you configure Microsoft IIS to only allow ciphers with key lengths of 128 bits or greater.

Weak ciphers, such as DES and RC4, should be disabled.

## Cipher configuration

A chosen Cipher Suite is unique to the security guidelines set forth by a user's organization. It is usually based on the level of restrictions required in the server environment, as well as the age of the software and devices connecting to the servers (for example, the need to support legacy browsers and regulatory requirements).

Users should implement a Security Best Practices cipher suite with Triple DES168 Cipher excluded (from SChannel) on Archer Servers including the web. It is recommended that you place the most secure cipher suites first because servers often select the first supported suite from the client's list.

As guidance, Archer has been tested with, as limited as, the following list of Cipher Suites and the product remains functional:

Hexcode	Cipher Suite Name (OpenSSL)	KeyExchange	Encryption	Bits	Cipher Suite Name (RFC)
xc028	ECDHE-RSA-AES256-SHA384	ECDH 521	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
xc014	ECDHE-RSA-AES256-SHA	ECDH 521	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
x9d	AES256-GCM-SHA384	RSA	AESGCM	256	TLS_RSA_WITH_AES_256_GCM_SHA384
x3d	AES256-SHA256	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA256



Hexcode	Cipher Suite Name (OpenSSL)	KeyExchange	Encryption	Bits	Cipher Suite Name (RFC)
x35	AES256-SHA	RSA	AES	256	TLS_RSA_WITH_AES_256_CBC_SHA
xc027	ECDHE-RSA-AES128-SHA256	ECDH 521	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
xc013	ECDHE-RSA-AES128-SHA	ECDH 521	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
x9c	AES128-GCM-SHA256	RSA	AESGCM	128	TLS_RSA_WITH_AES_128_GCM_SHA256
x3c	AES128-SHA256	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA256
x2f	AES128-SHA	RSA	AES	128	TLS_RSA_WITH_AES_128_CBC_SHA

### **Verify cipher configuration**

You can use various tools to verify the Cipher Suite hardening that you have enabled. Cipher Suite hardening may lead to limited connectivity; old clients cannot connect to servers with strong security requirements. Some of the tools will provide the details on these limitations.

### **Special cipher vulnerability cases**

- **BREACH (CVE-2013-3587)** - This cipher vulnerability is related to web server HTTPS Compression and can be handled via Web Server / Load Balancer Configuration.
- **LUCKY13 (CVE-2013-0169)** - This cipher vulnerability is a timing attack used against implementations of the TLS protocol using the Cipher Block Chaining (CBC) Ciphers. To prevent this vulnerability, make sure that you do not use cipher suites in the CBC mode.

## Chapter 5: Data Security

---

Encryption of Data at Rest .....	99
Encrypting Data .....	100
Configuring the Hardware Security Module .....	102
File Repository Path .....	103
Restrict Permissions on Repository Files .....	103
Keyword Index Files .....	104
Company Files Path .....	104
Disabling Metadata Publishing in ASMX Web Services .....	104
Enabling URLs In Saved Records .....	105
FIPS Compliant Mode .....	105

### Encryption of Data at Rest

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

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

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

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

## Encrypting Data

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

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

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

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

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

Related Area	Impact
Record Lookup Configuration	Only the filter options Equals, Does Not Equal, Field Value Match, and Field Value Does Not Match are available for encrypted fields.
Archer Mobile application	Encrypted fields are not supported.
Archer BCM mobile application	Encrypted fields are not supported.
Offline sync	You cannot sync an application with encrypted fields offline.
Subscription Notification filters	Only the filter options Equals, Does Not Equal, Field Value Match, and Field Value Does Not Match are available for encrypted fields.

## On this page

### Enable field encryption at the instance level

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

## Troubleshooting field encryption

The following table describes how to troubleshoot field encryption.

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

## Configuring the Hardware Security Module

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

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

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

2. On the General tab, go to the Hardware Security Module section.
  - a. Open the Archer Control Panel.
  - b. Go to Installation Settings.
  - c. Click the General tab.
3. In the Hardware Security Module section, select a module from the drop-down list.
4. In Module Token, enter the module value.
5. In Security Pin, enter the security pin value.
6. On the toolbar, click Save.

