Technical Requirements for Alma and Discovery Implementation

Ex Libris Alma is a pure cloud-based Software-as-a-Service (SaaS). Its architecture is based on leading cloud technologies, offering a secure, scalable SaaS. As a SaaS solution, Alma is accessible over the Web, requiring only a Web browser for the user. The move to a cloud-based SaaS offers great benefits and cost savings, together with faster response time to user requests. This document describes Alma cloud fundamentals, the technology driving the Alma cloud, the IT side of the Alma cloud infrastructure, and the Alma cloud's interaction with on premises institutional/campus systems.

The Alma Cloud Deployment Model

Ex Libris operates its cloud infrastructure as a private cloud, which is solely available for use by its customer community. This deployment model differs from a public cloud, which is available to the general public, or a hybrid cloud, which is a combination of two or more clouds.

Private cloud implementation provides Ex Libris with the opportunity to benefit from cloud computing without compromising on the architectural control required to ensure integrity of its customers' data, systems, and processes.

Note

This document goes hand-in-hand with *Getting Ready for Alma and Discovery Implementation*.

FedRAMP customers: the FedRAMP IP ranges are not listed in the IP range section, but the information in the rest of the document is still applicable.

Making the Cloud Vision a Reality

True Multi-Tenancy

The Alma system is based on multi-tenant architecture, in which the resources – both the software and the underlying infrastructure – are shared, in order to support all customers ("tenants").

Strict data isolation is applied to all layers of the Alma application: user-interface branding isolation, database isolation (via Oracle Virtual Private Database), storage isolation, and FTP-level isolation, etc.

Ex Libris' resources are focused on maintaining a single, current version of the application, rather than attempting to support multiple software versions for clients. As a result, no client is left behind when the software is updated with new features and innovations. Moreover, this delivery model enables Ex Libris to provide its customers with a fault-tolerant computing environment that includes dynamic resource allocation.

Vendor-Managed Updates

Because Alma is designed in accordance with the SaaS model, and deployed as a cloud-based service, it is Ex Libris' full responsibility to handle the software updates and upgrades. Ex Libris is committed to ensuring that its customers always have access to the latest features and incurs all the costs of maintaining and upgrading the required software. This enables

all customers to fully take advantage of the latest Alma features and innovation.

Monthly releases and software updates are performed automatically by Ex Libris seamlessly, without any customer intervention.

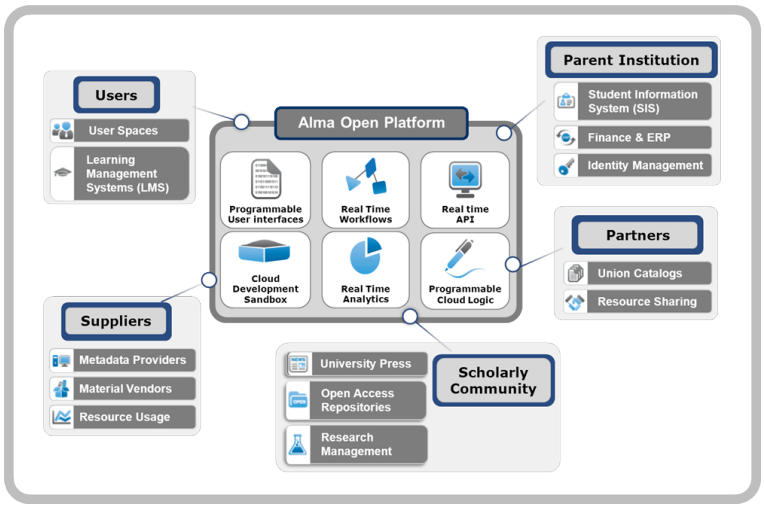
Seamless Integration/Open Platform

Alma embodies Ex Libris' Open Platform philosophy. This enables openness and interoperability between Alma and the other institutional/campus systems.

The Open Platform means open interfaces. It contains Web services, Web adapters, Application Programming Interfaces (APIs), plug-in interfaces, and more.

The Open Platform allows customers to share customer-written code so that one customer can benefit from the developments of another customer, leveraging the investments made by others for the benefit of everyone.

The following illustration demonstrates the various options for utilizing the Alma Open Platform to integrate with on premises systems that are part of the institution and library landscape.



