SECURITY UPDATE

GLOBALSIGN ROOT/INTERMEDIATE CERTIFICATE UPDATES TO R3

OVERVIEW

JAGGAER's Certificate Authority (CA), GlobalSign, has issued new certificates signed by the R3 Root, and JAGGAER ONE is required to use these new certificates moving forward. As a result, all new requests for RSA Certificates will be issued under the new RSA CA for Root R3, and customers will be required to trust the R3 Root and Intermediate CAs.

The purpose of this document is to provide guidance to customers on downloading and installing the GlobalSign Root R3 and OrganizationSSL Intermediate Certificates.

Impact to Customers

If the Root and Intermediate Certificates are not trusted by your integration, and you take no action, your systems will not be able to connect to the Jaggaer Production endpoints after this change is implemented. Your browsers will generate alerts, and your integrations will stop functioning. Please discuss this change with your technology teams to ensure that appropriate actions are taken to ensure uninterrupted service.

Important Dates

Date	Description
February 8, 2020	The new R3 certificates are moved into the UserTest environment. At this point, organizations can test their systems to ensure that there are no problems with the certificates prior to the certificates being moved into Production.
February 22, 2020	The new R3 certificates are moved into the Production environment. This is the deadline for customers to update their systems to avoid disruption of services.

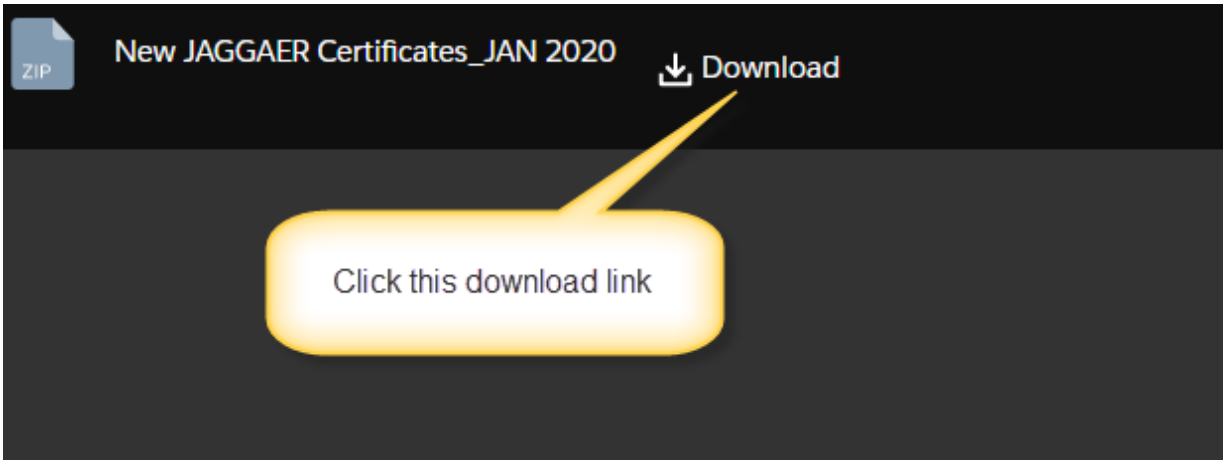
ACTIONS

If the R3 Root and Intermediate Certificates are not trusted by your browsers, applications, or libraries, you must download and install the certificates before the scheduled maintenance to avoid service disruption. Please work with your technology teams to determine what actions you must take to trust this CA.

Download and install the Root Certificate Bundle

Follow these steps to download and install the GlobalSign R3 Root and Intermediate Certificates:

1. For direct access to the updated security certificates available in multiple formats—including **.cer**, **.der**, **.p7b**, and **.pem**—please click the **Download** link on the following page, available: ***HERE***



2. Import the certificates into your trusted CA store based on your system parameters.

3. Restart services if applicable.

   Important Note! Some applications require a restart to use the new certificate for SSL connections, even if the trusted root store is in place.

For Java

You may need to install the GlobalSign R3 Root and Intermediate Certificates into your Java keystore on your application and integration servers.

For .NET

Click here for instructions on adding certificates to Trusted Certification Authorities store for local computers.

ADDITIONAL CONSIDERATIONS

- To avoid disruption of service, customers should make all necessary changes prior to JAGGAER migrating the new R3 Certificates to the Production environment on February 22, 2020.
- The new certificates will not be available in the UserTest and Production environments until February 2020. If your system has the ability to support multiple certificates, you may update your certificates to R3 at any time prior to February. If your system can hold only one certificate at a time, you will need to wait until February to make the update.
- When installing new Certificates (including renewals and re-issuance), be sure to install the new CA Certificate on the web servers.
- In some cases, the web server may need to be configured with the GlobalSign R3-R5 Cross Certificate or possibly with Root R3 or Root R5 as part of the standard configuration process. For your reference, you can check the GlobalSign Cross Certificates support article, which is found here.

Thank you for your support as it allows JAGGAER to maintain the highest security standards to ensure the safety of your data.