## File Repository Path

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

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

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

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

## Restrict Permissions on Repository Files

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

1. Log on to Windows servers.
2. Click Start > Administrative Tools > Services.  
For the Job Engine, the Log On As column identifies the account the service runs as.
3. Change each account as needed.

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

## Keyword Index Files

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

It is recommended that you do the following:

- Restrict the permissions on the keyword index files folder to read, write, and modify for the account that the Queuing service is running as.
- Define the location of the indexes folder in Archer to be a path set to off of any web server (avoid using a UNC path if possible to avoid performance impacts). The path can be a local path if the Archer installation includes a dedicated Services server.

## Company Files Path

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

It is recommended that you define the location of the company\_files folder in Archer to use a UNC path outside of any web servers, which eliminates the possibility of denial of service attacks and large file creation.

For configuration and permission details for the company\_files folder, see the *Archer Platform Installation and Upgrade Guide*.

## Disabling Metadata Publishing in ASMX Web Services

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

### Disable ASMX metadata publishing

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

1. In the web.config file, locate <system.web>.
2. In the child expression <webServices>, add the following:

```
<protocols>  
<remove name="Documentation"/>  
</protocols>
```



3. Click Save.
4. Perform an IIS reset.

## Enabling URLs In Saved Records

Users can directly access a URL within saved records in Archer if you activate the option for Links in Rich Text Fields. This option is inactive by default. You can activate this option for all Archer instances or for a single specific instance.

### Enable URLs in saved records for all instances

1. Go to the Security section on the Installation Settings tab for the Archer instance.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click the instance.
  - c. On the Installation Settings tab, go to the Security section.
2. In the Links in Rich Text Fields option, select Enable Links in Rich Text Fields.
3. On the toolbar, click Save.

### Enable URLs in saved records for an instance

1. Go to the Security section on the General tab for the Archer instance.
  - a. Open the Archer Control Panel.
  - b. From the Instance Management list, double-click the instance.
  - c. On the General tab, go to the Security section.
2. In the Links in Rich Text Fields option, select Enable Links in Rich Text Fields.
3. On the toolbar, click Save.

## FIPS Compliant Mode

The Federal Information Processing Standard (FIPS) is a United States and Canadian government standard that is intended to ensure secure data communications among compliant systems. FIPS 140-2 specifies the Security Requirements for Cryptographic Modules, including the approved encryption algorithms and hashing algorithms and the methods for generation and management of encryption keys. To qualify as FIPS compliant, Archer must be configured and operated in accordance with FIPS 140-2 requirements, using FIPS-certified components and algorithms in all required instances.

## Platform Release Supporting FIPS

Archer 6.0 and later can be configured for FIPS compliance.

### FIPS-Compliant Operation Requirements

You can configure FIPS compliance on any Windows system that supports Archer, including Windows Server 2016 and 2019.

**Note:** This requirement applies to all Archer components.

You must configure web browsers for FIPS operation. See [Configure Browser for FIPS Compliance](#).

### FIPS Certificates

Cryptographic modules that are FIPS 140-2 certified have undergone testing and verification by a government-approved evaluation laboratory. You can obtain the required FIPS certificates from the National Institute of Standards and Technology (NIST) website at:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

For a list of certificates applicable to Archer, see [Platform FIPS Certification](#).

### Set Up FIPS for Windows

Use the Local Security Policy tool to perform the FIPS setup for Microsoft Windows.

#### Procedure

1. Log on to Windows as a Windows system administrator.
2. Click Start > Control Panel.
3. In the Control Panel window, click Administrative Tools.
4. In the Administrative Tools window, click Local Security Policy.
5. In the Local Security Policy window, in the navigation pane, click Local Policies > Security Options.
6. In the Policy pane, double-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.
7. On the Local Security Setting tab, click Enabled.
8. Click Apply.
9. Click OK.
10. Close the Local Security Policy window.

