Calyx RIM Architecture

CALYX™

Contents

Cloud - Platform Overview

Cloud enables you to use native Azure features to create a secure next generation platform.

Application Hosting

Application components are hosted on a combination of Azure IaaS, PaaS and SaaS that allows to decouple micro services to create a more flexible, agile and scalable application architecture.

Power BI

Power BI provides reporting platform that includes out-of-the-box reports. Data between and Azure SQL synchronize via automated ETL (Extract, Transform, and Load) process.

File Synchronization

Azure File Sync seamlessly synchronizes data between user file share and file share.

Availability and Disaster Recovery

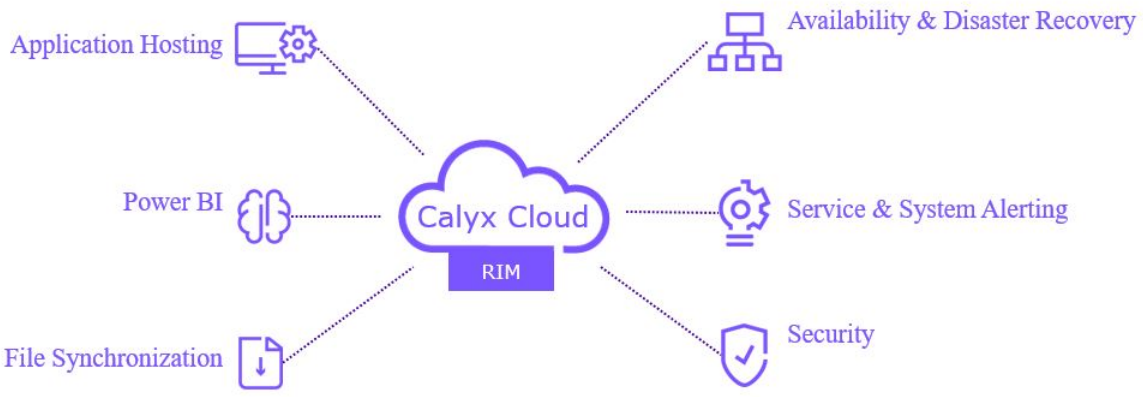
RIM uses Azure features to prevent single points of failure and automatic recovery. Data is backed up using Commvault and native Azure services with failover to secondary Azure regions.

Service and System Alerting

System alerting and monitoring is done via Azure Monitor & Oracle Enterprise Manager integrated with ServiceNow. Service management is also done via ServiceNow.

Security

N-tier architecture secured through Azure NSGs and firewalls (transport and WAF). End-to-end encryption is used throughout.



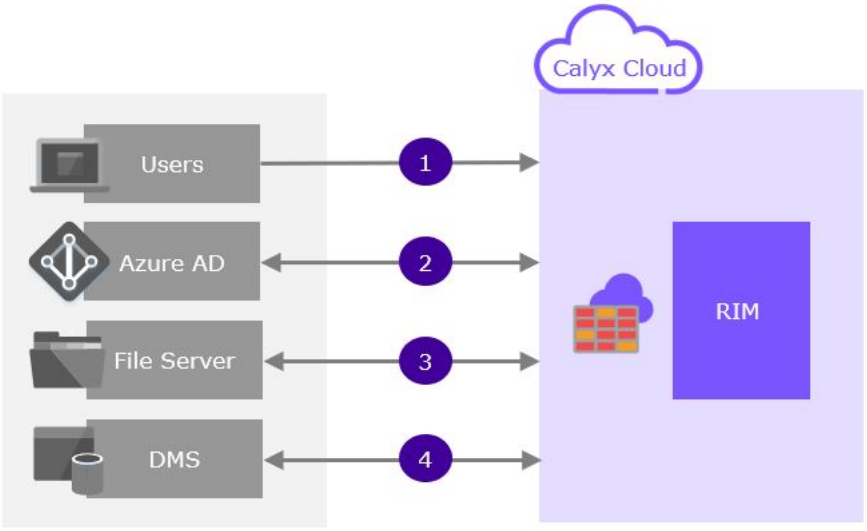
Changing Settings Post Implementation of

Changes must not be made to the settings after the implementation to prevent adverse security breaches.

Note: *Changes to the settings (such as the SCIM settings) on your environment post implementation of are prohibited to prevent adverse security vulnerabilities. To make any changes post implementation, please contact our technical support team.*

Cloud – High Level Architecture

Overview of the interaction between Cloud, users and other related components.
The following touch points exist between a user and .



Users

Users connect to 7.1 using https via the internet.

Azure Active Directory

Azure Active Directory integration is performed using https via the internet. Other identity providers can be federated with .

