FAQ: External Certificate Replacement 2024

Version: 1

Q1 What's changing?

A1 The external (Public) SSL certificate for *.pjm.com is expiring, and will be replaced in train and production environment on the below dates.

Train: Nov. 19, 2024
Production: Dec. 3, 2024

Q2 What is this change for? Additional security, updating a certificate, etc.? Or why is the Root and Intermediate certificate changing with this renewal?

A2 Certificate authorities occasionally update their root and intermediate certificates to enhance security or comply with industry standards. This ensures continued trust and security for encrypted connections. This is a standard practice and not an additional security.

Q3 How does this impact PJM members or anyone accessing PJM applications?

A3 If the new Root and Intermediate certificates are not properly installed, users may experience trust errors when accessing our services. It's crucial to ensure that the new certificates are installed in your TLS/SSL trust store for your Java/.net-based or any custom client-side applications/tool on the user end.

Most of the browsers have the updated TLS/SSL trust store; however, we recommend verifying the browser(s) TLS/SSL trust store as well.

Below is the high-level procedure on how to update the TLS/SSL trust store on Java/.net framework.

https://www.pjm.com/-/media/committees-groups/forums/tech-change/2024/20240926/20240926-installing-certificates-java-and-net.ashx

Q4 What should I do or what steps do we need to take to complete the renewal?

A4 Obtain the new Root and Intermediate certificates from the Certificate Authority (CA).

Please download and install the below Root and Intermediate certificates from the DigiCert CA.

	Root Certificate	Intermediate Certificate
Link	https://www.digicert.com/kb/digicert-root certificates.htm#roots	https://www.digicert.com/kb/digicert-root-certificates.htm#intermediates
File Name	DigiCert Global Root G2	GeoTrust TLS RSA CA G1

Note: The Root and Intermediate certificates can be downloaded and added to your existing trust store any time before the change window.

Q5 How can I validate I have the right root/immediate certificates?

A5 Please follow the validation instructions in the procedure document.

https://www.pjm.com/-/media/committees-groups/forums/tech-change/2024/20240926/20240926-installing-certificates-java-and-net.ashx

Q6 What if users experience issues after the renewal? Who can I contact for help?

A6 Clear your browser cache.

Restart your client application.

Verify the TLS/SSL trust store on your application or framework is updated with the required Root and Intermediate certificates. If problems persist, please feel free to reach out to contact PJM.

Q7 Will this affect our existing services?

A7 If all steps are followed correctly, there should be minimal or no impact during the change. You may also want to clear browser caches or restart applications.

Q8 What effect does this have on the browserless API?

A8 Make sure your client applications are updated to handle new certificate trust chains.