## SQL Server FIPS Setup

All versions of SQL Server that support Archer are configurable for FIPS compliance. For instructions on setting up FIPS on SQL Server, see the Microsoft SQL Server documentation.

**Note:** SQL Server 2017, SQL Server 2017 on Linux (Ubuntu), or SQL Server 2019 must be installed on a Windows Server 2016 or 2019-based server. The Windows server must be FIPS enabled prior to starting SQL Server.

For dialog security between services, the encryption uses the FIPS-certified instance of AES if the FIPS mode is enabled. If the FIPS mode is disabled, the encryption uses RC4. When a Service Broker endpoint in the FIPS mode is configured, the administrator must specify AES for the Service Broker. If the endpoint is configured to RC4, the SQL Server generates an error, and the transport layer does not start.

Messages in two logs verify that the SQL Server is running in FIPS mode:

- When the SQL Server service detects that FIPS mode is enabled at startup, it logs this message in the SQL Server error log:  
Service Broker transport is running in FIPS compliance mode.
- This message is logged in the Windows Event log:  
Database Mirroring transport is running in FIPS compliance mode.

### Configure Browser for FIPS Compliance

In addition to FIPS enablement on the host system, you must configure any web browser used to connect to the Archer for FIPS compliance. For more information, see [Set up FIPS for Windows](#)

When using supported versions of Microsoft Internet Explorer with the Platform in FIPS mode, enable TLS 1.2 or higher in the browser. For more information, see the Archer [Qualified and Supported Environments Guide](#).

1. Open Internet Explorer.
2. Click Tools, and then click Internet Options.
3. On the Advanced tools tab:
  - a. Verify that both Use TLS 1.0 and Use TLS 1.1 options are cleared.
  - b. Select Use TLS 1.2.
4. Verify that both Use SSL 2.0 and Use SSL 3.0 options are cleared.

## LDAP Configuration for FIPS Mode

**Note:** Archer assumes that you use Microsoft Active Directory as the LDAP server. For other types of LDAP servers, see their product-specific documentation.

Connections to Active Directory from Archer can be unencrypted or encrypted. If you intend to encrypt connections, you must configure Active Directory with a server certificate. You can achieve this with a server certificate on the Windows server, which installs the server certificate, using auto enrollment on Active Directory.

To configure Active Directory in FIPS mode, the Windows server hosting Active Directory must be FIPS enabled. For more information, see [Set Up FIPS for Windows](#).

## Platform FIPS Certification

The following tables list the FIPS certificates for the cryptographic components that Archer uses.

### Secure Hash Algorithm (SHA) Standard (FIPS 180-4)

Algorithm	Operating System	Certificate Number
SHS	Windows Server 2016	#3347
	Windows Server 2019	#C211

### Advanced Encryption Standard (AES) Algorithm (FIPS 197)

Algorithm	Operating System	Certificate Number
AES	Windows Server 2016	#4064
	Windows Server 2019	#C211

### Enable FIPS Window Server Configuration for 140-2 on the Web and Services Server

1. Enable FIPS mode on the web server.
  - a. Go to Administrative Tools.
  - b. In Administrative Tools, select Local Security Policy.
  - c. Expand Local Policies, and select Security Options.
  - d. Double-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.
  - e. Select Enable.
2. Download and install the JCE Unlimited Jurisdiction Policy files.
  - a. Go to <http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html> and follow the steps provided to download the JCE Unlimited Jurisdiction Policy files.

- b. Extract and open the ZIP file.
  - c. Edit the jar file names by adding the extension .org to the end of the files so that they are not overwritten later.
  - d. Paste the renamed files in %SystemDrive%\Program Files\Java\<java\_version\_directory>\lib\security.
3. In the %SystemDrive%\Program Files\Java\java\_version\_directory\lib\security directory, edit the java.security file by doing one of the following:
  - Add the line com.rsa.cryptoj.fips140initialmode=FIPS140\_MODE..
  - Change the line com.rsa.cryptoj.fips140initialmode=NON\_FIPS140\_MODE to com.rsa.cryptoj.fips140initialmode=FIPS140\_MODE.