File Server

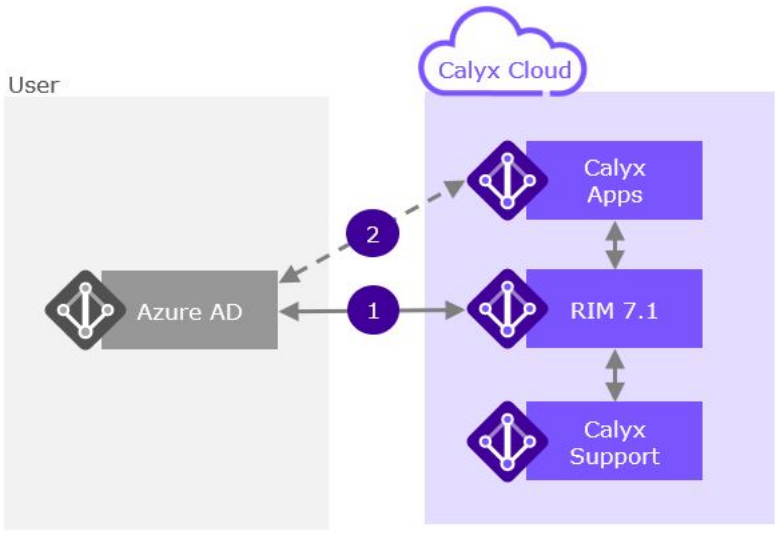
Document syncing is automated by Azure file sync using https via the internet.

DMS

Data between user DMS and is transferred via a secure connector.

Cloud - Azure Active Directory

authentication interactions are with one or more Azure Active Directories (AAD)
Use your own Azure Active Directory to authenticate. If you prefer to use an IDP alternative such as Ping or Okta, it will be via Direct Federation to an AAD registered with .



1. Azure Active Directory

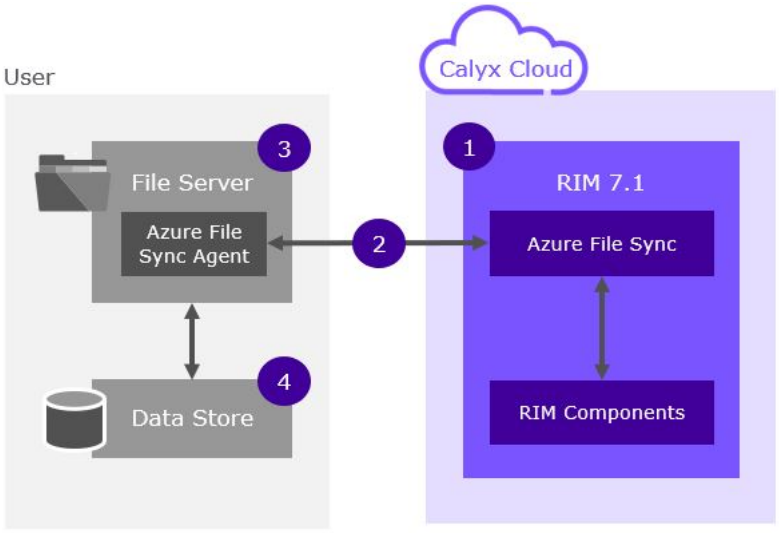
2. Direct Federation

— The recommended identity provider integration is though user Azure AD registration and SCIM identity provisioning.
— The SCIM service enables authentication via multiple instances of Azure AD that are user or managed.

Optional direct federation for B2B guests.

File Synchronization Overview

Synchronization of files between , Azure and data stores
The following process shows the file synchronization between , Azure server and the data server.



1. Storage

2. Azure File Sync

3. User File Server

4. User Data Stores

storage is protected by network security services in addition to Azure Defender and Azure Advanced Threat Prevention.

— Data is synced bi-directionally between and the user file server.
— Can be synced to multiple customer file servers.

— A user requires a Windows file server where the Azure File Sync Agent can be installed.
— All communications to are outbound from the agent via https (port 443).
— Agent can be placed behind a user proxy server.

— If data is stored on a non-Windows file server, the data should be directly attached to a Windows file server.

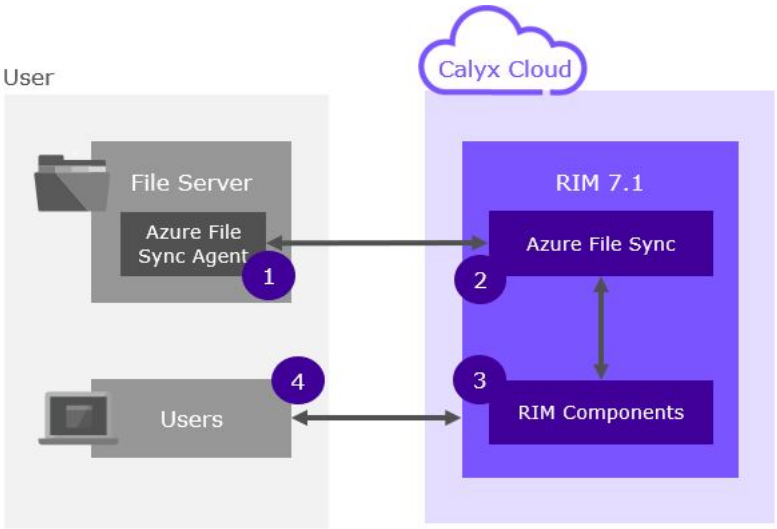
The following provides further details for file sychronization.

