

Retain 4.10.1

How Retain Works

March 2022

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Copyright © 2017–2021 Micro Focus or one of its affiliates.

Contents

Preface	5
About Retain	5
About This Guide	5
For Documentation Feedback	5
To Join the Retain Idea Exchange	5
For Additional Documentation	5
To Contact Technical Support	5
For Sales	5
For Professional Services	5
 1 Key Concepts	 7
What Retain Does	7
How Retain works	7
Retain Components and Their Roles	8
Modules Overview	9
Key Concepts	9
Modules	10
Profiles	12
How Retain Stores the Archives	12
Retain's Archive Data Organization	12
 2 Retain Functional Overview	 15
Importing and Archiving Data	15
Live Data	15
Offline Data	16
Metadata Vs. Message Data	16
Exporting Data from Retain	16
Using the Web Interface	16
Using the Outlook Plugin to Export Messages	16
Dealing with Large Quantities of Data	16
Removing Data from Retain	16
 3 Target Systems and Data Streams	 17
Smart Phone Targets	17
Email System Targets	17
Search Engine Targets	17
 4 Jobs	 19
How Archive Jobs Work	19
An Archive Job Example	20
 5 Retain Users and Groups	 21
Populating Retain's Archive Address Book	21
Retain Users and User Accounts	21
Retain Handles Users with the Same Name	23

Archive Address Book Users Are Protected from Removal	23
Retain's LDAP Service	23
General Account Control.	24
 6 Authentication, Standard and Multi-factored	 25
Authentication in Retain	25
Authentication Part 1: Username/Password or OpenID Connect	25
Authentication Part 2 (Multi-factor Authentication)	27
All Retain Users Can Be Enabled for MFA Authentication	29
Duplicate LDAP User Entries Are Not Allowed	29
MFA Can Work When Back-end Messaging Systems Are Offline	29
When Google and Office 365 Systems Require an App Password	30
Authentication is persistent	31
 7 Retention Services and Item Store Flags	 33
How Retain Works with GroupWise Retention Services	33
How Retain Works with Exchange and Office 365	34
Placing a Hold Prevents Loss of Unarchived Messages	34
Journaling Mailbox, an Alternative to the Item Store Flag but Not Recommended	34
How Retain Works with Gmail.	35
 8 Retain Unified Archiving Version Numbering	 37

Preface

About Retain

Retain Unified Archiving

- ♦ Archives email and text messages.
- ♦ Catalogs them for search and retrieval.

Retain is not a backup/restore system.

About This Guide

This guide presents a conceptual understanding of Retain Unified Archiving version 4.10.1.

For Documentation Feedback

Scroll to the bottom of the online page and enter a User Comment.

To Join the Retain Idea Exchange

Got an idea for a new Retain feature or enhancement? [Log in to Microfocus.com](#) and join the conversations happening inside the [Retain Idea Exchange](#).

For Additional Documentation

See the [Micro Focus Knowledge Base](#) website.

To Contact Technical Support

Browse to [the Micro Focus Support Page \(https://www.microfocus.com/support-and-services/\)](https://www.microfocus.com/support-and-services/) and begin typing *Retain Unified Archiving* in the **Search for a Product** field.

For Sales

Go to the [Micro Focus Contact page \(https://www.microfocus.com/en-us/contact\)](https://www.microfocus.com/en-us/contact).

For Professional Services

Contact Micro Focus Professional Services by sending an email to sales@microfocus.com or calling (877) 772-4450.

1 Key Concepts

- ♦ [“What Retain Does” on page 7](#)
- ♦ [“How Retain works” on page 7](#)
- ♦ [“Retain Components and Their Roles” on page 8](#)
- ♦ [“Modules Overview” on page 9](#)
- ♦ [“Profiles” on page 12](#)
- ♦ [“How Retain Stores the Archives” on page 12](#)
- ♦ [“Retain’s Archive Data Organization” on page 12](#)

What Retain Does

Retain

- ♦ Provides organizations with legal compliance and litigation protection.
- ♦ Frees up disk space on messaging systems.
- ♦ Enhances message-data management.
- ♦ Archives and stores messages and data from
 - ♦ Messaging systems
 - ♦ Phones
- ♦ Lets administrators
 - ♦ Perform advanced searches on archived messages
 - ♦ Review archive status and activity
 - ♦ Retrieve archived messages and data
 - ♦ Generate reports on archived messages and data
- ♦ Optionally, users can access and search their archived personal data.

IMPORTANT: Retain is NOT a backup or emergency-restoration system.

You must ensure that your messaging systems are backed up by other software and systems designed for that purpose, as required by organizational and governmental regulations.

How Retain works

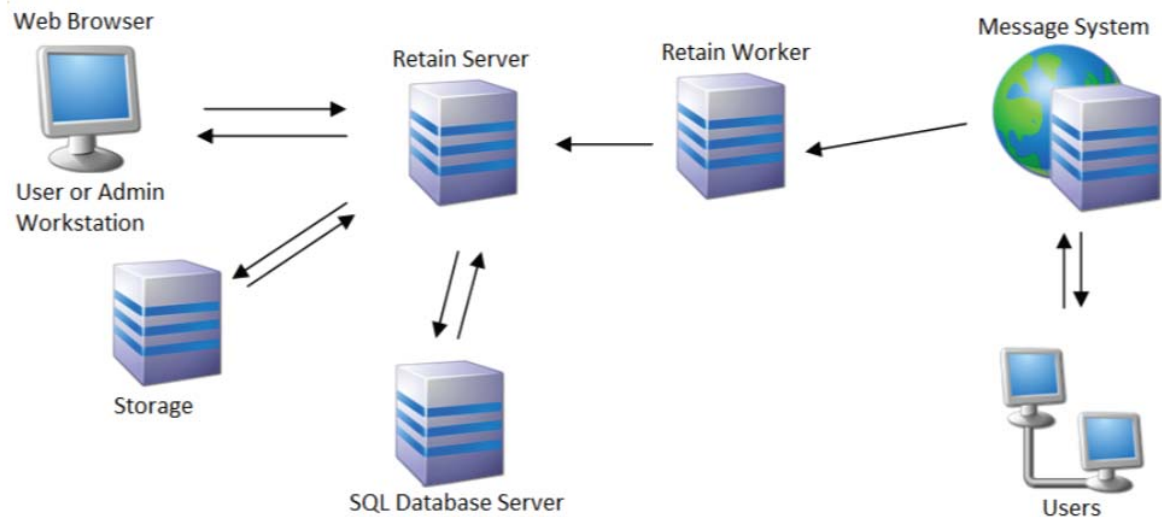
Briefly, Retain

1. Connects to targeted message systems.
2. Collects data by using each message system’s defined APIs (for example, SOAP for GroupWise and Exchange).
3. Archives the collected data.

4. Indexes the archives in an SQL database.
5. Provides search-access to users with sufficient access rights, as managed by Retain administrators.

Retain Components and Their Roles

Retain consists of several main parts which can be installed on the same server or on different servers, depending on the size and complexity of your messaging infrastructure.



- ♦ **Retain Server:** One per system.
 - ♦ Controls all Retain functions.
 - ♦ Houses the archive.
 - ♦ Manages Retain Workers
 - ♦ Stores index-targeted data in the database.
- ♦ **Retain Workers:** One or more per system; often one per messaging server.
 - ♦ Can be installed with Retain, on the targeted mail server, or on a standalone server.
 - ♦ Collects data and transfers it to the Retain server.
- ♦ **SQL Database:** One database per system.
 - ♦ Can be installed with Retain, as a single-server, or clustered.
 - ♦ Stores message header data, user data, and links to archived messages.

