LITERA

Litera Transact SeeUnity/iManage Integration

Data Security

May 2022

Litera
550 West Jackson Blvd.
Suite 200
Chicago, IL 60661
US: +1 630 598 1100   UK: +44 (0)20 3890 2860

On the Web: https://www.litera.com/

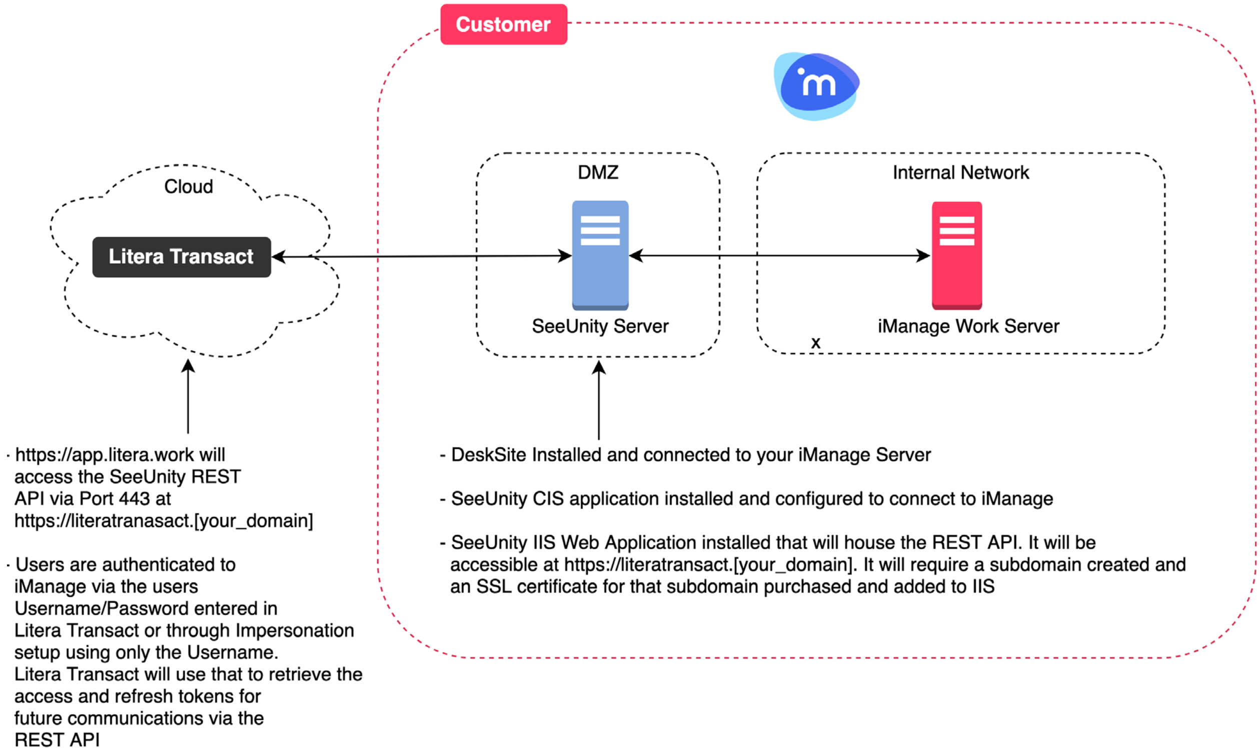
Contents

Overview

This document explains the security measures in place for data when using the Litera Transact transaction management platform, integrated into iManage Work server using SeeUnity.

It covers data in transit as it is transferred to and data at rest within the Litera Transact transaction management platform.

The following diagram shows the architecture of the system as a whole.



· https://app.litera.work will access the SeeUnity REST API via Port 443 at https://literatranasact.[your_domain]

· Users are authenticated to iManage via the users Username/Password entered in Litera Transact or through Impersonation setup using only the Username. Litera Transact will use that to retrieve the access and refresh tokens for future communications via the REST API

- DeskSite Installed and connected to your iManage Server
- SeeUnity CIS application installed and configured to connect to iManage
- SeeUnity IIS Web Application installed that will house the REST API. It will be accessible at https://literatransact.[your_domain]. It will require a subdomain created and an SSL certificate for that subdomain purchased and added to IIS

Note: For this integration, the iManage Work server must be installed on premise.

Litera Transact will access the SeeUnity REST API via Port 443 at https://literatransact.[your_domain].

Users are authenticated to iManage via the user’s user name and password entered in Litera Transact or through impersonation setup where Litera Transact uses the user’s SeeUnity user name.

Our approach to security

Litera has ISO 27001:2013 certification in respect of information security for the Litera Transact platform.

We know that keeping customer data safe and secure is of paramount importance and one of our most important responsibilities.

We are dedicated to ensuring that our customers have the highest confidence in our security practices and infrastructure.