— All communications are HTTPS, Port 443 FileREST Protocol.
— Although files are synced both ways all connections are initiated outbound from the Customer File Sync Server to the Azure File Sync Services. No inbound ports need to be opened in the Customer environment.
— File share can only be accessed with a SAS Token. This is created when the File Sync server is set up.
— File share is protected by a storage firewall that is configured to only allow customer IP addresses to access the endpoint.
— All servers are protected with Anti-Virus/Anti-Malware software.
— All servers are monitored by our Security Operations Centre (SOC).
— All storage accounts are protected with Microsoft Defender.

— Files within the application are modified and updated by customer publishing end users via the application, there is no other external access.
— Approximately 90% of files that are sent back are PDF.
— Any files that need to be synced with will need to be copied to a folder on the customer File Sync Server.
— End users will continue to access via a URL over the internet, there is no impact on their interaction with .
— 3rd Party pen testing has been completed as part of the product release.

File Synchronization Process

File synchronization happens when changes are made to the files.



1.User to Synchronization

2. to User Synchronization

3. File Access

4. Users

— Azure File Sync Agent uses Windows USN journaling to automatically initiate a synchronization session when changes are detected.
— Time to synchronize files with Cloud depends on the internet bandwidth.

— Azure File Sync Agents within the same sync group make file changes known to other agents in the sync group (typically within seconds).
— Time to synchronize files with Cloud depends on the internet bandwidth.

— The system can access files as soon as they are synced to the Cloud

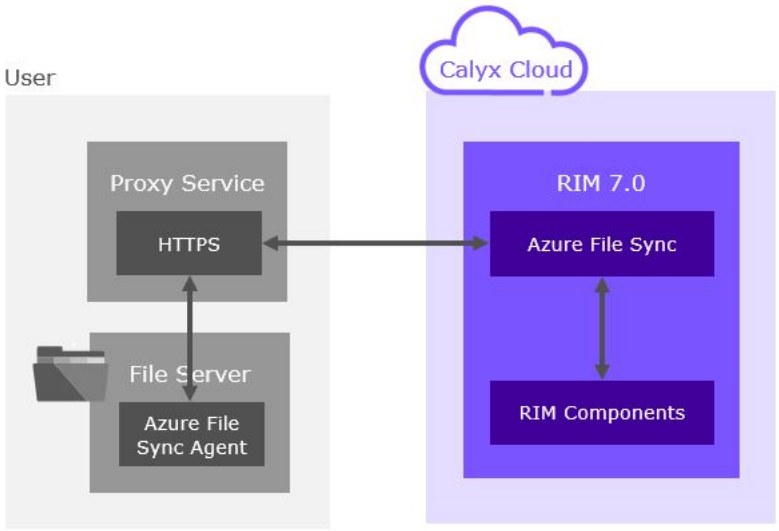
— users can access files in as soon as they are synced to the Cloud

File Synchronization Availability

Client file servers must be configured by the user for file synchronization.
Microsoft supports several common file server configurations with Azure File Sync such as:

— Windows File Server Clustering
— Windows Distributed File System
— Microsoft File Server Disaster Recovery Configuration

The common configuration provides involve multiple Azure File Sync Agents deployed within the same sync group as shown in the example below.



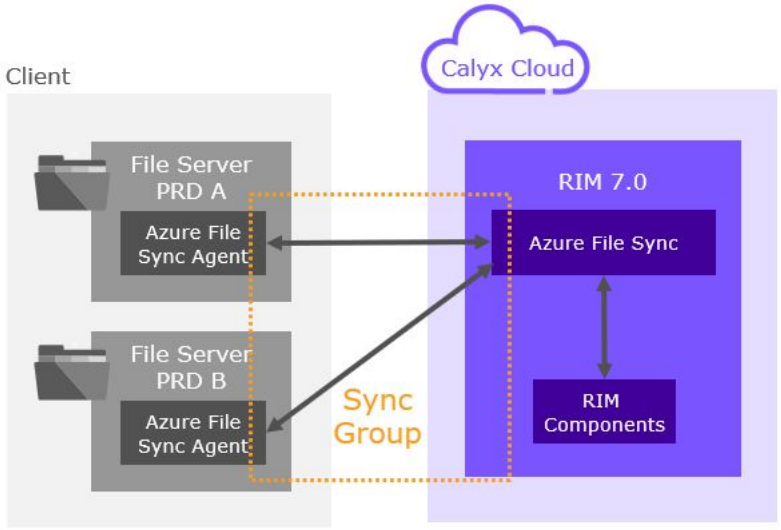
File Synchronization Web Proxy

Azure File Sync enables you to connect your on-premises servers to Azure files.

Proxy Support

The Azure File Sync agent supports the use of a web proxy (or firewall) as part of a standard deployment.