IMPORTANT: The Retain software doesn't include a database. You must install and maintain one of the supported SQL databases.

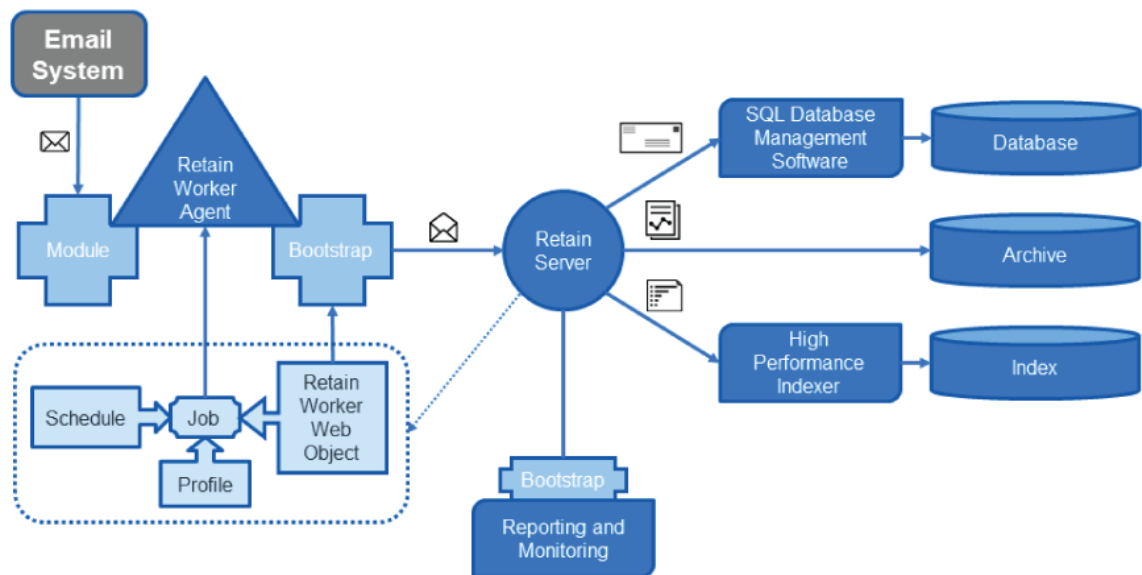
- ♦ **Reporting and Monitoring Server:** One per system.
 - ♦ Can be installed with Retain or on a standalone server.
 - ♦ Keeps job and server statistics.
 - ♦ Monitors mailbox errors.

- ♦ **Indexing Engine:** Installed on the Retain server (standard indexer), or separately in a High-Availability Indexer cluster.
 - ♦ Indexes all the data.
- ♦ **Stubbing Server:** Installed on the Retain server.

Only for GroupWise 8.0.1 and later

 1. Removes large messages from GroupWise storage.
 2. Archives the messages.
 3. Creates a database `stub` (link to the message in the archive).

Message-access experience is unchanged for GroupWise users.
- ♦ **Retain Router:** Installed in the network DMZ.
 - ♦ Gathers phone message data using REST, from registered Android or Blackberry devices.
 - ♦ Stores the data until it can forward it to the Retain Server for archiving as with other systems.



Modules Overview

The Module is how Retain connects to your messaging system.

Select the module that corresponds with your messaging system and configure the module.

Key Concepts

You must install a Module to connect to your messaging system, this reveals the Data Collection section in the console for setting up a job.

Archiving involves connecting Retain to your messaging system with a Module, setting up a schedule for when you want archives to happen, a profile that defines what should be archived, a worker agent needs to be installed, configured and connected to Retain, and finally a Job needs to be configured with all the previous components as well as who to archive.

To set up archiving, you need to configure:

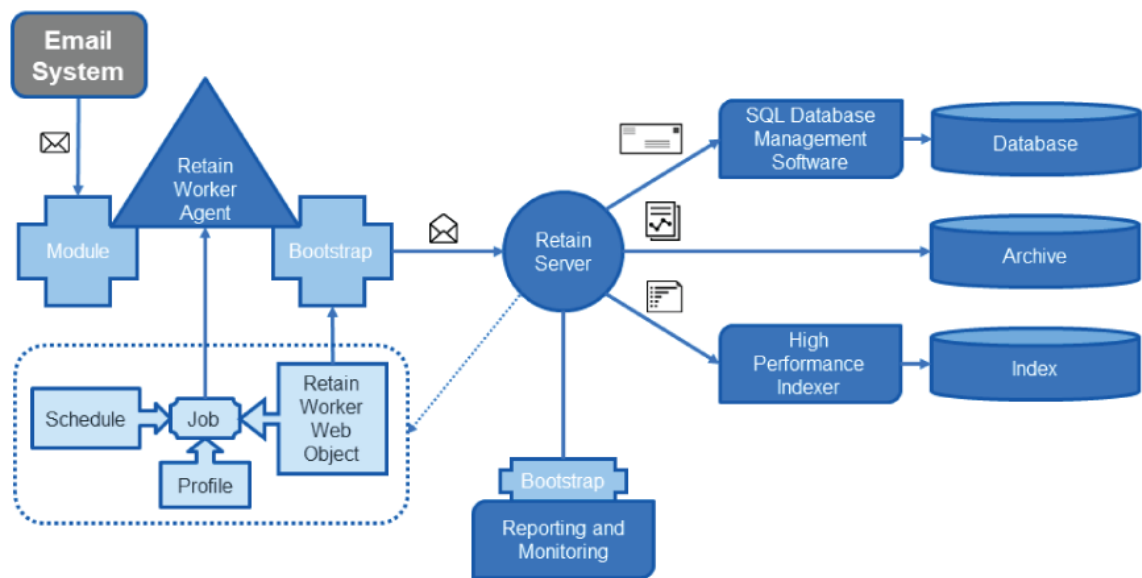
Module: How to connect your messaging system.

Schedule: When the job runs.

Profile: What types of messages the job is to archive.

Worker: The Worker is a combination of the Retain Worker Agent that can sit on the Retain server, the messaging server or another server, and the Retain Worker Web Object in the Retain Server console where you create the worker bootstrap which tells the Worker Agent how to connect to Retain Server.

Job: Who to archive, what expiration date to create, what schedule, profile, and worker to use.



Modules

Modules are how Retain connects to a messaging system and jobs specify what Retain archives.





Modules are where you provide the data needed for Retain to connect to the messaging system. This includes the address of the messaging system server and credentials to enter the system, such that Retain can access all the mailboxes.

This is used by the Retain Worker to connect to the messaging system. It is the Retain Worker that does all the work of bringing the data into Retain.

Since the Worker Agent software can be installed on a server separate from the Retain server itself we need to provide it with a bootstrap so it knows how to connect to the Retain server.

In Retain 4.2 and above, multiple modules of the same type can be enabled. This allows Retain to connect to multiple messaging systems of the same type at the same time that do not share common access. The modules can be given different names to make it easy to distinguish.

Multiple modules is enabled for GroupWise, Exchange, Google Apps (G Suite) and Mobile modules. It does not apply to the other modules.