Introducing the Litera Transact-SeeUnity-iManage integration

Litera Transact is a cloud-based SaaS application. Access to the application is delivered to end-users through a browser and no desktop installation is required. Customer accounts are set up within the multi-tenant cloud application, meaning the data of all customers is contained within a single application database. Individual users only see the deals that they have access to within the database. All data and files are hosted with Amazon Web Services (AWS).

The Litera Transact-SeeUnity-iManage integration provides a compromise between on-premise and cloud by linking a customer's multi-tenant cloud account to their iManage DMS. Effectively this creates an on-premise storage for files. The application database data remains in the cloud with AWS, but files uploaded into Litera Transact are stored in the same setup as the customer's iManage files. This deployment option is provided through the DMS integration technology provided by SeeUnity.

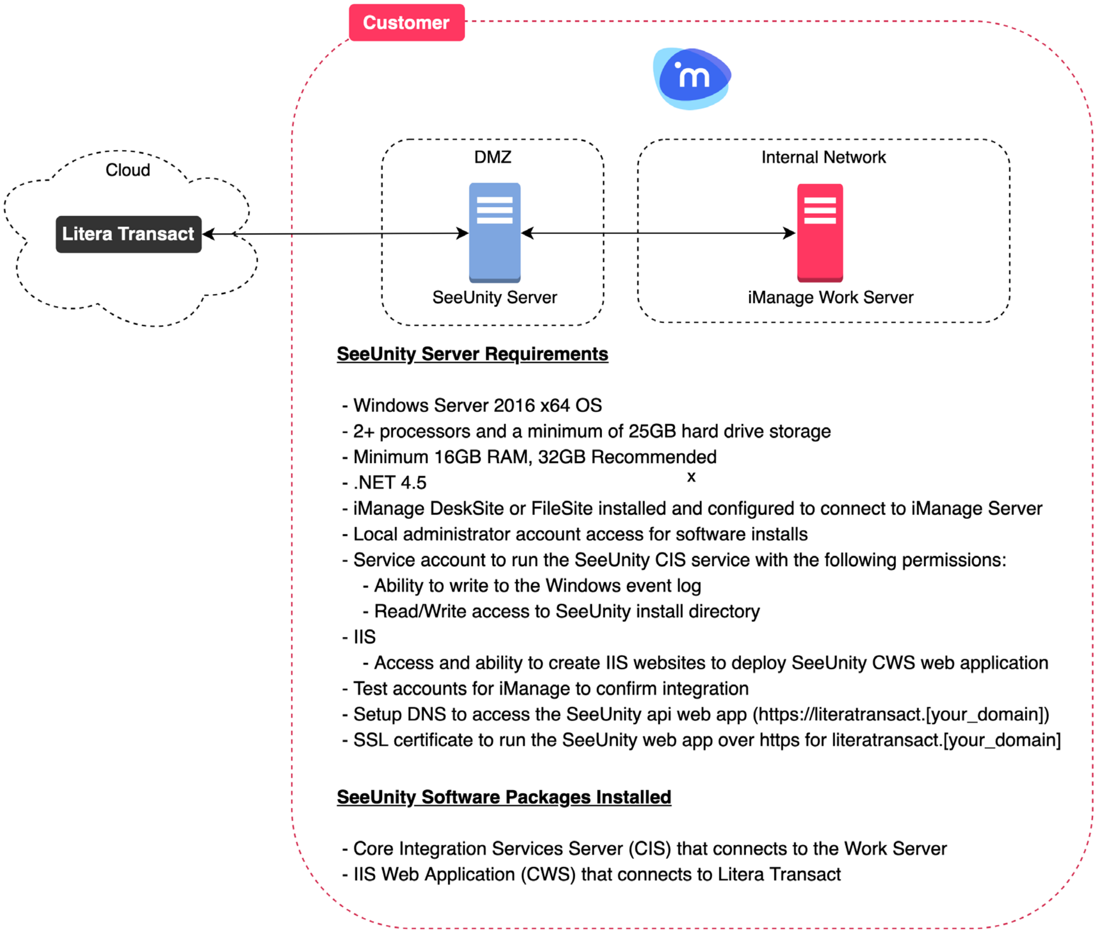
SeeUnity server requirements

The system requirements for the SeeUnity server are summarized below.

- Microsoft Windows Server 2016 x64 OS
- 4+ processors and minimum 25 GB hard drive storage
- Minimum 16 GB RAM (32 GB recommended)
- Microsoft .NET 4.5 (and 3.5)
- iManage DeskSite or FileSite installed and configured to connect to the iManage Server
- Local administrator account access for software installs

- Service account to run the SeeUnity CIS service with the following permissions:
  - Ability to write to the Windows event log
  - Read/write access to the SeeUnity install directory
- Microsoft Internet Information Service (IIS)
  - Access and ability to create IIS websites to deploy SeeUnity CWS web application
- Test accounts for iManage to confirm integration
- DNS setup to access the SeeUnity API web app (https://literatransact.[your_domain]
- SSL certificate to run the SeeUnity web app over https for literatransact.[your_domain]
- SeeUnity software packages installed:
  - Core Integration Services (CIS) server that connects to iManage Work server
  - IIS web application (CWS) that connects to Litera Transact

For a complete description, refer to the SeeUnity documentation.