Alma Open Platform

Security

Cloud security and confidentiality are top concerns with cloud computing and SaaS architecture. Committed to providing its customers with the most secure and reliable environment, Ex Libris has developed a multi-tiered security model that covers all aspects of cloud-based Ex Libris systems. The security model and controls are based on renowned international protocols and standards and industry best practices, such as ISO/IEC 27001:2013 and ISO/IEC 27018:2014, the standards for an information security management system (ISMS).

Performance and Service Availability

Ex Libris is aware of the fact that the performance of its cloud applications can have a significant impact on customer adoption and satisfaction. Ex Libris' cloud data centers leverage their infrastructure-renowned technologies and applications in order to meet the performance service-level agreements (SLAs) to which the Ex Libris is committed.

Moreover, Ex Libris employs a dedicated cloud services team, which is responsible for monitoring the applications and

platform performance and issuing periodic SLA reports.

Network Communication

As a library management solution, Alma must communicate with different on premises library systems. This section describes the different on premises systems with which Alma may need to communicate and the communication methods used. Ex Libris ensures that all network communication is done using the appropriate security measures. Therefore, Ex Libris uses up-to-date protocols and standards such as HTTPS and TLS 1.2 (see TLS Support). TLS is an updated and more secure version of SSL. TLS refers to the TLS 1.2 protocol.

Browser Communication

As a true cloud solution, Alma requires only a browser. Alma supports all the leading browsers: Chrome, Firefox, and Edge. There is an ongoing process of monitoring new browser versions and certifying their compatibility with Alma. Full browser certification details for Alma can be found here. Browser support information for Primo can be found here, and for Summon here.

Browser to Alma communication is conducted using TLS, over ports 443. The URLs (domains) to be used are provided to you by your Ex Libris project manager.

Note

To maintain a consistent level of security and user experience, the use of proxy servers to monitor and control traffic to and from the Alma and Discovery platform will impact the support level and user experience we are able to provide and, as a result, is not supported.

Network Communication

To function properly and completely, Alma must communicate with different on premises installed systems, such as financial systems, student information systems (SIS), self-check (SIP) machines, and other third-party systems.

The sections below describe the different components that Alma may communicate with outside of its cloud network. There is a table listing the different network communications used, as well as a network diagram illustrating the communication, protocol, and direction (in/out). Not all listed communications are necessarily relevant for each institution.

Note

Ex Libris MFT (Managed File Transfer) provides secure and reliable file transfer infrastructure to support the different Ex Libris products (See Ex Libris MFT). Alma also supports secure FTP (SFTP – over SSH, but not FTPS over TLS) using port 22 or standard FTP using port 21.

Higher-Ed Platform IP Range

Some on premises systems with which Higher-Ed products integrate (for example, ERP, SIS, SFTP, SIP machines) may require these Ex Libris regional IP/s in order to communicate with Alma.

The following IP ranges must be allowed access to/from your institution. (Note that the IP ranges below are in CIDR

notation, first/last IP address included.)

- In the U.S.A. (refers to the NA01, NA02, NA03, and NA04 instances on the Chicago data centers and the NA05, NA06, NA07 and NA08 instances on the Seattle data centers):
  - 66.151.7.40/29 [66.151.7.40-47]
  - 66.151.7.128/26 [66.151.7.128-191]
  - 66.151.7.192/28 [66.151.7.192-207] - Note that 66.151.7.202 is to enable calls from the Community Zone.
  - 66.151.7.224/30 [66.151.7.224-227]
  - 66.151.7.236
  - 66.151.14.128
  - 66.151.14.129
  - 74.217.12.128/27 [74.217.12.128--159]
  - 64.74.237.221
  - 64.74.237.229
  - 64.74.237.232/31 [64.74.237.232-233]
  - 216.147.208.128/26 [216.147.208.128-191]
  - 216.147.209.0/27 [216.147.209.0-31]
  - 216.147.212.20/30 [216.147.212.20-23]
  - 216.147.212.25
  - 216.147.212.64/26 [216.147.212.64-127]
  - 216.147.212.128/27 [216.147.212.128-159]
  - 216.147.212.21
  - 216.147.212.30
  - 64.74.237.220
- In Canada (refers to the Ex Libris Canadian data center):
  - 216.147.222.64/29 [216.147.222.64-71]
  - 216.147.222.128/29 [216.147.222.128-135]
  - 216.147.222.124/30 [216.147.222.124-127]
  - 216.147.222.188/30 [216.147.222.188-191]
  - 216.147.222.30
- In Europe (refers to the EU00, EU01, and EU02 instances on the Amsterdam data centers and the EU03, EU04, EU05, and EU06 instances on the Munich data centers):
  - 95.172.90.160/27 [95.172.90.160-191]
  - 31.186.254.128/28 [31.186.254.128-143]
  - 216.147.214.128/26 [216.147.214.128-191]
  - 216.147.218.128/26 [216.147.218.128-191]
  - 216.147.218.64/26 [216.147.218.64-127]
  - 216.147.215.0/27 [216.147.215.0-31]
  - 95.172.88.57