Module Configuration




After configuring a module, it is recommended you manually refresh the Address Book.

Refresh Address Book
Sync job is not running at this time.




Mailbox Mapping Options

Configured Modules

GroupWise4.214	GroupWise4.160	Exchange4.213	GBS Notes
			
Configure	Configure	Configure	Configure
Install 16-Nov-2016 Date 10:09:26 Last Address 23-Mar-2017 Book 01:02:10 Cache Status Configured.	Install 22-Mar-2017 Date 15:19:47 Last Address 23-Mar-2017 Book 01:02:13 Cache Status Configured.	Install 16-Nov-2016 Date 10:09:25 Last Address 23-Mar-2017 Book 01:02:14 Cache Status Configured.	Install 08-Dec-2016 Date 10:22:24 Status Configured.

You enter the Module name in the Module.

For example, the GroupWise4.214 module has a different domain and trusted application key compared to the GroupWise4.160 module.


GroupWise Module



GroupWise specific information is configured here. At a minimum, the CORE SETTINGS and SOAP tabs must filled out completely.

Core Settings
SOAP
LDAP
Proxy

Core Settings

Normally all of these entries should be enabled.

- Enable Address Book Caching determines if this module caches address book entries from its directory services during Maintenance.
- Enable Authentication indicates if users logging into Retain should be able to use the module's authentication system.
- If Enable Jobs is not enabled, no jobs pertaining to this module will be sent to Workers.

Module name	GroupWise4.214
Enable Address Book Caching	<input checked="" type="checkbox"/>
Enable Authentication	<input checked="" type="checkbox"/>
Enable Jobs	<input checked="" type="checkbox"/>

Set Storage Flags

If you are using either the Purge or Retention features in GroupWise, you probably want these to be advanced automatically as items are stored so users may delete messages in their mailbox that have been stored by Retain.

☒ Retention Flag ☐ Purge Flag

Normally this entry should be disabled.

- Send GroupWise items to an external system.

Select Send Method
disabled

Profiles

Once you have configured a module you can configure a Profile for the module type.

Profiles describe what to archive.

Not all modules have profiles.

How Retain Stores the Archives

Retain uses a hybrid data-storage approach.

- ♦ **SQL Database:** Stores meta data, folder structures, attachment information, and links to messages in the archive file.
- ♦ **Archive File System:** Stores message text and attachments in a single-instance storage scheme that is designed to protect against tampering.

Retain's Archive Data Organization

Retain organizes data streams in the archive by

- ♦ The user who created or used them

- ♦ The time they were created.
- ♦ The data source.

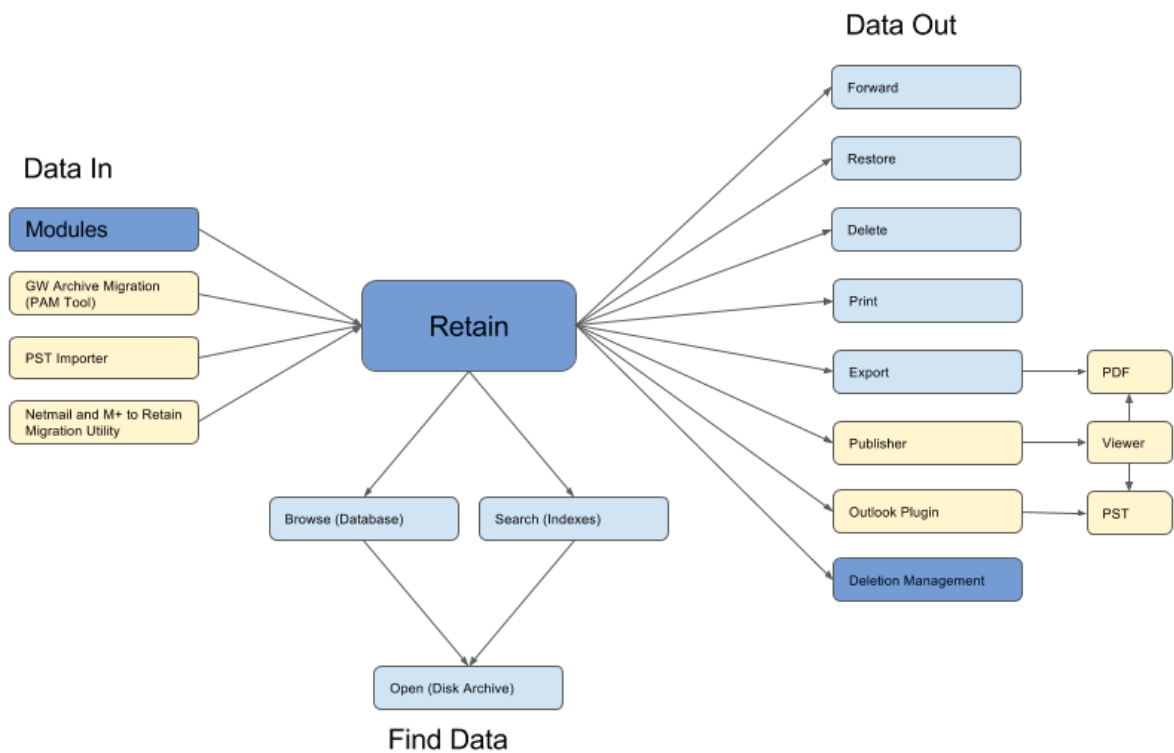
Retain then indexes items for searching, exporting, and publishing from the archive.

2 Retain Functional Overview

- ♦ “Importing and Archiving Data” on page 15
- ♦ “Metadata Vs. Message Data” on page 16
- ♦ “Exporting Data from Retain” on page 16
- ♦ “Removing Data from Retain” on page 16

Retain provides three functions:

- ♦ Importing and archiving data
- ♦ Finding specific data in the archives
- ♦ Exporting data from the archives



Importing and Archiving Data

- ♦ “Live Data” on page 15
- ♦ “Offline Data” on page 16

Live Data

Modules dredge data from live messaging systems.

Offline Data

Workstation tools migrate off-line data into Retain. In the top-right corner of the Retain web console, click the Tools drop-down.

Offline data migration tools include

- ♦ The GroupWise Archive Migration Tool
- ♦ The PST Importer
- ♦ The Netmail and M+ to Retain Migration Utility.

Metadata Vs. Message Data

Metadata is used for listing the content of mailboxes and delivering search results.

When you search in Retain, you are leveraging the indexes and metadata that Retain uses to find things quickly.

When you open a specific message, you are viewing the message data from the archive.

Exporting Data from Retain

Using the Web Interface

Using the web interface, click the checkbox for each message you want to export, then in the list of actions, click the action you want to take.

By default, users can view and save attachments, as well as forward and print messages.

Using the Outlook Plugin to Export Messages

The Outlook plugin lets users search and download messages from Outlook.

Dealing with Large Quantities of Data

For large quantities of data, use the workstation tool found under the Tools menu. See “[Retain Publisher and Viewer](#)” in *Retain 4.10.1: User Guide*.

Removing Data from Retain

When older messages have reached the end of the data retention policy, use Data Removal as described in “[Deleting Data](#)” in *Retain 4.10.1: Configuration and Administration*. to permanently remove messages from the archive.