For Microsoft proxy server support, see Azure File Sync proxy and firewall settings



Install Azure File Sync Agent

Organize your files in Azure Files using Azure File Sync agent.

Prerequisites

The following are the pre-requisites for installing Azure File Sync agent:

- The agent installation package must be installed with administrator permissions.
- The agent is not supported on Nano Server deployment option.
- The agent is supported only on Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2.
- The agent requires at least 2 GiB of memory. If the server is running in a virtual machine with dynamic memory enabled, the VM should be configured with a minimum 2048 MiB of memory. See Recommended System Resources for more information.
- The Storage Sync Agent (FileSyncSvc) service does not support server endpoints located on a volume that has the system volume information (SVI) directory compressed.

To install Azure File Sync Agent:

1. Disable IE Security Configuration to avoid web-related connection issues.
2. Download the `StorageSyncAgent_%SERVER_VERSION%.msi` file from the Microsoft web site.
3. Once the download is complete, launch the Setup wizard and accept the defaults.
4. Once the installer wizard finishes, the next installer will register the server to the Azure file Sync service establishing a trust relationship between your server and the Storage Sync Service.
5. After the installation is complete, the agent looks for an update or new release. Proceed by clicking OK.
6. Sign on to the Azure tenant to perform the registration with the Azure File Sync service.
7. Select Azure Public Cloud as the Azure Environment.

You are prompted for tenant credentials

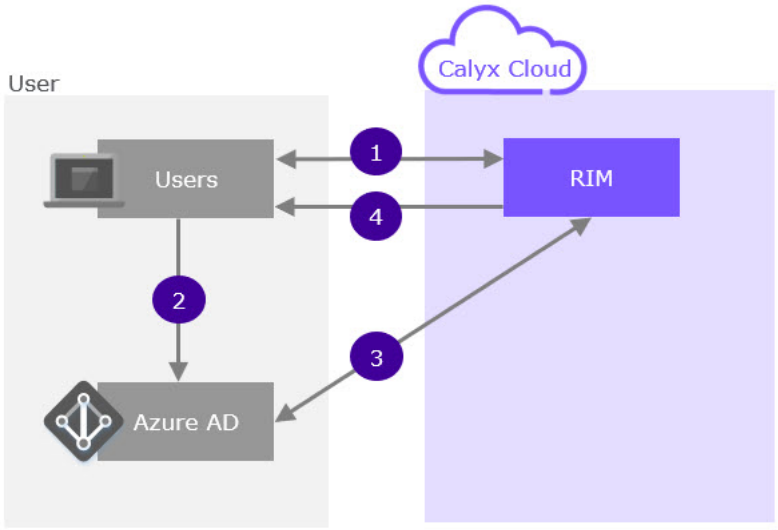
8. The tenant credentials are entered by via screen share
9. Enter username and password ensuring you use an account with global administrator permissions.
10. Enter the storage sync service details such as your Azure subscription, the resource group (Resource group of the Azure File Sync service on) to create the storage sync service, and the storage sync service name.

    Resource Group Name, Azure Sync Service Name, User Name and Password provided by .
11. Click Register.

    The registration is complete.

Single Sign-On Process Flow

Secure authentication of multiple applications using a single set of credentials
The following is the SSO process applications.



1. User connects to

2. User logs in via Azure AD

3. Azure AD & exchange info

4. User is authorised

— User tries to access .
— redirects user to Microsoft login page.

— User enters credentials.

— AAD validates and sends auth code to .
— exchanges auth code for ID token.

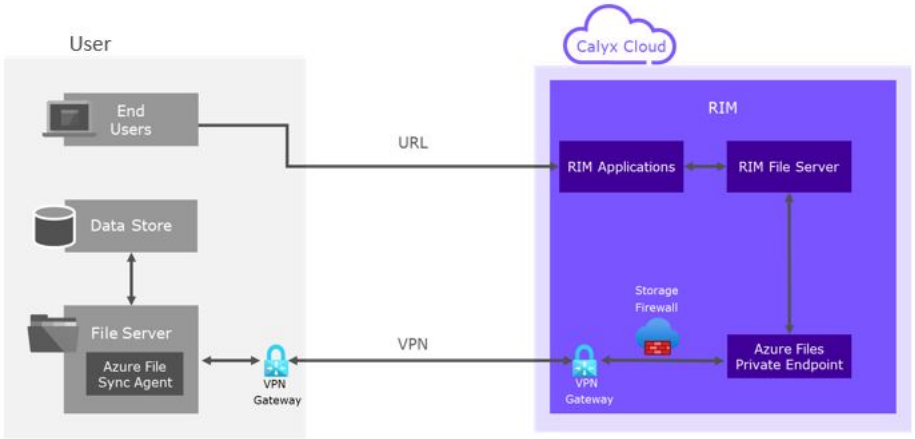
— AAD sends ID token to .

— validates the ID token and checks if a valid user exists in mapped to Azure user and displays user.