SeeUnity Server Requirements

- Windows Server 2016 x64 OS
- 2+ processors and a minimum of 25GB hard drive storage
- Minimum 16GB RAM, 32GB Recommended
- .NET 4.5
- iManage DeskSite or FileSite installed and configured to connect to iManage Server
- Local administrator account access for software installs
- Service account to run the SeeUnity CIS service with the following permissions:
  - Ability to write to the Windows event log
  - Read/Write access to SeeUnity install directory
- IIS
  - Access and ability to create IIS websites to deploy SeeUnity CWS web application
- Test accounts for iManage to confirm integration
- Setup DNS to access the SeeUnity api web app (https://literatransact.[your_domain])
- SSL certificate to run the SeeUnity web app over https for literatransact.[your_domain]

SeeUnity Software Packages Installed

- Core Integration Services Server (CIS) that connects to the Work Server
- IIS Web Application (CWS) that connects to Litera Transact

Authentication

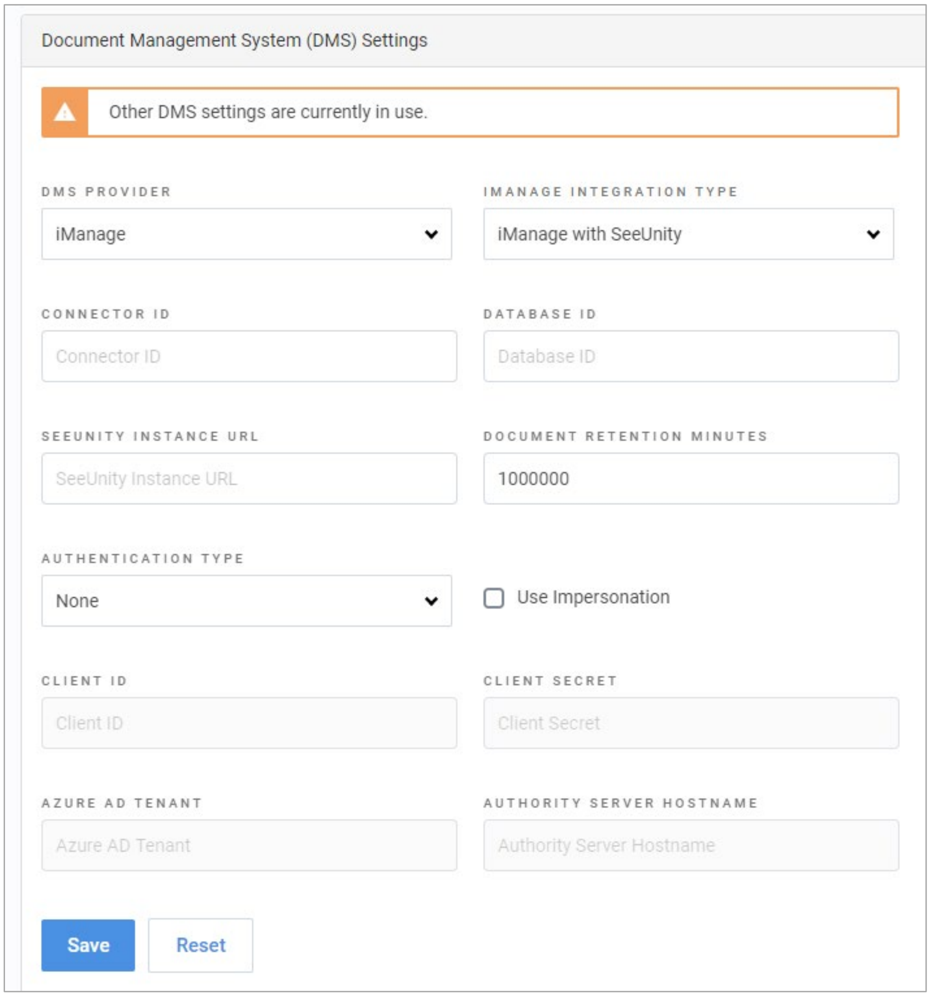
At the IIS-level, to protect the SeeUnity and IIS servers in the DMZ, Litera Transact supports two types of authentication - NTLM or Azure AD.

With regard to authenticating the user, the default authentication method is iManage user name and password. Litera Transact also supports an impersonation setup where Litera Transact uses only the user name to retrieve the access and refresh tokens for communication.