- 216.147.218.253

- In APAC (refers to the AP01 instance on the Singapore data center and the AP02 instance on the Sydney data center):
  - 117.20.42.16/31 [117.20.42.16-17]
  - 117.20.42.32/27 [117.20.42.32-63]
  - 117.20.42.137
  - 216.147.220.128/29 [216.147.220.128-135]
  - 216.147.220.64/28 [216.147.220.64-79]
  - 216.147.221.64/28 [216.147.221.64-79]
  - 216.147.221.96/28 [216.147.221.97-110]
  - 216.147.221.192/28 [216.147.221.192-206]
  - 117.20.42.12
  - 216.147.221.253
- In China (refers to the Ex Libris Beijing data center):
  - 124.251.9.0/26 [124.251.9.0-63]
  - 124.251.9.15

Note

Access to the above IP ranges may require firewall settings at the institution level and inclusion in the institution's SPF DNS record (in order to avoid Alma emails potentially being handled as spam).

Primo Classic IP Range

The following IP ranges must be allowed access to/from your institution. (Note that the IP ranges below are in CIDR notation, first/last IP address included.)

- In the U.S.A.:
  - 64.74.237.229 (MT NA01 and TC NA)
  - 66.151.7.8 (MT NA02)
  - 66.151.7.11 (MT NA03)
  - 66.151.7.55 (MT NA04)
  - 66.151.7.235 (MT NA05)
  - 64.74.237.218 (MT NA sandbox)
  - 216.147.208.160/27 [216.147.208.160-191]
  - 216.147.209.32/27 [216.147.209.32-63]
  - 216.147.212.20/30 [216.147.212.20-23] (SMTP Mail Gateway)
  - 216.147.212.25 (S/FTP)
  - 216.147.212.128/27 [216.147.212.128-159] (MT NA05 and TC NA sandbox)
  - 66.151.7.63 – proxy-na.hosted.exlibrisgroup.com
  - 64.74.237.200 – primo-instant-na.hosted.exlibrisgroup.com

- In Canada:
  - 216.147.222.112 (MT CA01)
  - 216.147.222.177 (MT CA01 sandbox)
  - 216.147.222.177 (CA01 implementation)
- In Europe:
  - 31.186.254.144 (MT EU01)
  - 31.186.254.179 (MT EU02)
  - 31.186.254.228 (MT EU03)
  - 31.186.254.96 (MT EU04)
  - 31.186.254.152 (TC EU)
  - 95.172.90.146 (MT EU sandbox)
  - 216.147.218.96/27 [216.147.218.96-127]
  - 31.186.254.83 – proxy-eu.hosted.exlibrisgroup.com
  - 95.172.90.153 – primo-instant-eu.hosted.exlibrisgroup.com
- In APAC:
  - 117.20.42.20 (MT APAC)
  - 117.20.42.129 (MT APAC03)
  - 117.20.42.134 (TC APAC)
  - 117.20.42.134 (TC APAC02)
  - 117.20.42.162 (MT APAC sandbox)
  - 216.147.221.96/28 [216.147.221.96-111]
  - 117.20.42.224 – proxy-ap.hosted.exlibrisgroup.com
  - 117.20.42.136 – primo-instant-apac.hosted.exlibrisgroup.com
- In China:
  - 124.251.9.21
  - 124.251.9.33 (sandbox)
  - 124.251.9.34 (implementation)

Primo VE IP Range

Primo VE uses the same IP ranges as the Higher-Ed Platform. For details, see Higher-Ed Platform IP Range.