## Chapter 6: Cryptography

---

SSL Certificate Guidance .....	110
SSL Certificate Validation - Redis .....	111

### SSL Certificate Guidance

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

It is recommended that you use a hardware security module (HSM) for field encryption over a certificate in a local store.

### Field Encryption certificate requirements

Certificates must meet the following requirements:

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

## How to secure a Field Encryption certificate

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

- Give Full Control and Read access to the certificate only to the Administrator account. All other accounts should have only Read access.
- Give the certificate read-only access to the following accounts:
  - In a server hosting the archer web application, only the AppPool account used by the web application should be given access (Read-Only) to the certificate.
  - In a server hosting archer services, for example, Configuration Service and Job Framework, only accounts used by the services should be given access (Read-Only) to the certificate.
- Revoke access for all accounts that are not required.
- Back up the encryption certificate regularly. The backup should be password protected and stored safely.

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

For information about industry best practices, see the following:

- [NIST SP 800-52](#)
- [PCI-DSS v3.2.1 - May 2018](#)

## SSL Certificate Validation - Redis

Redis does not have built-in support for SSL. It is recommended that you use tunneling software, such as stunnel, to enable SSL for your Redis Server. Stunnel configuration involves specifying the port for accepting secure connection and the certificate to be used as the server certificate.

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

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

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

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

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



## Chapter 7: Auditing and Logging

---

Log Description .....	113
Security Events Report .....	113
Archer Error Logs .....	115
Log Directory Permissions .....	115
Windows Event Logs .....	115

### Log Description

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

Component	Location
Security Events Report	The instance database
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 Archer. It is recommended that administrators define and enforce a retention policy for the 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

## Archer Error Logs

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

It is recommended 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 Archer Control Panel Help.

## Log Directory Permissions

It is recommended 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 Archer-installed services are running.

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

## Windows Event Logs

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

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

## Chapter 8: Physical Security

---

Physical Security Controls Recommendations .....	116
--	-----

### Physical Security Controls Recommendations

Physical security controls are designed to protect resources against unauthorized physical access and physical tampering. It is recommended that the physical servers for Archer be deployed in a secure data center leveraging the organization's best practices for physically securing a data center, server rack, and server.

## Chapter 9: Serviceability

---

Security Patch Management .....	117
Malware Detection .....	117
Virus Scanning .....	118
Ongoing Monitoring and Auditing .....	118
Securing Credentials .....	118

### Security Patch Management

Security patches are released on an as-needed basis.

All security patches for Archer originate as RSA and are available for download as an update, as long as you have a current maintenance agreement in place with RSA. Updates are available on Archer Community. Register your product and sign up to access the Archer Community.

Run the latest security patches for any software that you are using with Archer and ensure you are using the latest software as defined in the [Qualified and Supported Environments Guide](#).

Here is a list of third-party components for which patches are needed. The frequency of the patch updates is determined by the vendor. It is the customer's responsibility to ensure that third-party components are patched as appropriate, using the instructions provided by the vendor.

- Windows Server 2016 & 2019
- SQL Server 2017, 2017 on Linux (Ubuntu), & 2019
- Microsoft IIS
- .NET Framework

### Malware Detection

Deploy a malware detection solution on the web and database servers. The malware detection solution should be based on your standard tools and best practices. It is your responsibility to deploy patches and updates for the malware detection tools.

## **Virus Scanning**

Run virus scanning software on the deployed servers on a routine basis. If you are running Threat or Vulnerability feeds, it is strongly recommended that you disable virus scanning for the folder in which the Threat or Vulnerability data files are temporarily stored. A virus scanning engine could interpret the data as a virus or malware.

For information on configuring the folder, see Threat Data Feeds.

## **Ongoing Monitoring and Auditing**

As with any critical infrastructure component, constantly monitor your system and perform periodic and random audits, for example, configuration, permissions, and security logs. Ensure that the configurations and user access settings match your company policies and needs.

## **Securing Credentials**

The credential hashing algorithm selection uses the PBKDF2 algorithm with a randomly generated salt size.