3 Target Systems and Data Streams

The systems and data streams which Retain can archive are listed below:

- ♦ [“Smart Phone Targets” on page 17](#)
- ♦ [“Email System Targets” on page 17](#)
- ♦ [“Search Engine Targets” on page 17](#)

Smart Phone Targets

Retain can archive PIN, SMS, and phone call data, as configured.

- ♦ Blackberry (BES Server)
- ♦ BBM Enterprise (on all platforms)
- ♦ Android
- ♦ IOS and Android (via CellTrust Secureline)

Email System Targets

Retain archives all specified data, which can include: email, notes, appointments, meetings, reminders, and tasks, from the following email systems.

- ♦ Exchange
- ♦ Office 365
- ♦ GroupWise
- ♦ Gmail
- ♦ Bloomberg
- ♦ GBS Notes

Search Engine Targets

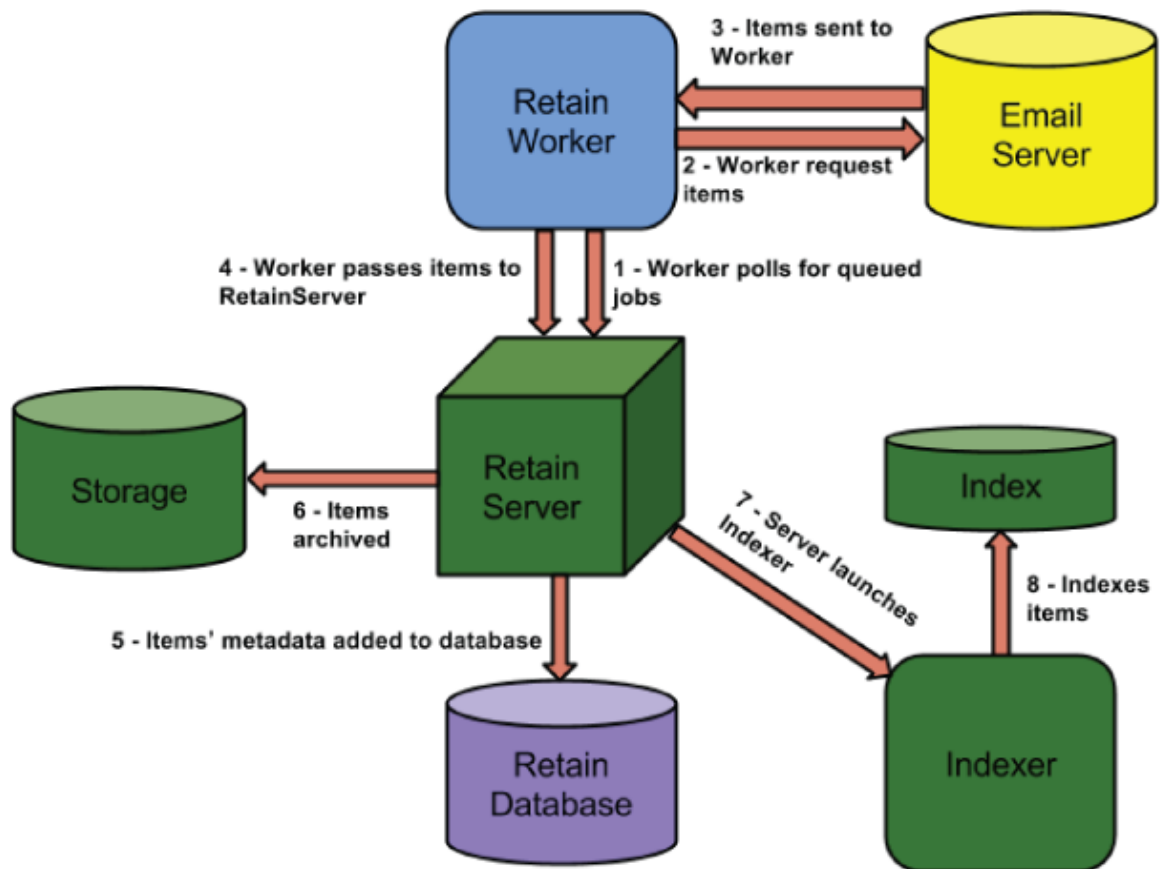
For Search Engines, Retain can archive the search criteria specified by search-engine users.

4 Jobs

- ♦ [“How Archive Jobs Work” on page 19](#)
- ♦ [“An Archive Job Example” on page 20](#)

How Archive Jobs Work

When an archive dredge job is running, the work flow follows this pattern.



1. The Worker polls the Server every 10 minutes (default) for new queued jobs it may need to run. It launches the job.
2. The Worker connects to the messaging system, logs in to each mailbox, and requests the items in that mailbox based on the settings in the profile.
3. The messaging system responds by sending the items to the Worker.

4. The Worker sends smaller items to the Server. For large items, it sends the item's metadata and awaits instructions from the Server as to whether the item already exists.
 - ♦ If it already exists, the Retain Server notifies the Worker that it does not need to send the item over.
 - ♦ If it does not exist, the Retain Server notifies the Worker to send the item.
5. The Retain Server updates the Retain database with a record of the item's metadata if a record does not already exist.
6. The Server adds the item to the storage area on disk.
7. The Server launches the indexing process (if it is not already running) to begin the indexing process.
8. The Indexer indexes any items that need to be indexed.

An Archive Job Example

1. User A sends message 1 to User B.
2. When a Worker processes User A's mailbox, Retain archives Message 1 in the Retain archive and creates a record in the database that points to the archived message and associates it with User A's mailbox.
3. When a Worker processes User B's mailbox, Retain notes that message 1 is already archived and that a database record already exists.
4. Therefore, Retain only needs to update the database record so that the message is also associated with User B's mailbox.

5 Retain Users and Groups

- ♦ “Populating Retain’s Archive Address Book” on page 21
- ♦ “Retain Users and User Accounts” on page 21
- ♦ “Retain Handles Users with the Same Name” on page 23
- ♦ “Archive Address Book Users Are Protected from Removal” on page 23
- ♦ “Retain’s LDAP Service” on page 23
- ♦ “General Account Control” on page 24

Populating Retain’s Archive Address Book

Username and other information associated with archived messages are imported to Retain’s [Address Book](#) the first time Retain archives a given user’s message data.

By default, these users can then authenticate to Retain using their messaging system credentials. For example, GroupWise users authenticate using SOAP or GroupWise LDAP, Exchange users authenticate using Active Directory credentials.

The first time they authenticate they are added to the list of Retain User Accounts, explained next.

NOTE: You can prevent users from logging in by using the “[Account Management Panel](#),” documented in [Retain 4.10.1: Configuration and Administration](#)

Retain Users and User Accounts

Whereas the Retain Address Book is integral to organizing the archive and tracking all user identities on the system, it is a system-level component that operates mainly “behind the scenes.”

The primary purposes of Retain User Accounts are administration and access to the Retain archive.

User Accounts store individual user configuration settings that govern such things as preferences, administrative rights, the mailboxes to which users have access, authentication requirements, and encrypted account passwords.

If a user in the Retain Address Book successfully logs in to Retain, the password used is encrypted for use in subsequent authentication requests, and the user is added to Retain’s [User Account List](#). This process is explained in “[Authentication Part 1: Username/Password or OpenID Connect](#)” on page 25.

There are three ways that User Accounts get created, as outlined in [Figure 5-1](#) and explained in [Table 5-1](#), “[Populating Retain’s User Account List](#),” on page 22.