In addition, the following IP ranges must be allowed access to/from your institution:

- In the U.S.A.:
  - 66.151.7.63 – proxy-na.hosted.exlibrisgroup.com
  - 64.74.237.200 – primo-instant-na.hosted.exlibrisgroup.com
- In Europe:
  - 31.186.254.83 – proxy-eu.hosted.exlibrisgroup.com
  - 95.172.90.153 – primo-instant-eu.hosted.exlibrisgroup.com
- In APAC:

- 117.20.42.224 – proxy-ap.hosted.exlibrisgroup.com
- 117.20.42.136 – primo-instant-apac.hosted.exlibrisgroup.com

Library Open Workflow

To use Library Open Workflows, the following IP addresses must be allowed access to/from your institution:

- In North America:
  - 64.74.237.30 – na-workflows.hosted.exlibrisgroup.com
- In Europe:
  - 95.172.90.30 – eu-workflows.hosted.exlibrisgroup.com
- In APAC:
  - 216.147.220.208 – ap-workflows.hosted.exlibrisgroup.com

Summon IP Range

There are no special IP requirements for communicating with Summon; Summon's IP requirements are covered by the Higher-Ed Platform. See Higher-Ed Platform IP Range.

Bandwidth Requirements

Number of Alma Named Users	Required Minimum Network Bandwidth
Up to 50	0.025 MB per user
Above 50	0.015 MB per user
Above 200	0.01 MB per user

For example:

- 10 Alma named users = 0.25 MB
- 500 Alma named users = 5 MB

Alma-Primo

Note

This section is not relevant to Primo VE, which is deployed on the Higher-Ed platform.

Ex Libris Primo customers that are also Alma users work with Primo in the Ex Libris cloud and thus benefit from a complete cloud environment and smooth updates of both solutions. Alma and Primo communicate within the Ex Libris cloud network and the only external communication is between patrons and Primo functions over port 80 or 443.

Note

If you have PCs in your institution that are open only to specific servers and ports (and specifically to Primo), make sure that these PCs/firewalls are also open to the Alma server and port.

If the customer is using on premises / local Primo deployment, Alma communicates with Primo in a bi-directional manner, as follows:

- Alma to Primo: an OAI-PMH XML of published metadata is sent from Alma to Primo via Secured FTP over ports 21/22
- Alma-Primo: bi directional HTTPS communication of patron services over port 443

For more information on Alma-Primo integration, refer to the *Alma-Primo Integration Guide*.

Alma-Primo Patron Services

Patron requests delivered to Alma via Primo (Get It, View It, and so forth) are verified and authenticated prior to any service being rendered. The flow is such that patrons are first required to authenticate external to Alma. After they successfully authenticate, Alma communicates with Primo in a bi-directional manner, over a secured HTTPS port (443), in order to validate the patron authentication prior to providing the requested services.

Primo Back Office

Note

This section is not relevant to Primo VE, which is deployed on the Higher-Ed platform.

In order for staff users to access the Primo Back Office, outgoing HTTPS communication must be allowed/opened on port 1443.

Alma-MetaLib (when MetaLib is in use)

For local installations of MetaLib, where MetaLib communicates with Alma for full-text indication, the communication between Alma and MetaLib is via API over HTTP port 80.

For hosted MetaLib, Alma and MetaLib communicate within the Ex Libris cloud network.

Alma-Summon

Summon and Alma are both hosted services and thus benefit from a complete cloud environment and smooth updates of both solutions. Alma and Summon communicate within the Ex Libris cloud network, and the only external communication is between patrons and Summon over port 80 or 443.

Metadata published from Alma to Summon is sent with secure FTP using port 2022.

Alma-Summon Patron Services

Patron requests in Summon (Get It, View It, and so forth) are verified and authenticated prior to any service being rendered. User authentication is provided by Alma. For more information, see the *Alma-Summon Integration Guide*.

Summon Admin Console

The Summon Admin Console is accessed by staff users through Alma, using port 443.

Alma – Self-Check Machines/SIP-based Systems

Alma supports communication over the SIP2 protocol, which is used primarily for communication with local self-check machines. The communication is bi-directional.