File Synchronization with VPN

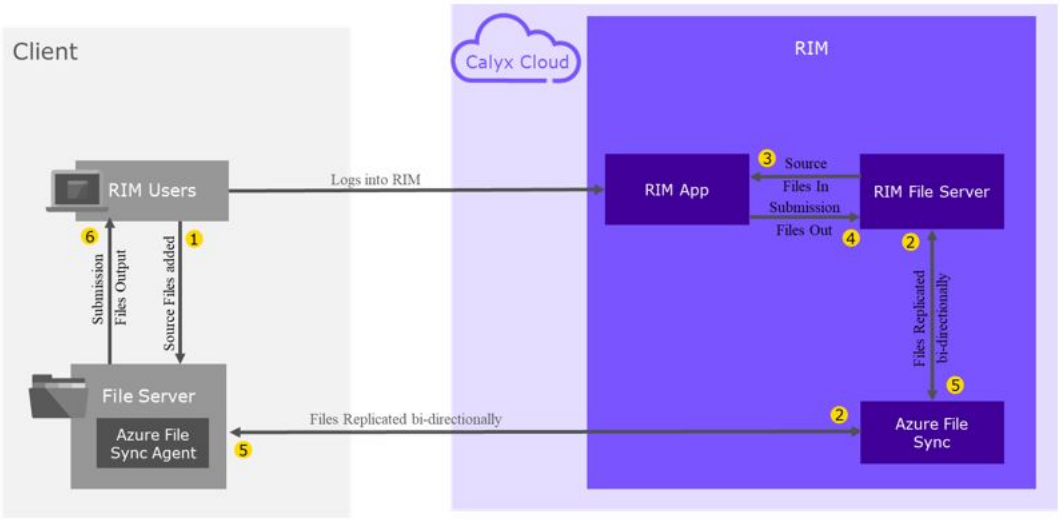
VPN connection provides secure file synchronization.
File Synchronization with VPN.

— Link between Customer and will be via a Site-to-Site VPN
— All communications are HTTPS (port 443).
— Although files are synced both ways all connections are initiated outbound from the Customer File Sync Server to the Azure File Sync Services. No inbound ports need to be opened in the Customer environment.
— File share can only be accessed with a SAS Token. This is created when the File Sync server is set up.
— File share is protected by a storage firewall that is configured to block internet access, therefore disabling access to the storage public endpoint.
— File Share will only be accessible via a private endpoint and so is only accessible externally via the VPN.
— All servers are protected with Anti-Virus/Anti-Malware software.
— All servers are monitored by our Security Operations Centre (SOC).
— All storage accounts are protected with Microsoft Defender.
— Files within the application are modified and updated by Customer publishing end users via the application, there is no other external access.
— Approximately 90% of files that are sent back are PDF.
— Any files that need to be synced with will need to be copied to a folder on the customer File Sync Server.
— End users will continue to access via a URL over the internet, there is no impact on their interaction with .



Files Flow

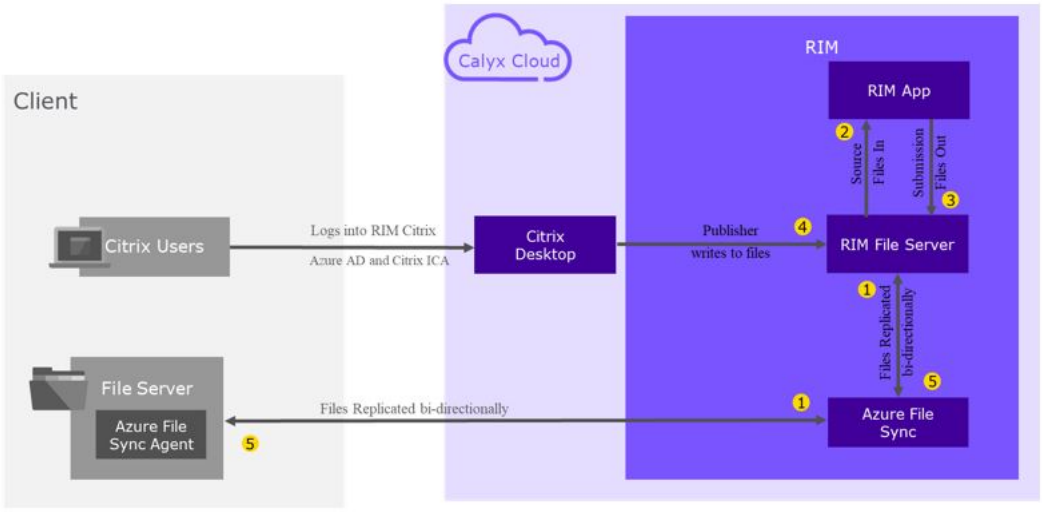
The flow of files between client server and .
The following diagram shows the flow of files.