Figure 5-1 Retain User Account Creation

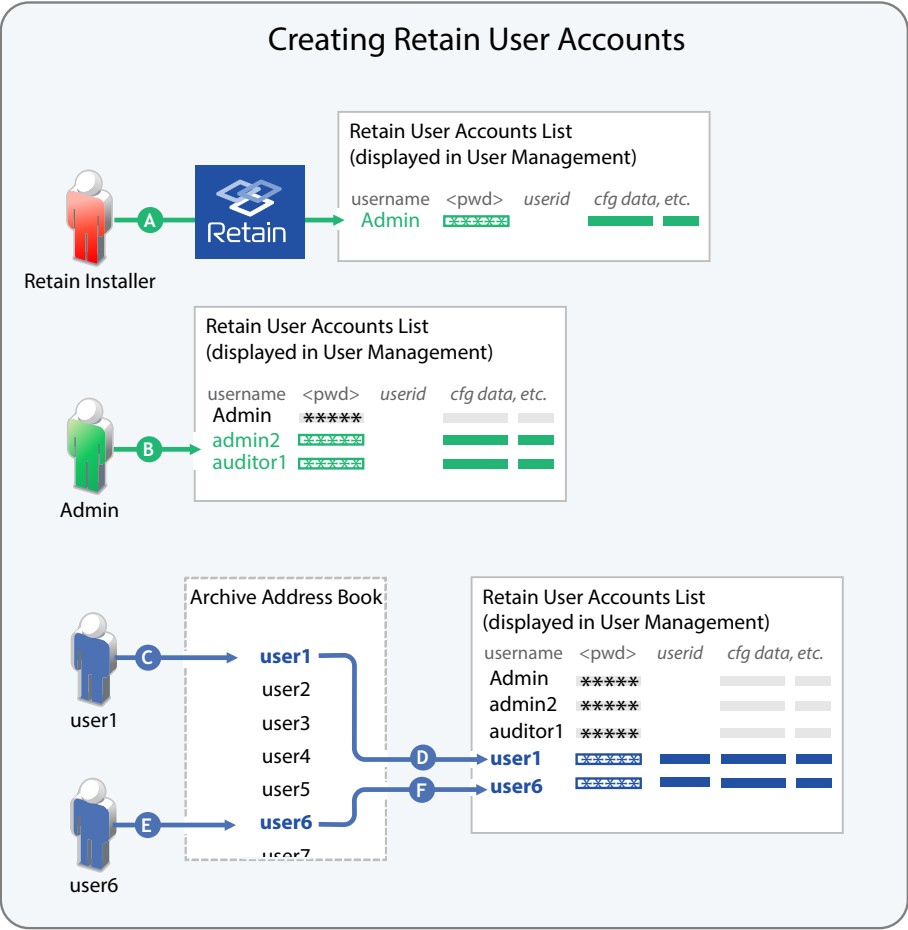


Table 5-1 Populating Retain's User Account List

Letter	Explanation
A	The first Retain User Account is created during the Retain installation process and is the system administrator, Admin.
B	After Retain is installed and configured, the Admin user can create other Retain users to help with various administrative functions, such as report generation and auditing. These users authenticate using what Retain calls "Offline Passwords," which you create for them. "Offline" means that no connection to a separate messaging system is required for authentication because the password is encrypted and stored locally. In the example graphic, Admin creates the users admin2 and auditor1.
C	As message data is archived, usernames associated with the archived data are created in the Archive's Address Book. At this point there are no Retain User Accounts associated with the usernames. In the example graphic, User1 wants to access the Retain archive, so it enters the same username and password as when accessing the back-end messaging system.

Letter	Explanation
D	<p>Next, the processes described in “Authentication Part 1: Username/Password or OpenID Connect” on page 25 take place.</p> <p>As described in Figure 6-1 on page 26, letter N, if User1 enters valid credentials, a User Account is created in the Retain User Account List.</p>
E	User6 also wants to access the archive, so it enters the username and password from its back-end messaging system.
F	<p>The same process occurs for User 6 as described for User1 in letter D.</p> <p>At this point, the Archive Address Book contains at least 7 users with archived data, but only two of them have Retain User Accounts.</p>

Retain Handles Users with the Same Name

Retain distinguishes between multiple users with the same name by assigning each user a unique userid in the archive.

For example, “John Smith” added today, is a different user from “John Smith” who began working at the company six months ago, and from “John Smith” who left the company last year.

Archive Address Book Users Are Protected from Removal

The Retain Archive Address Book contains all users (current and past) who have archived data. These might or might not have associated [Retain User Accounts](#) through which they can access the Retain Archive and perform administrative tasks.

As long as users have archived messages, their mailboxes cannot be removed from the archive’s address book. For more information about removing users who no longer have archived messages, see [“Deleting Mailboxes”](#) in the [Retain 4.10.1: Configuration and Administration](#) guide.

Retain’s LDAP Service

Starting with version 4.10, Retain provides an internal LDAP directory service that delivers identity services for the users with Retain User Accounts (listed in the [User management dialog box](#)).

You enable Retain’s embedded LDAP service in the [“NetIQ Advanced Authentication Configuration Panel,”](#) documented in the [Retain 4.10.1: Configuration and Administration](#) guide.

The sole purpose of this service is to provide multi-factor authentication (MFA) for those with Retain User Accounts, including mobile and offline users.

MFA is provided through an integration with NetIQ Advanced Authentication. For configuration instructions, see [“Configuring Retain for NetIQ Advanced Authentication MFA Support”](#) in the [Retain 4.10.1: Configuration and Administration](#) guide.

WARNING: Do not attempt to manage Retain’s embedded LDAP service using an LDAP management tool. Doing this will break the service.

User and Group creation and deletion, port configuration changes, etc. must be made only through the Retain management UI.

General Account Control

The “[Account Management Panel](#),” documented in [Retain 4.10.1: Configuration and Administration](#), lets you control:

- ♦ When/how new accounts are created.
- ♦ When accounts expire.
- ♦ Which users can log in.
- ♦ How strong passwords must be (except when overridden by associated messaging systems).

6 Authentication, Standard and Multi-factored

To access archived content or administer Retain services, users must authenticate to Retain.

- ♦ [“Authentication in Retain” on page 25](#)
- ♦ [“Authentication Part 1: Username/Password or OpenID Connect” on page 25](#)
- ♦ [“Authentication Part 2 \(Multi-factor Authentication\)” on page 27](#)
- ♦ [“All Retain Users Can Be Enabled for MFA Authentication” on page 29](#)
- ♦ [“Duplicate LDAP User Entries Are Not Allowed” on page 29](#)
- ♦ [“MFA Can Work When Back-end Messaging Systems Are Offline” on page 29](#)
- ♦ [“When Google and Office 365 Systems Require an App Password” on page 30](#)
- ♦ [“Authentication is persistent” on page 31](#)

Authentication in Retain

Of necessity, access security has increased over the years and Retain now supports multi-factor authentication (MFA) for all Retain users.

Security enhancements have been included in the following releases:

- ♦ **Retain 4.9.1:** Introduced OpenID Connect integration, which added **Login Using Office 365** and **Login Using Google** buttons to the Retain Login dialog.

If you have configured your Retain system to support existing OpenID Connect implementations on [Office 365](#) or [GSuite](#), those users can click their respective Login button and authenticate directly to their email systems. If they are already signed in, Retain opens without further input.