Note: The impersonation setup requires that a SeeUnity service account is configured and used to authenticate/establish the connection to the SeeUnity server.

On Litera Transact, authentication is configured from the Admin Portal. Configuration will also be required in IIS.

1. In the Admin Portal, select the **DMS** tab.
2. From the **DMS Provider** dropdown, select **iManage**.
3. From the **iManage Integration Type** dropdown, select **iManage with SeeUnity**.



Document Management System (DMS) Settings

Other DMS settings are currently in use.

DMS PROVIDER	IMANAGE INTEGRATION TYPE
iManage	iManage with SeeUnity
CONNECTOR ID	DATABASE ID
Connector ID	Database ID
SEEUNITY INSTANCE URL	DOCUMENT RETENTION MINUTES
SeeUnity Instance URL	1000000
AUTHENTICATION TYPE	
None	□ Use Impersonation
CLIENT ID	CLIENT SECRET
Client ID	Client Secret
AZURE AD TENANT	AUTHORITY SERVER HOSTNAME
Azure AD Tenant	Authority Server Hostname

Note: The message at the top alerts you when DMS integration has already been configured and you are making changes.

4. Specify the following parameters:

   Connector ID The name of the SeeUnity web server (WORKSITE, IMANAGE, etc.) You must specify this parameter. If the name includes characters other than letters and numbers, such as periods, you must also specify the **Database ID**.

   Database ID The name of the SeeUnity iManage database. This is only required if the **Connector ID** contains characters other than letters and numbers, for example, a fully qualified server name with periods.

   SeeUnity Instance URL The URL of the SeeUnity server.

   Document Retention Minutes The length of time that a file will be cached in Litera Transact. The minimum is 60 minutes and the maximum is 1,000,000 minutes. 1,000,000 minutes is recommended because the Litera Transact document cache is completely secure and users are less likely to have to wait for Litera Transact to fetch from the DMS when viewing documents.

   Authentication Type Select if the SeeUnity requires NTLM (Windows-based authentication) or Azure AD (Azure authentication).

   Client ID The SeeUnity user name required to access the IIS website on the SeeUnity server.

   Client Secret The SeeUnity password required to access the IIS website on the SeeUnity server.

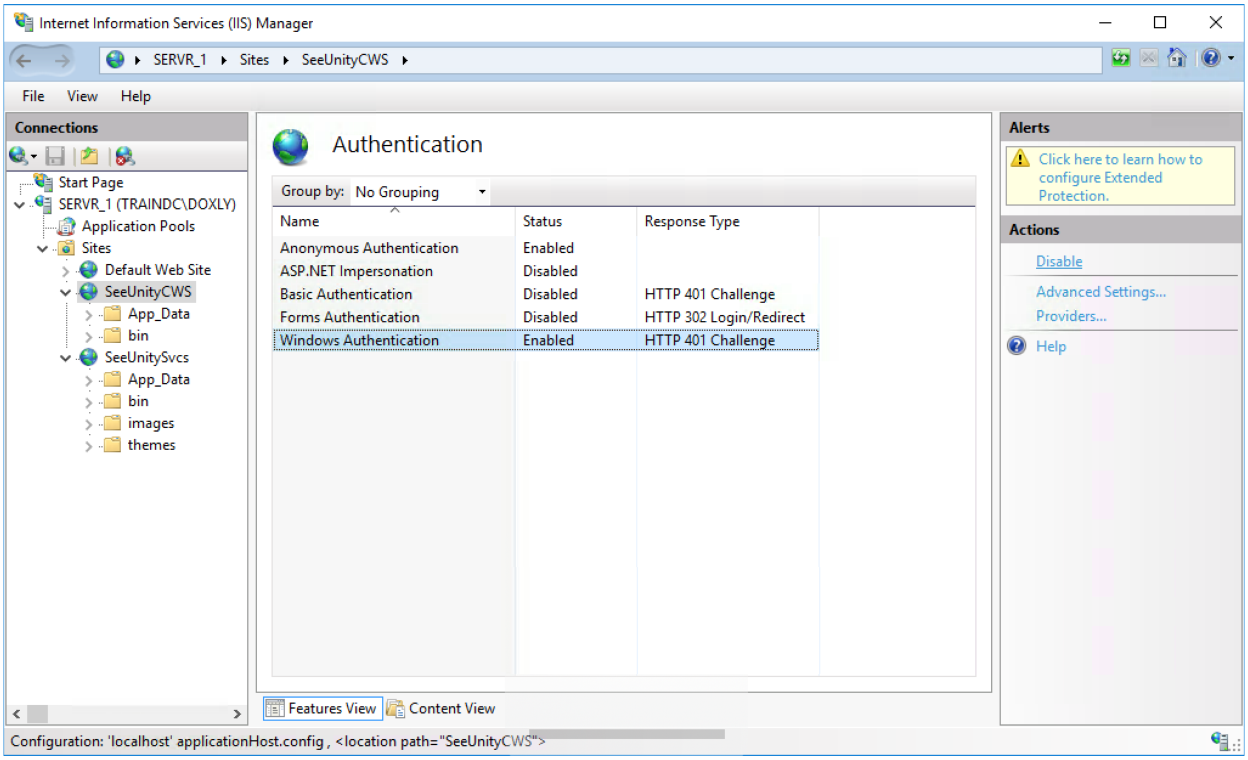
   Azure AD Tenant The GUID of the Azure tenant to authenticate to.