1. User uploads file to their file server.
2. Source file is synced between client file server and file server using Azure File Sync.
3. Source files are loaded from File Server into the Application.
4. Submission files are sent from application to File Server.
5. Submission file is synced between file server and client file server via Azure File Sync.
6. User copies submission files from client file server.

Citrix Files Flow

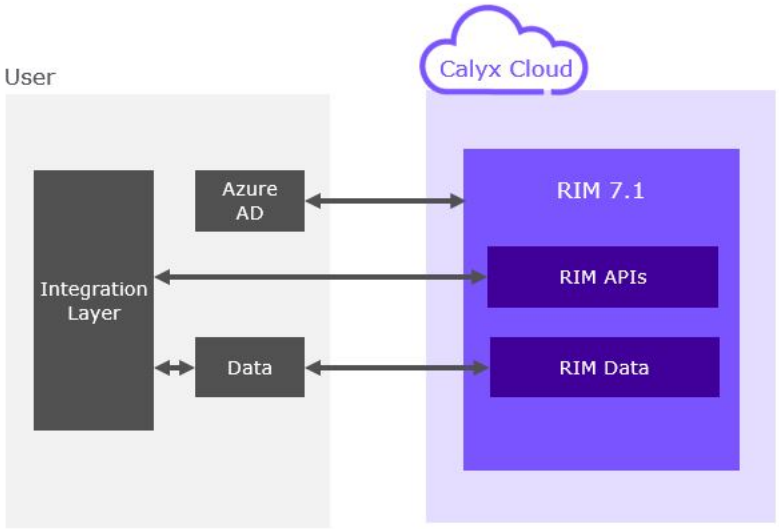
The Citrix flow of files between client server and .
The following diagram shows the flow of files in a Citrix environment.



1. Source file is synced between client file server and file server using Azure File Sync.
2. Source files are loaded from File Server into the Application.
3. Submission files are sent from application to File Server.
4. Citrix user modifies the submissions file.
5. Submission file is synced between file server and client file server via Azure File Sync

Integrations

Integration of APIs and Data
Overview of APIs and Data integration



APIs

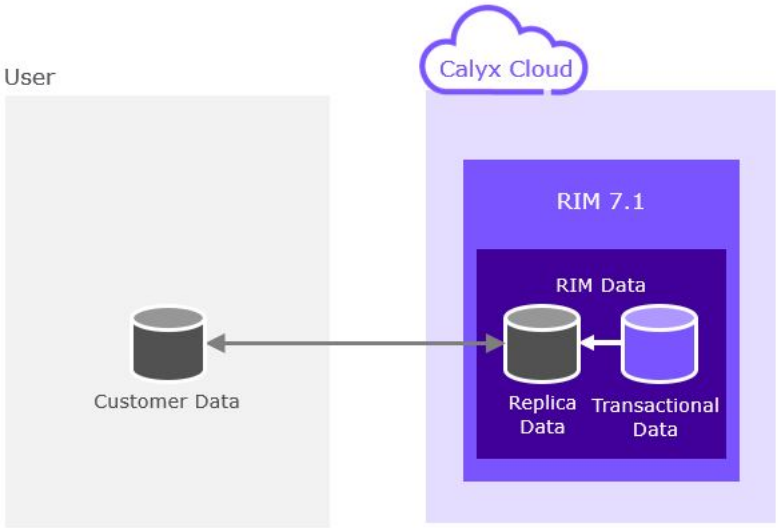
APIs allow customers to build integrations directly into their own integration layer.

Data

— Data can be shared between and customers through various methods.
— DMS data is transferred via secure purpose-built connectors.
— File server data is transferred securely via Azure File Sync.
— data can be made available through our Data as a Service offering.

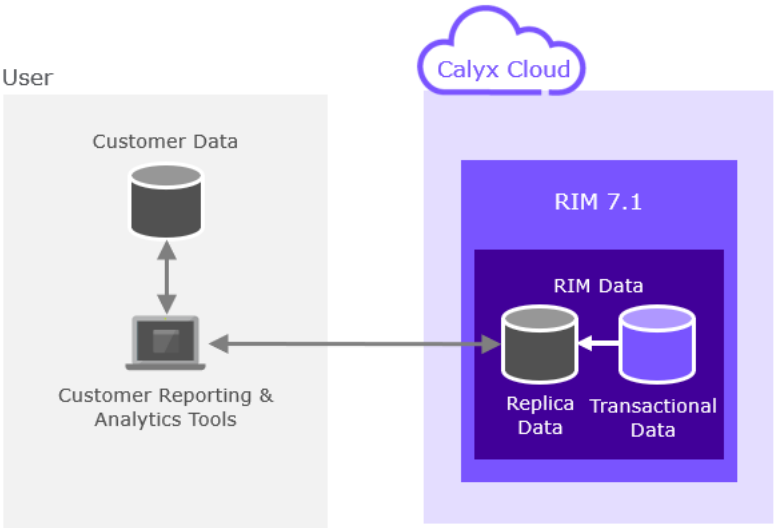
DaaS

The Data as a service (DaaS) is used to access and interact with data.
The following options provide you the choice to select the set up that suits your environment.