Other users must enter a username and password as the first step.

- ♦ **Retain 4.9.2:** Added an integration with NetIQ Advanced Authentication that supported multi-factor authentication for GroupWise and Exchange users by leveraging their respective LDAP identity services.
- ♦ **Retain 4.10:** Extends MFA support to all Retain users, including mobile and offline. This leverages a special-purpose LDAP service associated with Retain’s Archive Address Book.

Current Retain Authentication processes are summarized in the following sections:

Authentication Part 1: Username/Password or OpenID Connect

Traditionally, users authenticate to Retain by entering a username and password.

[Figure 6-1 on page 26](#) illustrates how Retain processes initial input to the Login dialog.

Figure 6-1 Authentication - Part 1

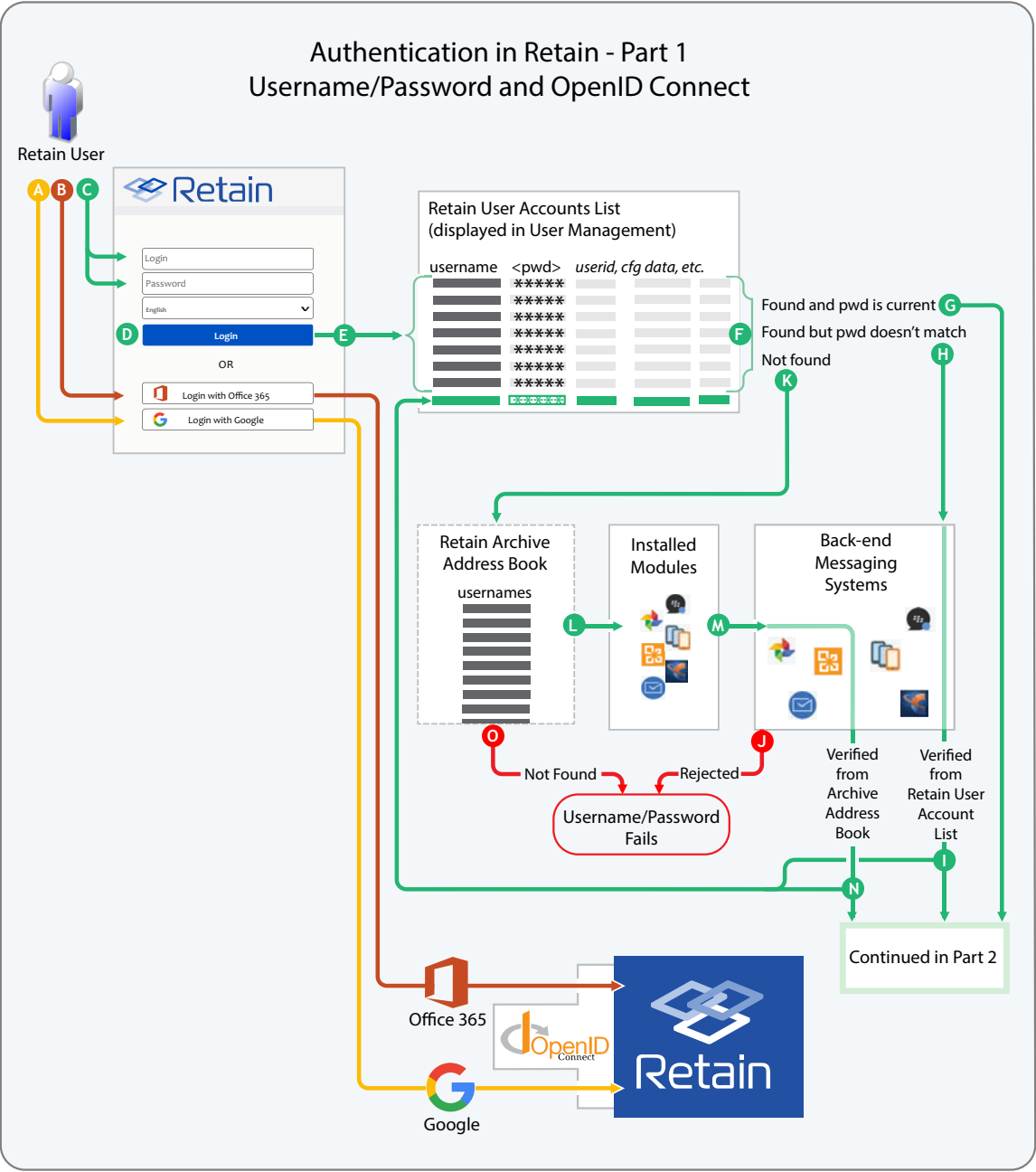


Table 6-1 Authentication - Part 1

Letter	Explanation
A	GSuite users who are enabled for access through Google's OpenID Connect implementation, can click the Login with Google button. They can then authenticate to their GSuite account and Retain recognizes the authentication as valid.

Letter	Explanation
B	Office 365 users who can access their Office 365 account through Microsoft's OpenID Connect implementation, can click the Login with Office 365 button. They then authenticate to their Office 365 account and Retain recognizes the authentication as valid.
C	The user types a username and a password.
D	Then the user clicks Login .
E	Retain checks for the username in the User Account List and if it is found, Retain then checks the entered password against the one that is cached for the user.
F	There are three possible results: <ul style="list-style-type: none"> ♦ G User Account found, Password current: In this case the authentication process continues as illustrated in Figure 6-2, "Authentication - Part 2," on page 28. ♦ H User Account found, Password doesn't match: In this case Retain requests verification with the back-end messaging system associated with the user account. <ul style="list-style-type: none"> ♦ I If the back-end system verifies the username/password, Retain updates the cached password and the request continues in Figure 6-2, "Authentication - Part 2," on page 28. ♦ J If the verification request fails, the authentication process stops and notifies the user. ♦ K User Account not found, the authentication process checks the archive's Address Book. <ul style="list-style-type: none"> ♦ L If the user is in the address book, the process accesses the installed modules for back-end messaging system connections. ♦ M The process connects to relevant back-end messaging systems. ♦ N When a back-end system verifies the username/password combination, Retain encrypts the password and adds the user to the User Account list. The request then continues the process in Figure 6-2, "Authentication - Part 2," on page 28. ♦ O If the user is not in the archive's address book or if no back-end system verifies the username/password, the verification request fails, and the authentication process stops and notifies the user.

Authentication Part 2 (Multi-factor Authentication)

After a user authenticates to Retain by entering a correct username and password, Retain must then determine whether additional authentication is required before granting access to its archives and administrative functions.

[Figure 6-2 on page 28](#) illustrates how Retain determines additional authentication requirements and provides a high-level overview of how and when processes happen.