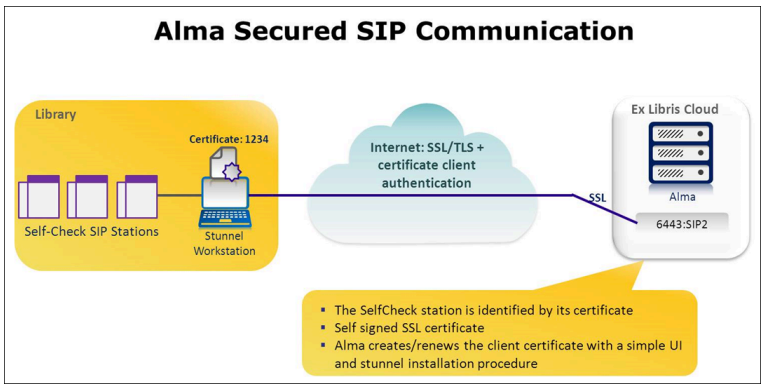
Since the vast majority of the SIP-based systems were built and designed without the cloud in mind, the SIP2 protocol lacks several components in order to fully support a cloud-based SaaS – namely, a unique institution ID and secure communication channel (which is supported in SIP3). Once SIP3 becomes the de-facto standard with cloud capabilities, Ex Libris will support it as well.

To secure SIP2 communication, Alma uses an open source TLS encryption wrapper called Stunnel (http://www.stunnel.org). This is a lightweight component installed locally on standard operating systems, such as Linux or Windows (see supported operating systems: https://www.stunnel.org/ports.html). This component creates a secure TCP "tunnel" communication over port 6443 (which is open to all and not limited to any IP range) with Alma and also serves as a means to uniquely identify and securely route each institution's requests.

The communication flow is as follows:

- The SIP2 local machines communicate with Stunnel software that is installed on the local Windows/Linux workstation.
- The Stunnel encryption component encrypts the TCP communication using a standard encryption method and a security certificate, and will send the SIP2 requests to the Alma cloud over the secure port 6443.

The following diagram describes this architecture:



Alma Secured SIP Communication

Alma – Financial/SIS Systems/Vendor EOD, EDI/SMS (File-Based)

Alma exchanges data with local financial systems, student information solutions, and embedded order data (EOD) using files. FTP or secure FTP is used to facilitate this communication over ports 21/22. SMS communication is also file-based via FTP or secure FTP.

For information on integrating Alma with these systems, refer to the *Alma Integration with External Systems Guide*.

OCLC Connexion

OCLC Connexion (Web or client) interacts with Alma using the TCP-based protocol. Communication occurs via a single port (5500), rather than multiple ports, in order to simplify implementation, while maintaining secure and separate access per institution to the service. This port is open on Ex Libris' side. Ensure that it is open for your institution as well for the workstations which require OCLC Connexion communication with Alma.

To support communication via port 5500, configuration is required in both Alma and OCLC Connexion (Client/Web). For details, refer to Importing Records from OCLC Connexion.

Resource Sharing (ILL)

Communication can be configured between Alma and a resource sharing partner - either peer-to-peer or broker-based. For details, see Resource Sharing Partners.

Peer-to-peer communication takes place over port 9001. Broker-based communication takes place over port 443.

Data Providing

Alma supports several different standard methods of sharing Alma title data with third-parties. Some involve standard online protocols to allow authorized individuals to search their Alma catalog directly (Z39.50 – TCP, OAI-PMH – HTTPS, SRU-SRW – HTTPS, Google scholar and other third-parties from the Discovery services page and Alma delivery – HTTPS).

Others involve publishing data for use outside of Alma (using Alma's robust publishing platform) in a file-based manner using FTP or Secure FTP.

Digital Resources

Institutions that use digital functionality must have HTTPS access to the Ingest and Delivery URLs specified in the S3 Regions and Buckets section of the following page:https://developers.exlibrisgroup.com...al/almadigital

Alma Authentication

To ensure data privacy, end-user authentication must be performed via an institutional identity management system (such as Lightweight Directory Access Protocol/LDAP, SAML 2.0, or CAS 2.0). Your external authentication system must be up and running properly before you can begin Alma implementation.