Option 1

— The standard Data as a Service offering provides a replica database that you can interact with.
— Site-to-site VPN recommended to secure data access/transfer
— This solution allows to control the interactions with the transactional database in order to appropriately manage performance and security of the solution
— Users have a number of options available to them to copy the data from the replica database to their own data stores (For example, through ETLs or through data replication)



Option 2

— The standard Data as a Service offering provides a replica database that you can interact with.
— Site-to-site VPN recommended to secure data access/transfer.
— This solution allows to control the interactions with the transactional database in order to appropriately manage performance and security of the solution.
— Customer can use their own reporting and analytics tools to interact with the replica database.

Security and Connectivity

Microsoft Azure secures the data transferred and the connections between and users.

Cloud Native Security Services

— Services including, but not limited to, Azure Firewall and Azure Application Gateway WAF are used to secure the perimeter of the Cloud.
— Security in depth is used on our virtual networks throughout the solution using services such as Azure Network Security Groups and Azure Application Security Groups.

Cloud Connectivity

Users can connect to in several ways to meet different requirements.

— Internet – Secure TLS (1.2) access directly over the Internet.
— VPN – For an added layer of security site-to-site VPNs can be used.

Typical Connections to Calyx RIM

A standard RIM deployment requires the following access:

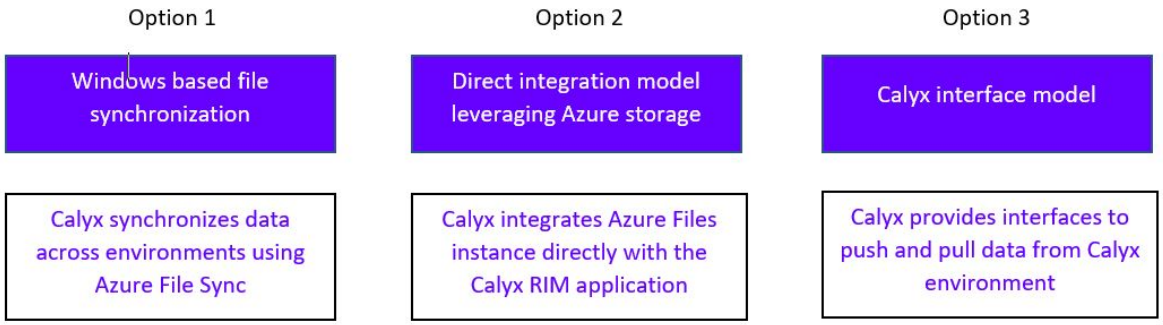
Service	Connection Type	Direction
RIM Application	HTTPS (443)	Customer > Calyx
Calyx Citrix	HTTPS (443)	Customer > Calyx
Azure AD	HTTPS (443)	Customer <> Calyx
Office 365	HTTPS (443)	Calyx > Customer
File Server Sync	HTTPS (443)	Customer > Calyx
DMS	<Differs Per DMS>	Calyx > Customer

File Integration Options

Different file integration options provide additional flexibility and deliver maximum performance.

As data is separated between our environments and data volumes are large, each option has different trade-offs. Choose the option that suits your business needs and make informed decisions. The different options are:

— Windows based file synchronization
— Direct integration model leveraging Azure storage
— interface model



Windows based file synchronization

— Data is synchronized as soon as your users make a change.
— Data is local to your application so performance of the solution is maximized.
— Data can be synchronized with multiple shares within your environment.
— To achieve a performant synchronization for your data volumes data must be hosted locally to a Windows server.

Direct integration model leveraging Azure storage

— Data remains within your environment.
— With Azure Files you can achieve a low latency direct integration model not possible with other methods. This provides high performance experience similar to your on-premise model.

interface model

— provides standard Azure interfaces for your systems to synchronize data to the environment.
— You can use the tools you use to synchronize data for your users from anywhere within your environment.

For more information about Azure File Sync planning and deployment, see Planning for an Azure File Sync deployment and Deploy Azure File Sync

User Migration

Users and User Groups must be created in Azure Active Directory to use on Cloud.
To add users and groups you must be a User administrator or Global administrator. For steps on how to create users and groups, see Add Users in Azure Active Directory.

Once users and groups are created, find the User Object Ids for migration. For instructions on how to find the Object Ids, see Find Tenant ID, Object ID, and partner association details.

Configure AAD Authentication - Register an Application

Applications must be registered to access them on Azure.

To register an application:

1. Sign in to the Azure Portal using an account with administrator permissions
2. Select Azure Active Directory > App registrations
3. Click New Application Registration
4. In the *Register an application* page, enter the details for the application.

Option	Description
Name	The name that is displayed when the application is used.
Who can use this application or access this API?	Select Accounts in any organizational directory (Any Azure AD Directory - Multitenant)
Redirect URL (Optional)	Enter the Public DNS provided by .