Figure 6-2 Authentication - Part 2

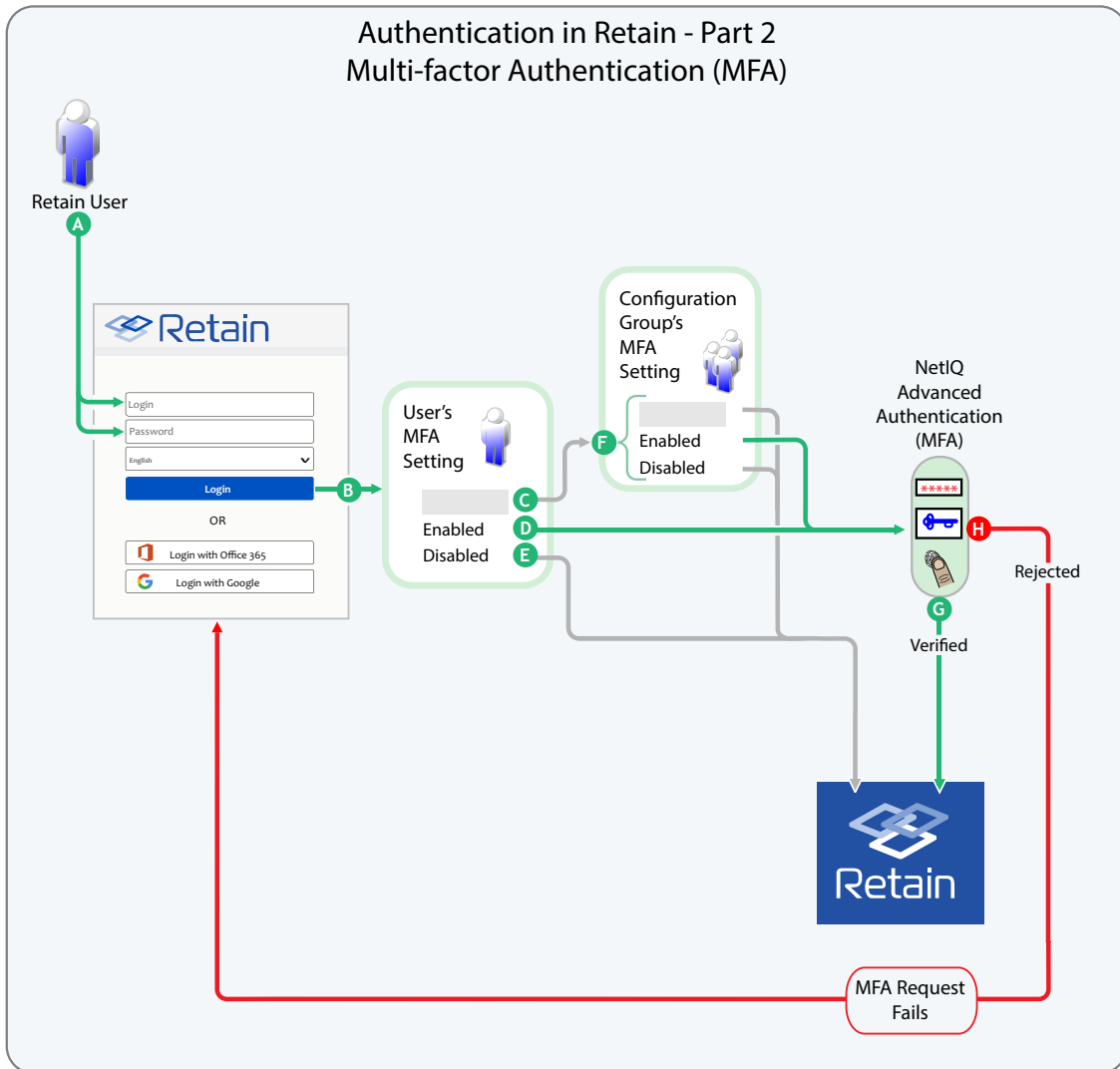


Table 6-2 Authentication - Part 2

Letter	Explanation
A	All other users start the authentication process by entering a Username and Password.
B	After the request is validated as illustrated in Figure 6-1 on page 26 , Retain accesses the user's configuration settings to determine whether there are MFA requirements. User settings always override group settings.
C	If a user's MFA setting is Blank (not set): Retain checks the Configuration Group's MFA setting , as explained in H below.
D	If a user's MFA setting is Enabled: Retain displays the MFA prompts defined in the applicable NetIQ Advanced Authentication configuration. For more information about configuring Retain to interface with NetIQ Advanced Authentication, see " Configuring Retain for NetIQ Advanced Authentication MFA Support " in Retain 4.10.1: Configuration and Administration .

Letter	Explanation
E	If a user's MFA setting is disabled: Retain verifies the username and password and logs the user in.
F	If a user's MFA setting is blank (C), Retain uses the applicable Configuration Group's setting as follows: <ul style="list-style-type: none"> ♦ If the Group's MFA Setting Is Blank or Disabled: Retain authenticates the user. ♦ If the Group's MFA Setting Is Enabled: Retain displays the MFA prompts defined in the applicable NetIQ Advanced Authentication configuration.
G	If the user completes the MFA requirements successfully, Retain recognizes the authentication as valid.
H	If the user fails the MFA requirements, Retain rejects the authentication request and notifies the user

See the following sections for more information on Multi-factor Authentication in Retain:

All Retain Users Can Be Enabled for MFA Authentication

You can configure NetIQ AA service to provide MFA authentication for any Retain users with a [Retain User Account](#).

To set this up, follow the instructions in “[Configuring Retain for NetIQ Advanced Authentication MFA Support](#)” in the [Retain 4.10.1: Configuration and Administration](#) guide.

Duplicate LDAP User Entries Are Not Allowed

Although NetIQ AA can leverage multiple LDAP identity repositories, you must ensure that Retain users only appear in one of them.

For example, if you configured NetIQ AA multi-factor authentication for GroupWise or Exchange users in Retain 4.9.2, it follows that you also defined AA repositories for their respective LDAP services.

If you now add a repository for Retain's User Accounts LDAP service, your GroupWise and Exchange users will have duplicate accounts. Therefore, you must remove their respective LDAP repositories from your NetIQ AA service.

MFA Can Work When Back-end Messaging Systems Are Offline

If users have previously connected to Retain using MFA, they can still log in to Retain using MFA, provided that

- ♦ The NetIQ Advanced Authentication service is online and accessible to Retain.
- ♦ The LDAP identity repositories configured in NetIQ AA are still accessible to it.
- ♦ The users needing access are able to use offline access. See “[Authentication Method](#)” in the [Retain 4.10.1: Configuration and Administration](#) guide.

When Google and Office 365 Systems Require an App Password

NOTE: The explanations in this and other sections use the general term “Username/Password Authentication” to refer to the following authentication methods: Google IMAP, Exchange Authentication, GroupWise LDAP, GroupWise SOAP, and Retain Offline Authentication.

When the following conditions are both met, Google and Office 365 require their users to enter an assigned App Password rather than the password associated with their email accounts.

- ☐ The Google or Office 365 systems provide Two-Factor Authentication (2FA) support through OpenID Connect.
- ☐ Users choose to authenticate by entering a username and password rather than by clicking their respective Login button.

In other words, GSuite users request authentication through Google IMAP and Office 365 users request authentication through Exchange Authentication, both of which are username/password authentication systems.

Example 1

1. Rather than clicking the **Login with Office 365** button in the Retain Login dialog, an Office 365 user enters a username and password.
2. Because the user’s account has no [Authentication Method Restrictions](#), Retain seeks confirmation from the Office 365 system through the Exchange Authentication method, generally illustrated in [Figure 6-1 on page 26](#).
3. If the user enters its assigned App Password, the request succeeds, the App Password is cached for the User Account, and so on as illustrated.

On the other hand, if the user enters its email account password (or anything other than the App Password), the request fails.