Alma supports authentication of staff users via the institutional LDAP (Lightweight Directory Access Protocol), using a secure connection. The connection should be secured with a certificate issued by a recognized certificate authority (the list of supported certificates can be found here). To allow LDAP integration, the Alma Data Center IP ranges (mentioned above, according to your location) must be defined. You must also open the port for communication initiated by Alma in the firewall (port 636), as listed in the table below.

In addition, Alma supports SAML (Security Assertion Markup Language) and CAS, which are XML-based, open standard data formats for exchanging authentication and authorization data between parties via HTTPS—in particular, between an identity provider and a service provider such as Alma. The most important problem that SAML and CAS address is the Web browser single sign-on (SSO) problem. Alma supports the SAML 2.0 Web Browser SSO profile and CAS 2.0 Web Browser SSO profile.

For more information on authentication, refer to the following pages on the Ex Libris Developers Network:

- Authentication in LDAP
- SAML Authentication
- Authentication Using CAS

Printers

Printing from Alma is handled in one of the following ways:

- Print to a locally defined PC printer, via the Alma Print Queue. For more information, see The Printout Queue and Quick Printing in Alma.
- Email and corresponding printing rules
  - Each library/institution defines the email addresses of its local printers in Alma, which route staff-oriented, Alma-originating e-mails (including request and transit slips) to the appropriate printer.
  - Newer printers have their own built-in email addresses to support cloud computing. If you are using a new printer, therefore, the email address for notifications should be the printer's email address.
  - Older printers do not support direct emailing and will therefore require a print proxy. There are several applications available to manage printer routing. For example:
    - MS Outlook printing rules – It is possible to create an email address and link this address to a printer via your MS Outlook printing rules.
    - Automatic Email Manager (AEM) by Namtuk – For details, see http://www.namtuk.com/

Note

The above are examples only. Any print proxy that meets your institution's needs can be used.

Emails

Alma sends emails to users, patrons, vendors, and other recipients: acquisition requests, borrower activity status, hold request notifications, overdue reminders, and so forth. In some cases, recipients are expected to send responses to these emails; these responses should be entered manually into Alma (for record keeping; for example, vendor invoices).

Primo and Summon also send emails: catalog records, search alerts, and so forth. No responses are expected for these emails.

You can have Alma email directly or use your institution's mail relay server (see Mail Relay Gateways). The default SMTP-Envelope-From address for these emails is what is defined for the **From:** address in the letter. In Alma, an administrator can configure how Alma sends emails and the **From:** address using the mail handling integration profile; see Configuring Outgoing Email.

Note that the SMTP-Envelope-From address is different from the email's message header **From:** address, which is used for replies and which can be configured separately for most emails.

- The SMTP Envelope-**From** address is used only by the mail server.
- The email's message header **From:** address is used primarily by the email client (such as Outlook or Thunderbird). It may also be looked at by anti-spam filters.

The customer may want to change these two addresses to be email addresses within the customer's domain, such as <somename>@cust_domain.edu for one or both of the following reasons:

- The customer wants all emails sent on their behalf to be branded with their own domain.
- The customer wants to receive bounce emails (automatic notification of non-delivered emails) directly to a mailbox on their own mail server.

To change these addresses to be email addresses within the customer's domain:

- The customer must change **EnvelopeFrom** to a valid mailbox in the customer's domain, for example library-bounce@cust_domain.edu.
- The customer must change the message header **From:** addresses in relevant Alma letters to addresses in the same domain used for **EnvelopeFrom**, for example library-noreply@cust_domain.edu. These addresses do not have to be valid mailboxes.

The customer must add an SPF Include Entry for the Ex Libris' mail-relay servers into the SPF record of the customer's domain (see Mail Relay Gateways).

Ex Libris supports the DomainKeys Identified Mail (DKIM) standard to help prevent email spoofing for outgoing messages where the "From" address is <some_name>@exlibrisgroup.com. As of February 2024, DKIM is supported for outgoing messages where the "From" address is set to a customer's domain. We do offer secure email delivery alternatives – i.e. SPF validation and/or Mail Relaying via customer's Mail Infrastructure.

Note

For Primo Classic, DKIM is not supported in multi-institutional environments (such as Primo MT/TC environments).

Mail Relay Gateways

Alma and Primo use dedicated mail-relay servers in each region. Summon does not use such servers.