5. Click Register
   The initial application registration is complete.
6. Select Authentication
7. Add the reply URL: `https://<PublicDNS>/insight/openId/doEsignature`

`PublicDNS` is provided by .

Configure AAD Authentication - Generate Secret Key

An application secret key is used in place of a certificate to identify itself.

To generate a secret key:

1. In the Azure portal, in App registrations, select your application.
2. Select Certificates & secrets > Client secrets > New client secret
3. Add a description for your secret key.
4. For secret key expiration, enter `12 months`.
5. Click Save.
   The Client Secret Key is generated and will be a part of the authentication credential.

Configure AAD Authentication - Grant Admin Consent

Administrators can provide their consent for the specific permissions requested for the application data and capabilities.

Prerequisites

The following users with Azure AD account can provide can grant admin consent.

— Global Administrator or Privileged Role Administrator - to grant consent for applications requesting any permission for any API.
— Cloud Application Administrator or Application Administrator - to granting consent for applications requesting any permission for any API except Azure AD Graph or Microsoft Graph app roles (application permissions).
— A user with custom directory role - to grant required permissions to applications.

To grant admin consent:

1. Sign in to the Azure portal with required role listed in the prerequisites section.
2. Select Azure Active Directory > Application Registrations.
3. Select the application to which you want to grant admin consent.
4. Select API permissions.
5. Review the permissions the application requires and then click Grant admin consent.

Configure AAD Authentication - Configure Group Claim

Application registration in Azure AD are configured to include group claims in tokens.

To configure group claim:

1. Sign in to the Azure portal.
2. Select Azure Active Directory > Application Registrations > Selet Application > Manifest.
3. To enable group membership claims, select SecurityGroup for groupMembershipClaim.
4. Click Save.

SCIM Endpoint Provisioning - Create an Enterprise Application

You must create an application in Azure before you can use it.

Note: *To prevent security vulnerabilities, the following procedure must be used for configuration during initial implementation only. For changes post implementation, contact our technical support team.*

To create an Enterprise Application:

1. Sign in to the Azure Active Directory Admin Center.
2. In the menu on the left, click Enterprise applications.
3. Enter a name for the application.
4. Select Add to create an app object.
5. In the menu on the left, click Provisioning.
6. Select Automatic and enter details for the following options:

Option	Description
Tenant URL	SCIM micro-service URL. This is provided by .
Secret Token	SCIM token applied to the SCIM micro-service. This is entered by via shared screen.

7. To check AAD connection to SCIM endpoint, click Test Connection.
8. Click Save.
9. Under Provisioning, click Mappings > Provision Azure Active Directory Users .
10. Under Attribute Mapping, click mailNickName attribute.
11. Select the nick name from the Target attributes drop-down list and click Ok.
12. Under Attribute Mapping, click Add New Mapping.
13. Select objectId for Source attribute and externalId for Target attribute and click Ok.
14. Click Save > Yes.
15. Select the Provisioning tab, select Settings.
16. Switch Provisioning Status to On.
17. Click Save.

SCIM Endpoint Provisioning - Configure Provisioning Error Notifications

Configure to receive an e-mail notification when an error occurs in your application.

Note: *To prevent security vulnerabilities, the following procedure must be used for configuration during initial implementation only. For changes post implementation, contact our technical support team.*

To configure provisioning error notifications:

1. Sign in to the Azure Active Directory portal.
2. Select Enterprise Applications and select your application.
3. Select Provisioning.
4. Click Edit provisioning for your application name.
5. Under Settings, enter the e-mail address of the user or the group who should get the provisioning error notification.
6. Select Send an email notification when a failure occurs.
7. On the *Provisioning* window, select Scope from the drop-down and select Sync only assigned users and groups.
8. Click Save.

SCIM Endpoint Provisioning - Add Users and Groups to Provisioning Scope

User and groups can connect to user management API endpoints.

Note: *To prevent security vulnerabilities, the following procedure must be used for configuration during initial implementation only. For changes post implementation, contact our technical support team.*

To add users and groups to provisioning scope:

1. Sign in to the Azure Active Directory portal.
2. Select Enterprise Applications and select your application.
3. Under Manage, click Users and Groups.
4. On the *Users and groups* page for your application, click Add user/group.
5. On the *Users and groups* page, click Users and group.
6. Select all the necessary users and groups.
7. Click Select > Assign.

SCIM Endpoint Provisioning - Provision on Demand

On-demand provisioning validates and verifies the changes made to the configuration for Azure AD connection.

Note: *To prevent security vulnerabilities, the following procedure must be used for configuration during initial implementation only. For changes post implementation, contact our technical support team.*

To enable Provision on demand:

1. Sign in to the Azure Active Directory portal.
2. Select Enterprise Applications and select your application and go to the provisioning configuration page.
3. Configure provisioning by entering your admin credentials.
4. Click Provision on demand.
5. Search for a user by first name, last name, display name, user principal name, or email address.
6. Click Provision.

Index