   Authority Server Host Name The base URL of where to authenticate to, typically login.microsoftonline.com or login.windows.net.

5. Select the **Use Impersonation** checkbox if you use impersonation in your iManage/SeeUnity integration. This will add an **Add SeeUnity Username** field for every user in the **Firm Roles** tab.
6. Click **Save**.

IIS configuration

When you select NTLM as your authentication type, you will need to disable **Anonymous Authentication** and enable **Windows Authentication** in IIS Manager.

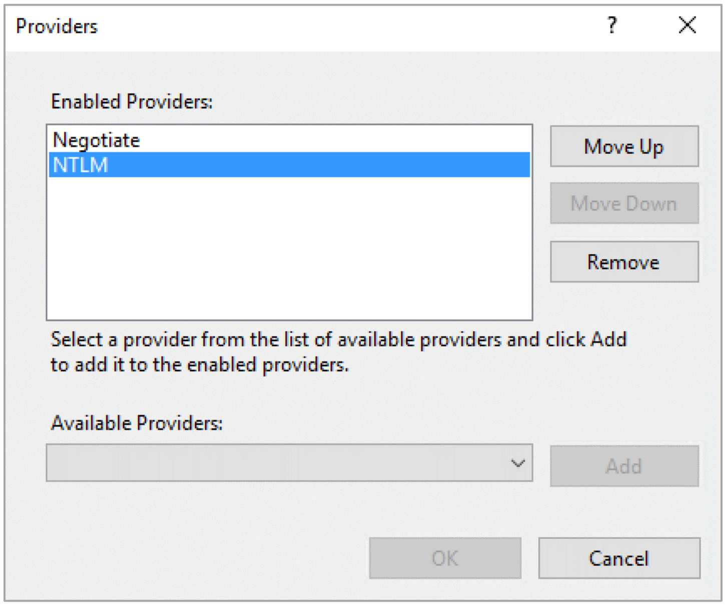


Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="SeeUnityCWS">

To confirm NTLM is an enabled provider, click **Providers**.



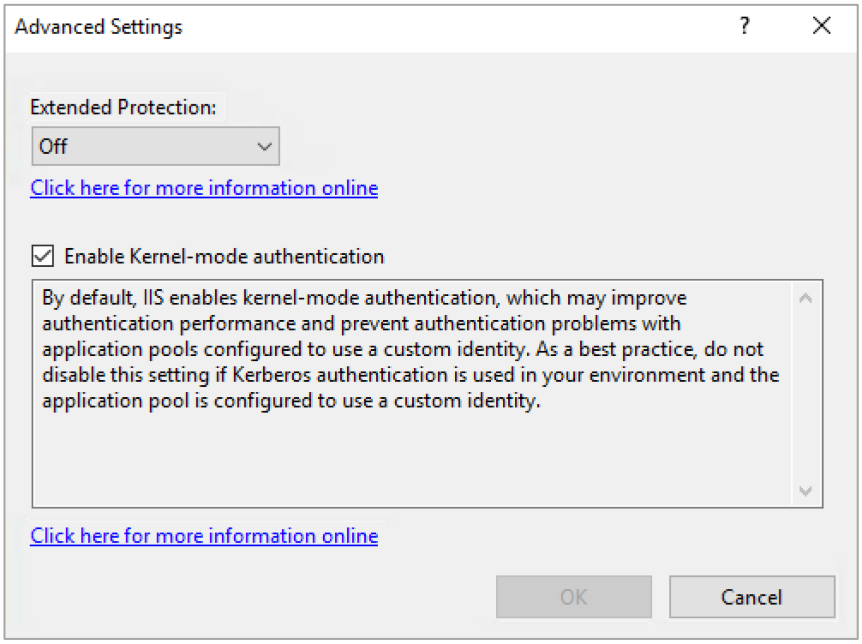
Enabled Providers:

Negotiate
NTLM

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

To change advanced settings, click **Advanced Settings**:



Advanced Settings

Extended Protection:

Off

Click here for more information online

☑ Enable Kernel-mode authentication

By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.