## Chapter 10: Additional Security Considerations


---

- [Creating Global iViews](#)
- [Managing iViews](#)
- [Formatting iView Videos](#)
- [Adding Objects to the Layout](#)
- [Offline Access](#)
- [Installing Offline Access](#)
- [Elasticsearch Security Considerations](#)
- [JavaScript Transporter Security Considerations](#)
- [Archer IRM Mobile App Security Considerations](#)

### Creating iViews

iViews are containers for information that you want to present to your users in a dashboard. iViews most commonly display reports, but they can also display links, videos, embedded web pages, and more. For details on the different iView types, see [Workspaces, Dashboards, and iViews](#) in the Archer Online Documentation.

#### Task 1: Create the iView

1. Do any of the following:
  - From the menu bar, click  > Workspaces and Dashboards > Global iViews, and click Add New.
  - From Manage Dashboards > *DashboardName*, click the Layout tab, and click Select iViews.
  - From a dashboard, click ... > Add iView Content.
2. Select your iView type, and click OK.
3. In the General Information section, enter a name and description.
4. In the Folder field, select or create a folder.


Folders allow you to group iViews to make it easier for you to select related iViews when you build a dashboard.
5. (Optional) Attach supporting documentation about the configuration of your iView.

## Task 2: Configure the options for your iView type

In the Options section, configure your iView.

### Configure a canvas iView

Canvas iViews are often used for welcome messages or to share information about the dashboard.

1. In the Canvas Style field, click , select the layout that you want, and click OK.
2. In the Title field, enter the title that you want to appear in the iView.
3. In the Content field, enter the content that you want to appear in the iView.

### Configure a custom iView

Custom iViews allow you to build layouts with HTML, embed Flash presentations, execute custom scripts, such as JavaScript.

**Important:** It is recommended that only trusted administrators have permission to create and edit custom iViews.

1. In the Custom Content field, enter the content.
2. Select a refresh rate.

### Configure an embedded URL

The Embedded URL iView displays a web page within the context of a dashboard. This iView acts as a mini browser that can be displayed within the Archer Platform. You are only allowed to display one web page per iView. If you want to display multiple web sites on a dashboard, you will need to use multiple Embedded URL iViews.

1. In the URL field, enter the URL you want to embed.
2. Select a refresh rate.

### Configure a global search iView

The global search iView allows users to run a keyword search against the applications you select. The system only returns records that the user has access to.

1. In the Column Display field, select one or two columns.
2. (Optional) If you want to embed the iView description (from the General Information section) in the iView itself, select the checkbox.



3. (Optional) If you want to use a different search button, click Add to select another image or upload your own.
4. In the Applications section, click Add New to select the applications that you want your users to be able to search. For each application, select the visibility and default behavior.

Applications			Add New
Application Name	Visibility	Default Behavior	Action
Applications	Visible	Disabled	
Business Unit	Hidden	Enabled	
Contacts	Visible	Enabled	

The Visibility setting determines whether a checkbox displays under the search field for that application. The Default Behavior settings determines whether that checkbox is selected by default.

For example, in the image, Applications and Contacts are both set to visible, but only Contacts is set to enabled. Business Unit is set to hidden and enabled, so it will be included in the search, even though it is not displayed here.

Search

GO

Applications  
 Contacts

**Tip:** If the Visibility is set to Hidden, do not set the Default Behavior to Disabled, otherwise users will not be able to search that application.

#### Configure a landing page iView

1. In the Background field, select your background image.
2. In the Title field, enter the title that you want to appear in the iView.
3. In the Configuration section, add links to internal pages and external URLs.
  - a. Click Add New.
  - b. Enter a name and description, and select an action for your link.
  - c. Select your internal page or enter the URL of your external link.
  - d. Click OK.
  - e. Repeat steps a - d, to add up to eight links to the iView.
 

**Note:** If you select more than four links, the iView will automatically use two columns.
  - f. (Optional) To configure the display order, click Display Order.