Example 2

A Google back-end email system is configured to provide Two-factor Authentication (2FA) through OpenID Connect.

However, the Retain Administrator has not enabled Retain to support OpenID Connect on the Google system. This leads to the following scenario.

1. The **Login with Google** button doesn’t display in the Retain Login dialog.
2. Therefore, the user must use Username/Password (Google IMAP) authentication to access Retain.
3. Because the Google system provides 2FA through OpenID Connect, Google IMAP only accepts an assigned App Password.
4. If the user knows about the App Password requirement and enters that, it can access Retain as illustrated in [Figure 6-1 on page 26](#).

On the other hand, if the user enters an incorrect password (including the one that it uses to access its GSuite account), the request fails.

IMPORTANT: If you want your Office 365 or GSuite users to only authenticate through their respective email services, consider restricting their Authentication Methods to “[Microsoft OpenID Connect Exclusive](#)” or “[Google OpenID Connect Exclusive](#)” as detailed in the [Retain 4.10.1: Configuration and Administration](#) guide.

If you choose not to restrict their authentication methods for whatever reason, they can choose to enter a username and password rather than clicking the appropriate **Login** button.

As explained in the Examples above, if their back-end systems provide Two-factor Authentication (2FA) through OpenID Connect, they need to enter their assigned App Password rather than the one they normally use.

You should inform them of the App Password requirement because the only system feedback they will receive is that the Login attempt failed.

Authentication is persistent

After authentication credentials are entered, they last until the browser’s associated cookies have expired.

7 Retention Services and Item Store Flags

- ♦ [“How Retain Works with GroupWise Retention Services” on page 33](#)
- ♦ [“How Retain Works with Exchange and Office 365” on page 34](#)
- ♦ [“How Retain Works with Gmail” on page 35](#)

Retain keeps an "item store flag" to ensure that no item gets left behind.

With Exchange and O365 Holds and the Recoverable Items folder can be used for retention compliance. With On-Premise Exchange a journaling mailbox can be used but it is not recommended.

Gmail, by default, does not have a retention service.

GroupWise, on the other hand, has its own built-in feature called "Retention Services" that prevents items from being emptied from the mailbox until they have been successfully archived.

The following sections explain Retain's support of the GroupWise Retention Services, followed by a discussion of how Retain ensures that all items get archived in all other email systems.

How Retain Works with GroupWise Retention Services

GroupWise has a feature that can be enabled in its GroupWise Administration option called Retention Services.

When enabled, GroupWise prevents a user from emptying an item from Trash that has not yet been confirmed to have been archived. The way it does this is through a date/time field in each user database called the "digest retention time". It relies on third party archiving solutions like Retain to set that date/time, but GroupWise is the one that enforces it when set. This prevents any item newer than the date/time set in the "digest retention time" field from being emptied from Trash. This "digest retention time" is known in Retain as the "retention flag."

When Retain runs an archive job on a mailbox, it sets the digest retention time to the date/time of the newest/latest message it archived. However, if an error occurs on any item during that job which prevents Retain from archiving it or its attachment, Retain sets the digest retention time in the GroupWise user database for that mailbox to the date/time of the item that could not be archived due to an error.

And, even though Retain encounters an error on an item and cannot archive it, it moves beyond that item and continues to archive all other mailbox items; however, again, it doesn't advance the retention flag past the date/time of the FIRST error it encountered. Thus, when the next archive job gets run on that mailbox, Retain checks the item store time set in its database of the user and uses that date/time as its starting time for the new job, minus one hour.

Example: If today is September 17, 2014 but an item in the previous job produced an error, could not be archived because of that error, and had a delivered date/time of September 15, 2014 09:15, then when today's job runs, it asks GroupWise for all items beginning with September 15, 2014 08:15 and later.

Now let's say that a month has passed and the problematic mail message has not been properly dealt with and we run a job. Even though Retain may have archived all items in the user's mailbox up to - let's say October 15th - it still starts the query with the item store time of September 15, 2014 08:15 because it could not advance the retention flag. If it were to do so, then the problem message would never get archived because Retain starts the query for items beginning with the digest retention time. Thus, if Retain were to advance the flag to the date/time of the newest/latest item it archived, then the problematic message would fail to fit within the query range and GroupWise would never send it to Retain.

How Retain Works with Exchange and Office 365

These email systems do not have a built-in retention service similar to GroupWise, there is no "digest retention time" field in any of their mail system databases that Retain can use; thus, Retain uses its own field in the "retain" database to keep track of its job starting point. This "item store flag" works just like the "retention flag" with GroupWise jobs. That date/time gets set to the date/time of the newest/latest item archived for a given mailbox; or, if an error(s) occurred during a job, the item store flag gets set to the date/time of the first item that had an error. That way, when the next archive job runs, it starts with the date/time of the item store flag, ensuring that Retain tracks the item until it is properly archived. However, it is important to note that not advancing the item store flag does not prevent the user from emptying the item from their Trash in these email systems because they do not have a retention feature similar to GroupWise.

Placing a Hold Prevents Loss of Unarchived Messages

To prevent items from being deleted from Exchange/O365 a hold must be placed on the mailboxes. This can be an In-Place or Litigation hold. When a user deletes a message from Outlook the message is moved to the Trash, the user can then empty the trash. Exchange/O365 then moves the message to a Recoverable Items folder for 14 days before removing it from disk. However, a user can right-click on the trash and attempt to recover a deleted item, and at this point can purge an item immediately to remove it completely. This may be against your data retention policy, so to prevent the deletion, a hold then moves the item to the hidden Purged folder, where the user cannot remove it but Retain can still archive it.

Journaling Mailbox, an Alternative to the Item Store Flag but Not Recommended

Alternatively, a journaling mailbox may be used on On-Premise Exchange. When a journaling mailbox is set up in Exchange, it can be configured in a way that redirects a copy of each message that is either sent or received throughout the entire mail system into the journaling mailbox. Retain can be configured to include the journaling mailbox in its archive job. Thus, even if a user empties an item from Trash, a copy of that item already exists in the journaling mailbox and remains in that mailbox until it is archived by Retain. If configured properly, Retain removes that item from the journaling mailbox upon successfully archiving it. Items emptied from a user's Exchange mailbox but archived from the journaling mailbox do not appear in the user's Retain mailbox; however, they are searchable using the Retain search feature.

Because of the fact that duplicates of all email messages system wide get placed in the journaling mailbox, it can fill up fast. For this reason, we recommend that you not use the journaling mailbox feature and go with the Recoverable Items feature instead. If the journaling mailbox gets too big, Exchange is no longer able to serve the mailbox. Thus, when Retain tries to run an archive job against it, it fails because Exchange never responds back. This is why it is no longer recommended.

How Retain Works with Gmail

Gmail does not have retention services, by default. That requires the purchase of their Vault service.

8 Retain Unified Archiving Version Numbering

Retain software versions are incremented as follows:

major-version.minor-version.service-pack.patch-release

Each number in the version string is 1 or 2 digits (0-99).

Examples include (in chronological order):

- ♦ **4.0** The initial release of Retain 4
- ♦ **4.8** The eighth minor- version release of Retain 4
- ♦ **4.8.0.1** The first patch release for Retain 4.8
- ♦ **4.8.2** The second service pack release for Retain 4.8
- ♦ **4.10** The tenth minor-version release of Retain 4

Patches and service packs are generally developed for the current version only.