Click here for more information online

Data Security

How data is secured between Litera Transact and iManage

The following sections show the flow of data when Litera Transact users:

- Log into the iManage integration
- Browse iManage matters, folders and files from Litera Transact
- Upload iManage files to the Litera Transact checklist
- Download files from the Litera Transact checklist to iManage

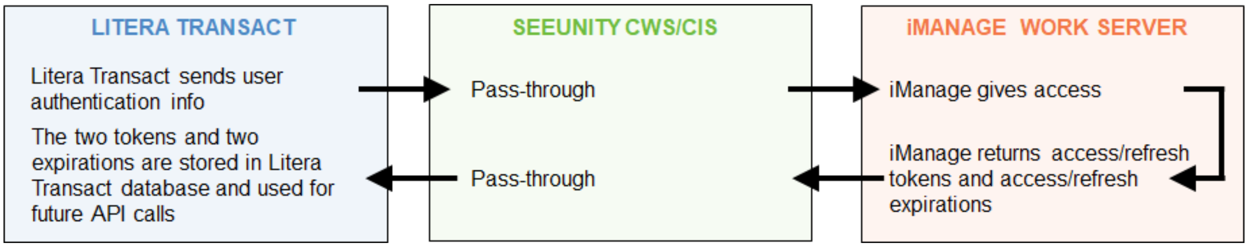
To achieve the above, system actions take place. The data flow is initiated in the user's browser and flows through the various components of the Litera Transact-SeeUnity-iManage ecosystem.

Note: All calls shown are made using HTTPS and therefore all communication is encrypted.

Litera Transact makes API calls in JSON. iManage Work 10.1 and above using REST API will also make API calls in JSON. However earlier versions of iManage Work server or servers using COM APIs will use XML. In that scenario, the SeeUnity server will convert the XML to JSON.

Authentication with user name and password

The user goes to the Integrations tab in Litera Transact and logs in with their iManage user name and password.



LITERA TRANSACT

Litera Transact sends user authentication info

The two tokens and two expirations are stored in Litera Transact database and used for future API calls

SEEUNITY CWS/CIS

Pass-through

Pass-through

iMANAGE WORK SERVER

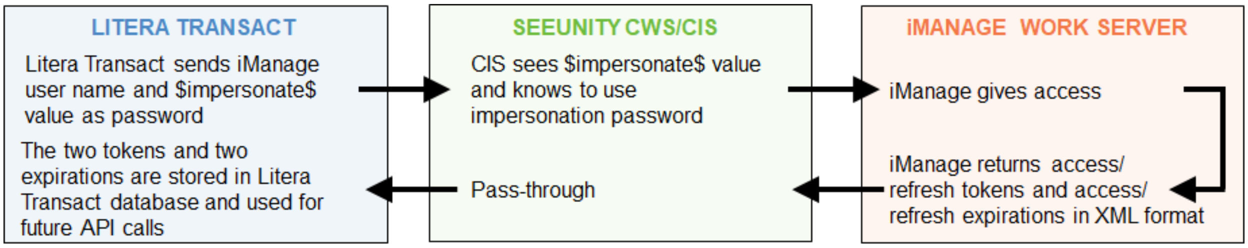
iManage gives access

iManage returns access/refresh tokens and access/refresh expirations

Authentication with user name and impersonation setup

The user goes to the Integrations tab in Litera Transact and provides their email address.

Setup required: Litera gets a list of users from a customer with the email and iManage user name for each user. A background task is run on Litera Transact that matches email address to iManage user and sends a request for each user. On CWS/CIS, the impersonation password is entered during install and stored in CIS.



LITERA TRANSACT

Litera Transact sends iManage user name and $impersonate$ value as password

The two tokens and two expirations are stored in Litera Transact database and used for future API calls

SEEUNITY CWS/CIS

CIS sees $impersonate$ value and knows to use impersonation password

Pass-through

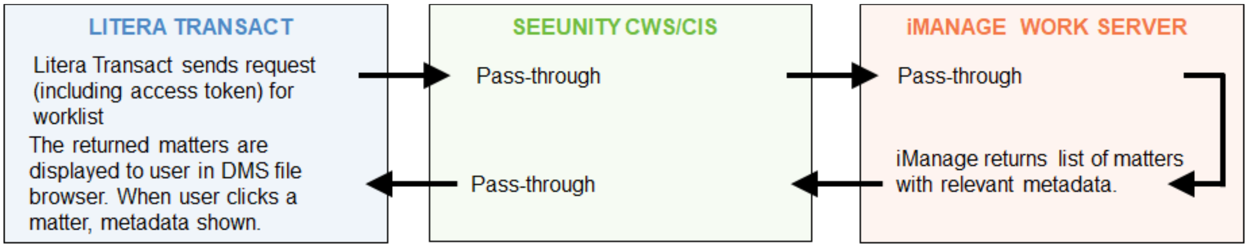
iMANAGE WORK SERVER

iManage gives access

iManage returns access/ refresh tokens and access/ refresh expirations in XML format

Browse matters, folders and favorites

In the checklist, the user clicks a document and selects to browse in iManage. The Litera Transact DMS file browser is displayed and the user clicks My Matters.