You can have Alma email directly or use your institution's mail relay server; see Configuring Outgoing Email.

Ex Libris supports Transport Layer Security (TLS) 1.2 on the mail-relay servers to deliver mail securely.

Secure SMTP over TLS allows for encrypted messages; TLS uses Public Key Infrastructure (PKI) to encrypt messages from mail server to mail server.

The preferred (default) setup of the Alma email servers involves the use of encrypted transactions. If a customer's email servers support TLS, Ex Libris upgrades the SMTP session to use TLS. If TLS is not supported on the customer's email servers, Ex Libris establishes the session without TLS.

Alma email servers support encrypted emails (TLS) signed with a GoDaddy certificate. If a customer's email servers support TLS, it is recommended that GoDaddy be added as a root certificate authority to the MTA. (Note that when the certificate is not verified, the email is delivered as "untrusted" to the customer.)

Ex Libris strongly recommends that the customer allows the IP addresses of Ex Libris' mail-relay servers (see below) as permitted SMTP servers in any anti-spam filters managed by the customer or any email service to which they are subscribed.

The Ex Libris mail-relay server IPs and hostnames for Alma and Primo are as follows:

Region	SPF Include Record	IPs/IP Ranges
APAC	include:spf-ap.exlibrisgroup.com	117.20.42.8/29 (117.20.42.8 - 15)

Region	SPF Include Record	IPs/IP Ranges
		216.147.221.8/31 (216.147.221.8 - 9)
Canada	include:spf-ca.exlibrisgroup.com	216.147.222.12/30 (216.147.222.12 - 15)
China	include:spf-cn.exlibrisgroup.com.cn	124.251.9.14/31 (124.251.9.14 - 15)
North America	include:spf-na.exlibrisgroup.com	64.74.237.230/31 (64.74.237.230 - 231) 216.147.212.20/30 (216.147.212.20 - 23)
Europe	include:spf-eu.exlibrisgroup.com	95.172.90.143 95.172.90.156 216.147.218.8/30 (216.147.218.8 - 11)

Note

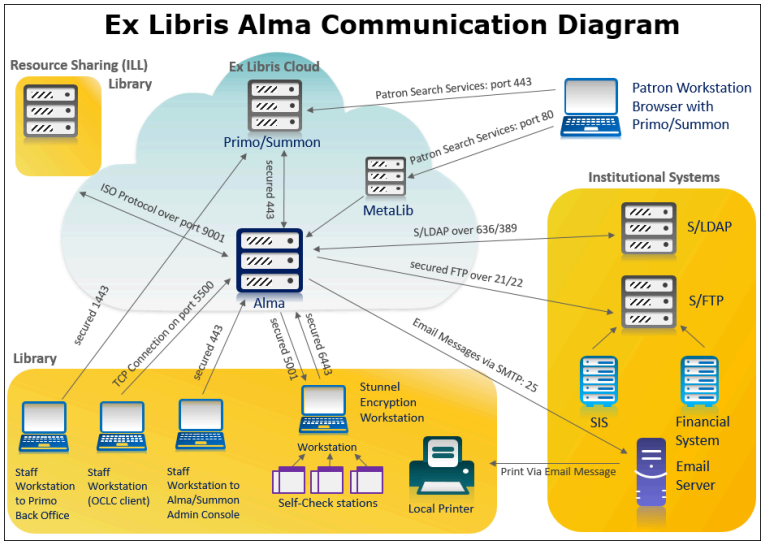
Only the SPF entry or IP address(s) in the customer's region need to be included.

Ex Libris recommends using the SPF include entry listed above, rather than the IPs, since mail-relay IPs may change.

For allowing mail-relay IPs in mail filters for any European instance of Alma or Primo, both IP addresses must be added.

Network Communication Diagram and Table

The following diagram describes the different possible network communications with Alma.