### Configure a links list iView



Links list iViews allow you to create links to web sites, intranet sites, and frequently used Archer pages.

1. In the Layout field, select Simple List or Descriptive Links.
  - Note:** If you selected Descriptive Links, enter a name and description.
2. In the Column Display field, select One Column or Two Columns.
3. In the Configuration section, add links to internal pages and external URLs.
  - a. Click Add New.
  - b. Enter a name and description, and select an action for your link.
  - c. Select your internal page or enter the URL of your external link.
  - d. Click OK.
  - e. Repeat steps a - d, to add up to eight links to the iView.
    - Note:** If you select more than four links, the iView will automatically use two columns.
  - f. (Optional) To configure the display order, click Display Order.

### Configure a report iView

Report iViews allow you to display global reports, including charts generated from a statistics search. Reports are reloaded every time that the iView is accessed to provide real-time data.

If your instance has caching enabled, you can enable iView report caching to optimize performance. Instead of generating search results every time a user opens a workspace or dashboard containing Report iViews, stored search results are displayed when they are opened within the cache duration. Users can manually update search results for a Report iView at any time with the Refresh option.

1. Select the report or reports that you want displayed in the iView.
2. To change the display order of the reports in the iView, click the report title and use   to arrange the reports in the preferred order.
  - Note:** The first report listed is the report that is initially displayed to the user.
3. Select the checkbox for each report that you want to allow horizontal scrolling.

### Configure an RSS feed iView

RSS iViews allow you to display data from an RSS feed, such as headlines and summary information.

1. Enter the URL and select an authentication type. If required, enter the username and password.
2. In the Feed Elements field, select which elements from the feed you want to display in the iView.
3. Select the number of articles that you want to display and for how many days you want them to display.
4. Select how often you want the feed to refresh.

### Configure a video iView

In the Embedded Video HTML field, enter the embedded HTML or the URL.

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

For example:

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

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

For example:

```
<video width="320" height="240" controls>
<source src="/ACME_Company/video.mp4" type="video/mp4">
</video>
```

### Task 3: Determine who can access the iView

1. Go to the Access tab.
2. Select whether you want the iView to be public or private. If you select private, select the users, groups, roles, or solutions that you want to give access to.


**Note:** Assigning rights to the iView does not assign a user the rights to see the content in the iView. For example, if you make a Report iView public, all users would potentially be able to see the iView (provided they also have access to the workspace and dashboard). However, to view the contents of the iView, they would also need rights to the report itself.

3. Click Save.




## Managing iViews

The Manage iViews page is your starting point for all iViews tasks. You can view existing, [create new](#), copy and delete existing iViews, and create folders for global iViews.

### Create a folder for a Global iView

1. From the menu bar, click  > Workspaces and Dashboards > Global iViews, and select a global iView.
2. In the General Information Section, in the Folder field, click Edit.
3. In the Manage Folders window, click Add New.
4. Enter the name of the folder, and click OK.
5. In the Folder list, ensure that the correct folder is selected, and click OK.



### Update an iView display

1. In the iView title bar, click  and select Edit Properties.
2. In the Options section, edit the iView display as needed, and click OK.  
**Note:** The list of available menu options depends on the type of iView that you are viewing and the access rights assigned to you by your administrator.
3. (Optional) To resize the iView, click and drag the bottom-right corner of the iView, and click .
4. (Optional) To move the iView, click and drag the title bar of the iView to the new location, and click .

### Delete a global iView

You must have Delete rights to the Workspaces and Dashboards: Manage Global iViews page to complete this task.

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

1. From the menu bar, click  > Workspaces and Dashboards, and click Global iViews.
2. In the Actions column of the iView you want to delete, click .
3. Click OK.

