Chrome browser identifies connection as "Not Secure"

- **Product:** Cross-Product
- **Relevant for Installation Type:** Multi-Tenant Direct, Dedicated-Direct, Local, TotalCare

Description

As part of Google's initiative to promote secure browsing, beginning in October 2017, Chrome will show the 'Not secure' warning when users enter data on an HTTP page. It is Google's plan to label HTTP sites as non-secure in gradual steps, based on increasingly broad criteria. Starting in version 62, Chrome will show the "Not secure" warning when users type data into HTTP sites. See: Next Steps Toward More Connection Security, *Chromium Blog*, posted Thursday, April 27, 2017.

While this change has no impact on the actual security level provided by Ex Libris solutions, users visiting an HTTP (as oppose to HTTPS) web page in which data is entered may see a "Not Secure" warning in Chrome, depending on the product and the way it is configured by the customer.

Resolution

For products which are currently accessed through HTTP and that can support HTTPS, customers may wish to consider moving to HTTPS in order to avoid the 'Not Secure' message.

The table below lists our products and whether:

- **HTTPS is enforced** – meaning that HTTPS is the only option that exists to connect to the solution and no action is required to be done by you
- **A local configuration is needed** – means that the product can support HTTPS and a configuration change is needed to enable HTTPS. The specific product's user guide will contain detailed information regarding the configuration change
- **A Salesforce request is needed** – indicated by "Request through Salesforce," meaning that a special security certificate needs to be provided by Ex Libris in order to enable HTTPS connectivity. Please open a Salesforce case.
- **HTTPS is not available** – indicated by "No." While there is no change in the supported security capabilities of the product, it is not possible to enable to HTTPS.

To enable HTTPS configurations, read and follow the specific product knowledge article for the specific Ex Libris product.

Ex Libris products and HTTPS:

Ex Libris Product	Local	Hosted	SaaS
360 Link/EJP	Not applicable	Not applicable	HTTP/HTTPS

Ex Libris Product	Local	Hosted	SaaS
360 Client Center	Not applicable	Not applicable	Enforced
Alephino	Local configuration	Request through Salesforce	Not applicable
AquaBrowser LiQuid	Not applicable	Request through Salesforce	Request through Salesforce
AquaBrowser Classic	Request through Salesforce	Request through Salesforce	Not applicable
Aleph (OPAC) web service	Local configuration	Request through Salesforce	Not applicable
Aleph (GUI)	Not applicable	Not applicable	Not applicable
Alma	Not applicable	Not applicable	Enforced
campusM	Not applicable	Not applicable	Supported
DigiTool	Request through Salesforce	Not applicable	Not applicable
Intota	Not applicable	Not applicable	Enforced
Intota assessment	Not applicable	Not applicable	Not applicable
Leganto	Not applicable	Not applicable	Enforced
MetaLib	Local configuration	Request through Salesforce	not applicable
Pivot	Not applicable	Not applicable	Enforced
Primo BO	Local configuration	Request through Salesforce	Enforced
Primo FE new UI	Local configuration	Enforced	Enforced

Ex Libris Product	Local	Hosted	SaaS
Primo FE Old UI	Local configuration	NO	NO
RefWorks	Not applicable	Not applicable	Enforced
Rosetta	Local configuration See also: Rosetta Load Balancer Example	Not applicable	Not applicable
SFX	Local configuration	Request through Salesforce	Request through Salesforce
Summon	Not applicable	Not applicable	Supported
Ulrich's	Not applicable	Not applicable	Supported
Voyager	Local configuration	Request through Salesforce	Request through Salesforce

---

- **Article last edited:** 27-Sep-2017