LITERA TRANSACT

Litera Transact sends request (including access token) for worklist

The returned matters are displayed to user in DMS file browser. When user clicks a matter, metadata shown.

SEEUNITY CWS/CIS

Pass-through

Pass-through

iMANAGE WORK SERVER

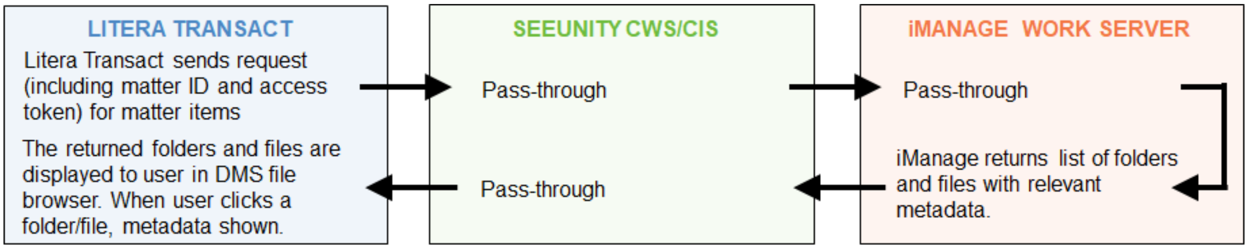
Pass-through

iManage returns list of matters with relevant metadata.

Note: Metadata includes information such as Name, FileID, etc.

Browse a matter

In the Litera Transact DMS file browser, the user double-clicks a matter.



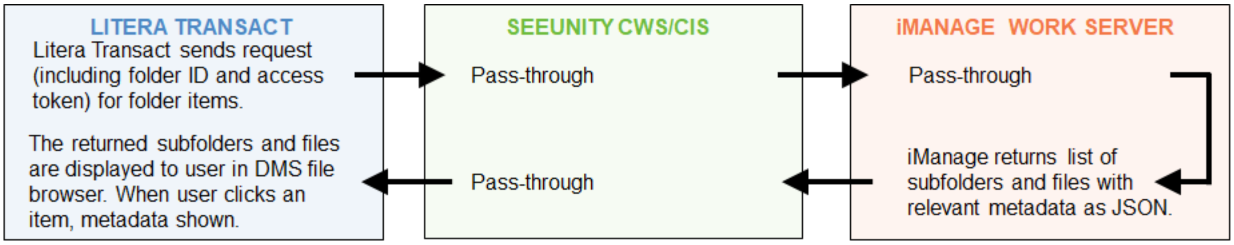
Litera Transact sends request (including matter ID and access token) for matter items

The returned folders and files are displayed to user in DMS file browser. When user clicks a folder/file, metadata shown.

iManage returns list of folders and files with relevant metadata.

Browse a folder

In the Litera Transact DMS file browser, the user double-clicks a folder.



Litera Transact sends request (including folder ID and access token) for folder items.

The returned subfolders and files are displayed to user in DMS file browser. When user clicks an item, metadata shown.

iManage returns list of subfolders and files with relevant metadata as JSON.

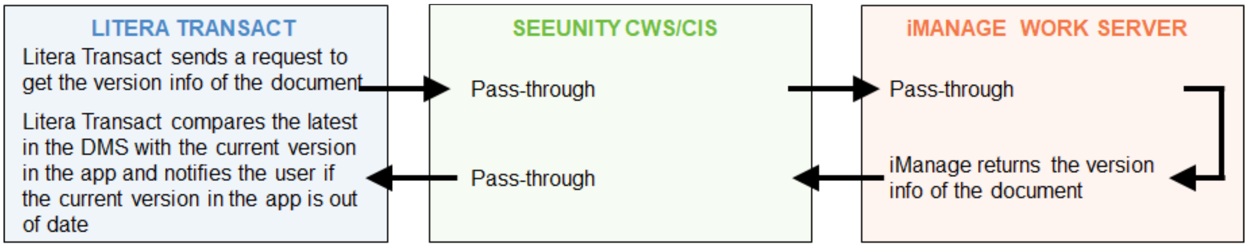
Select a document/select a version

In the Litera Transact DMS file browser, the user selects a file. The right panel shows the version dropdown with the first version selected. The metadata of the selected version is shown as well. When the user selects a different version of the file, the metadata of the selected version is shown.

Litera Transact has all the required information from the browse matter and folder actions so no API calls to iManage are required.

Check for latest version

In Litera Transact, the user selects a document and is informed if there is a later version of the document available in the DMS.