## Formatting iView Videos

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

### Embedding From an External Source

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

**Sample YouTube source embed code:**

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

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

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

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

### Embedding From an Internal Source

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

**Sample internal source embed code:**

```
<video width="320" height="240" controls>  
<source src="/ACME_Company/video.mp4" type="video/mp4">  
</video>
```

## Adding Objects to the Layout

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


### On this page

## Key guidelines for adding objects to the layout

- To move a single object, click the object and drag it to the location you want.
- If you are working in a multi-tab layout and you want to move an object from one tab to another, click and drag the object to the tab you want.
- If you are working in a two-column layout and want a custom object, placeholder, text box, or trending chart to span across columns, do the following:
  1. Click the drop down arrow on the layout object.
  2. Select Edit Span Properties and select column and row span options.

## Add sections


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

1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Section option to the layout area.
3. In the Section Name field, enter the heading that you want to display in the layout.
4. In the Default Visibility field, select whether you want the section to be expanded or collapsed by default.
5. (Optional) Do one or both of the following to add panel text or help text to the section:
  - To add an information panel to provide your users with additional details about the section, select Panel Text and enter the text that you want to display.
  - To add Help text to provide your users with detailed instructions and background information about the section, select Help Text and enter the text that you want to display.
6. (Optional) Customize your text and add dynamic elements, such as images and Flash animation, using the options available in the Rich Text Editor toolbar.
7. Click OK to close the Section Description dialog box.
8. Click  to save your changes.

## Add text boxes


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

1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Text Box option to the layout area.
3. In the Text Box Name field, enter a name for the text box.

4. In the Text field, enter the text that you want to display in the text box when it is displayed for users.
5. Select whether you want the text box to display when users view the record, edit the record, or both.
6. Click OK.
7. Click  to save your changes.

## Add placeholders

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


1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Placeholder option to the layout area.
3. Click  to save your changes.

## Add custom objects

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


**Note:** It is recommended that only trusted administrators create and edit custom layout objects, as this flexibility introduces a potential attack vector.

1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Custom Object option to the layout area.
3. Enter a name and description for the custom object.

**Note:** The name is not displayed for users when they add, edit, or view records in the application.
4. In the Code field, enter or paste the HTML or JavaScript code for the object.
5. Select whether you want the custom object to display when users view the record, edit the record, or both.
6. Click OK.
7. Click  to save your changes.

## Add trending charts

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


1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Trending Chart option to the layout area.
3. In the Name field, enter the heading that you want to display in the layout.
4. From the Trending Field list, select the trending-enabled field for which to display chart data.
5. (Optional) In the Show Title field, click the Display the chart name as the title when users open the application or questionnaire.
6. Click OK.
7. Click  to save your changes.

## Add report objects

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

1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Report Object option to the layout area.
3. Enter a name and description for the report object.  
**Note:** The name does not display for users when they add, edit, or view records in the application.
4. Under Report Selection, select the report from the Available Reports column.  
**Note:** Only global and search based reports are available for selection, and you can only select only report.
5. (Optional) Add or update filter options for how you want to view the report.  
**Note:** If the selected report has default filters, they are automatically populated as existing filters.
  - a. In the Field to Evaluate field, select the field to evaluate for one or more specific values.
  - b. In the Operator column, select the filter operator. For more information, see "Report Operator Field Types" in the Archer Online Documentation.



- c. In the Value(s) column, select the values for the condition. Depending on the operator type, the selection can be a value or a field.
  - d. (Optional) To create additional conditions, click Add New and repeat steps a-c.
  - e. (Optional) If you create more than one condition, apply logic to your filter criteria in the Advanced Operator Logic section. For more information, see "Advanced Operator Logic" in the Archer Online Documentation.
6. In the Load Report section, select whether you want the report object to be display as soon as the page loads or when a user clicks the report object.
  7. In the Display section, select whether you want the report object to display when users view the record, edit the record, or both.
  8. Click OK.
  9. Click  to save your changes.


## Adding tab sets

Tab sets provide a means for grouping related tabs and fields, to help users quickly find the fields they need to add or edit in a record.


**Note:** If a user does not have access to any of the fields on a tab, the tab is not displayed when the user adds or edits records. Using data driven events, tabs can be dynamically shown or hidden based on the current state of content, including nested tabs. When a data driven event hides all sections on a tab, the tab is also hidden.

**Important:** If you want to add a new section to the layout and give it the same name as a new tab set, you must add the section before you add the tab set.