Alma Communication

The table below summarizes the complete network communication between the Alma cloud and the customer's network:

Integration Type	Initiator	Target	Protocol	Ports	Comments
Staff workstation	Staff workstation	Alma	HTTPS	443	
	Staff workstation	Primo (Back Office)	HTTPS	1443 (multi-tenant)	
	Staff workstation	Summon Admin Console (via Alma)	HTTPS	443	
Patron workstation	Patron workstation	Primo	HTTPS	443	
	Patron workstation	Summon	HTTPS	443	
Staff authentication	Alma	CAS (SSO) SAML (SSO) Social Login	HTTPS	443	
		Secure LDAP	TLS-Secured	636	
Alma-Primo	Primo	Alma	HTTPS	443	
	Primo Central	Alma	HTTPS	443	Primo central registration with Alma URL
Alma-Primo end-user authentication	Primo	CAS (SSO) SAML (SSO) Social Login	HTTPS	443	
		Secure LDAP	TLS-Secured	636	
Alma-Summon	Summon	Alma	HTTPS	443	

Integration Type	Initiator	Target	Protocol	Ports	Comments
Alma-Summon end-user authentication	Summon (via Alma)	CAS (SSO) SAML (SSO) Social Login	HTTPS	443	
		Secure LDAP	TLS-Secured	636	
Email	Alma	Email Server	SMTP	25	Print via email messages
S/FTP file-based integrations (outgoing)	S/FTP Server	• ERP/financial • Bursar payment fines/fees • EDI • SMS • Publishing platform • File-based remote storage • Link resolver statistics	S/FTP	21/22	
	S/FTP Server	Publishing platform - Summon	S/FTP	2022	
S/FTP file-based integrations (incoming)	• Student Information Systems (SIS) • ERP/financial • MD import including EOD • EDI • Course Loader	S/FTP Server	S/FTP	21/22	
Ex Libris APIs (for more information, see the Developer Network)	Client applications	Alma	HTTPS	443	
Remote storage (for file-based remote storage, see **S/FTP file-based integrations - outgoing** above)	Stunnel workstation (Dematic ASRS remote storage facility system)	Alma	TLS-secured	6443	Using Stunnel
	Alma	Stunnel workstation (Dematic ASRS remote storage facility system)	TLS-secured	5001	Using Stunnel
Self-check	Stunnel workstation (SIP2 Self-Check Stations)	Alma	TLS-secured SIP2	6443	Using Stunnel

Integration Type	Initiator	Target	Protocol	Ports	Comments
Resource sharing (ILL) system (Alma or non-Alma)	Peer to peer resource sharing (ILL) system	Alma	TCP	9001	
	Alma	Peer to peer resource sharing (ILL) system	TCP	9001	
	Broker resource sharing (ILL) system	Alma	HTTPS	443	
	Alma	Broker resource sharing (ILL) system	HTTPS	443	
RFID	Alma	RFID driver installed on a user's PC	HTTP	Determined by user	For more information on port configuration, see the Developer Network.
OCLC Connexion	OCLC Connexion	Alma	TCP	5500	Accelerated servers are not supported.
Google Scholar and other third-party electronic service providers	Electronic service provider	Alma (via Discovery)	HTTP or HTTPS	80 or 443	Via Discovery services page directed to Alma's delivery services
Z39.50 data providing	Z39.50 server	Alma	TCP	1921 or 210	210 is open on all production environments; sandbox environments support only 1921
OAI-PMH data providing	OAI	Alma	HTTPS	443	
SRU-SRW data providing	SRU-SRW	Alma	HTTPS	443	
Aleph Central Catalog for Aleph contribution	Alma	Aleph	HTTP or HTTPs	Institution-specific port definition	
Aleph Central Catalog for Aleph bibliographic record updates	Alma	Aleph	TCP	Institution-specific port definition	
Aleph Central Catalog for Aleph retrieving bibliographic records (external search)	Alma	Aleph	TCP	Institution-specific port definition	
Aleph Central Catalog for SBN contribution	Alma	SBN	HTTP	Institution-specific port definition	
Aleph Central Catalog for SBN retrieving bibliographic/authority	Alma	SBN	HTTP	Institution-specific	

Integration Type	Initiator	Target	Protocol	Ports	Comments
records (external search)				port definition	
Electronic access proxy (EZProxy, etc.)	Alma	Proxy	HTTPS	443	
Webhooks	Alma	External server	HTTPS	443	
Deposit using SWORD	Alma	Alma SWORD server	HTTPS	443	
Online payment	Alma	WPM education system	HTTPS	443	
	Primo	WPM education system	HTTPS	443	
Learning Tools Interoperability (LTI)	Course management system	Alma	HTTPS	443	