Litera Transact sends a request to get the version info of the document

Litera Transact compares the latest in the DMS with the current version in the app and notifies the user if the current version in the app is out of date

iManage returns the version info of the document

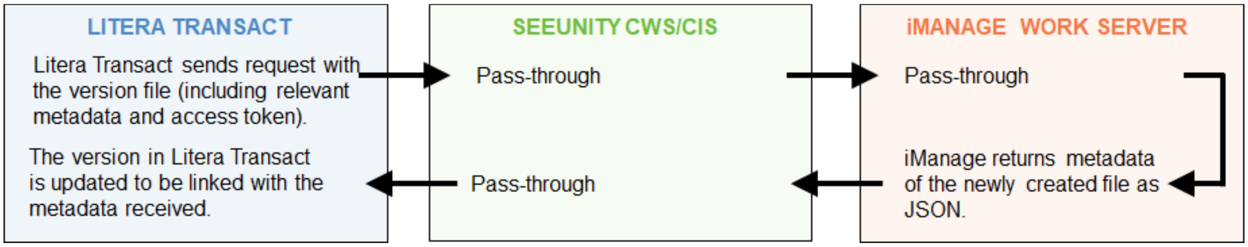
Download a version to Litera Transact

In the Litera Transact DMS file browser, the user selects a version of a file and then clicks **Save**.

No API calls to iManage are required. Litera Transact sends a request to the Litera Transact backend to store the version ID and the relevant metadata so the document in Litera Transact gets linked to the version in iManage.

Upload a version or new document to iManage

In Litera Transact, the user selects a version and clicks **Send to iManage**. The DMS file browser opens and the user selects a folder location to save the file as a new document or as a version of an existing document.



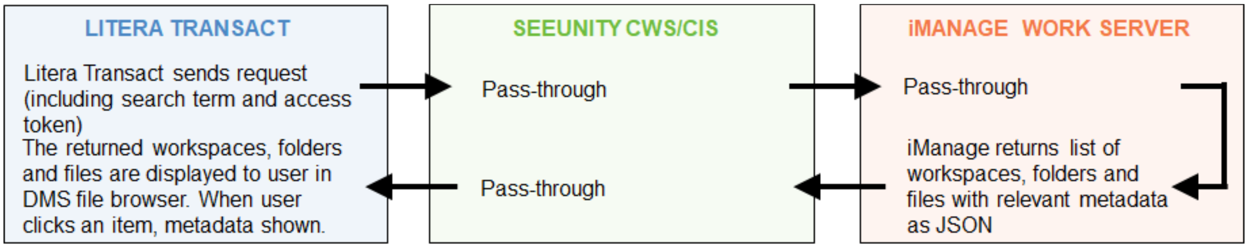
Litera Transact sends request with the version file (including relevant metadata and access token).

The version in Litera Transact is updated to be linked with the metadata received.

iManage returns metadata of the newly created file as JSON.

Search

In the Litera Transact DMS file browser, the user enters a search term and presses Enter.



Litera Transact sends request (including search term and access token)

The returned workspaces, folders and files are displayed to user in DMS file browser. When user clicks an item, metadata shown.

iManage returns list of workspaces, folders and files with relevant metadata as JSON

Caching

iManage files are cached for short periods within the Litera Transact file storage system. At the time of installation and setup, customers select the period of time that they would like their documents to be cached within Litera Transact. This helps with performance so Litera Transact doesn't have to pull the document down from iManage every time it is requested by a user (viewing, execution, closing binders, etc.).

The cache period is specified in minutes and once it expires, the document is deleted from Litera Transact. When a user tries to access the document again, it is pulled down from iManage and the cache period resets.

The only time a document is in Litera Transact indefinitely is when it is uploaded from the desktop of the user or if it was uploaded by an external collaborator. Litera Transact doesn’t currently automatically push the document to iManage, so it stays in Litera Transact until the user chooses to push it into iManage. Once it is successfully pushed, the cache period is initiated.

How data is secured by Litera Transact

Litera Transact runs in AWS (Amazon Web Services). Each customer is provisioned their own S3 bucket on AWS and that is where all of their documents are stored (encrypted at rest and in transit).

The Litera Transact servers do not have public IP addresses, and thus are not directly exposed to the internet. The servers only accept HTTPS traffic – no other in-bound traffic is allowed.

Data is encrypted in transit with TLS1.2 and higher technology and with 256 Advanced Encryption Standard (AES) encryption for any data at rest held.

Strategically separated, geographically remote data centers prevent data destruction under catastrophic scenarios and real-time replication speeds data recovery.

What does AWS offer in the way of security?

The key features of AWS security are automatically applied by default within Litera Transact allowing us to prevent, detect, and respond to breaches. In particular, AWS, encrypts data at rest, provides access restrictions at the storage account level so we can restrict access by IP and user credentials. For more information about AWS security, see the following:

- https://aws.amazon.com/security/
- https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html
- https://aws.amazon.com/security/

Penetration testing

Penetration testing on Litera Transact is owned by Litera, and carried out annually by 3rd party testing providers Pondurance.