### Add a new tab set

1. In the left pane, expand the Layout Objects list.
2. Click and drag the Add Tab Set option to the layout area.
3. In the Tab Set Name field, enter a name for the tab set.
4. From the Height list, select one of the following options:
  - To use default height settings for the tabs in the tab set, select All from the Height list, and click OK.
  - To select the height in pixels for the tabs in the tab set, select the value, and click OK.
5. Click  to save your changes.

### Add tabs to a tab set

1. Click the New tab in the tab set that you added.
2. In the Tab Name field, enter a name for the tab
3. (Optional) In Default Tab field, click Display this tab by default when users first access the page to display a tab by default when users open the application, questionnaire, or sub-form.
4. Click OK.
5. Click  to save your changes.

### Add fields to a tab set

1. Add a section to the tab.
2. Drag and drop the fields onto the Layout page to add fields.
3. Arrange the fields until they display in the correct order.
4. Click  to save your changes.

## Offline Access

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

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

It is recommended that only trusted users with secure laptops with strict firewall rules restricting remote access to Offline Access have permission to Offline Access.

## Archer features not supported for offline access

The following are features not supported for offline access:

- Application Builder
- Data Feeds
- Data Publications
- Data Imports

- Discussion Forums
- LDAP Synchronization
- Notifications
- Packaging
- User Preferences

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

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

## Installing Offline Access

The installation process for Offline Access is separate from the Archer installation. It is recommended to install 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

Review the required versions of the following components before installing offline access. For the supported and qualified software and environments, see [Archer Qualified and Supported Environments](https://community.rsa.com/t5/archer-platform-documentation/rsa-archer-qualified-and-supported-environments/ta-p/568750) on the Archer Community. (<https://community.rsa.com/t5/archer-platform-documentation/rsa-archer-qualified-and-supported-environments/ta-p/568750>)

- Microsoft Windows Operating System
- Memory
- Disk Space
- Additional Software
- Microsoft Sync Framework: must be installed on the Services Server. For more information, see "Preparing the Services Servers" in the *Archer Installation and Upgrade Guide*.

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

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

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

## Install Offline Access

The offline access version must always match the 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 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

File or Process	Default Location
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

## Elasticsearch Security Considerations

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

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

It is recommended that you take the following additional security considerations into account when using Elasticsearch:

- Elasticsearch should be configured for unicast network discovery. This prevents a new node from joining the cluster unless explicitly specified.
- In the event of index deletion or corruption, the Elasticsearch Index can be rebuilt. For more information, see "Rebuilding Search Indexes" in the Archer Control Panel Help.
- When using Elasticsearch, data is stored in Archer and the Elasticsearch cluster node. It is recommended that you follow the best security practices for data in both locations as outlined in [Encryption of Data at Rest](#).
- If visualization tools are used with Elasticsearch, users should ensure the tools are securely deployed following guidance from the tool provider to protect Archer data.
- Encrypted field types in Archer will also be stored as encrypted fields in the data store for Elasticsearch in the Archer database. For more information, see [Encrypting Data](#).

## JavaScript Transporter Security Considerations

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

- Communicate with external systems using APIs protected by SSL/TLS protocol.
- Communicate with external systems using APIs that involve a strong authentication mechanism.
- Mark sensitive parameters as "Protected" in the Custom Parameters section of the Transport tab in the JavaScript Transporter Settings in the Archer Control Panel.
- If you create a JavaScript file, it is recommended to sign the file and enter the digital thumbprint of the trusted certificate in the JavaScript Transporter Settings in the Archer Control Panel. For more information, see "Obtaining Digital Thumbprints" and "Configuring JavaScript Transporter Settings" in the Archer Control Panel Help.

## Archer IRM Mobile App Security Considerations

The following measures have been put in place to ensure a secure connection between Archer and the Archer IRM Mobile app:

- The app is only available on https protocol.
- The app is only compatible with CA certificates. Self-signed certificates are not supported. The configured login type rejects requests if it is not communicating using valid public certificates.