Troubleshoot Ceritifcate Expiration Error during Umbrella Integration Access

Contents

[Introduction](#)

[Issue](#)

[Cause](#)

[Resolution](#)

Introduction

This document describes how to troubleshoot a certificate expiration error when an Umbrella integration accesses **s-platform.api.opendns.com** or **fireeye.vendor.api.opendns.com**.

Issue

Umbrella integrations which use some third-party clients can fail with an error verifying the digital certificate of the server for the Umbrella APIs at s-platform.api.opendns.com and fireeye.vendor.api.opendns.com. The error text or code varies depending on the client program used in the integration, but typically indicates that an expired certificate is present.

Cause

This issue is not caused by the server's certificate, which is currently valid. Rather, the issue is caused by an out-of-date certificate trust store used by the client.

The webserver which serves s-platform.api.opendns.com and fireeye.vendor.api.opendns.com uses a digital certificate that is issued (that is digitally signed) by the intermediate certificate **R3** from certificate authority Let's Encrypt. R3 is signed by a public key which is found in both the current **SRG Root X1** root certificate from Let's Encrypt, and an older, cross-signed version of SRG Root X1. Thus, two validation paths exist: one which terminates at the current SRG Root X1, and one which terminates on the issuer of the cross-signed version, the **DST Root CA X3** certificate, issued by certificate authority IdenTrust.

A diagram of the issuance is available from Let's Encrypt. Additionally, the Qualys SSL Labs tool can be used to view the two "Certification paths" with their respective certificates and the certificate details, such as the expiration dates.

Root certificates are kept in one or more certificate trust stores on client systems. On September 30th, 2021, the DST Root CA X3 certificate expired. Since this date, clients which have the DST Root CA X3 certificate in their trust store, but do not have the newer RG Root X1 root certificate, fails to connect to s-platform.api.opendns.com or fireeye.vendor.api.opendns.com due to a certificate error. The error message or code can indicate an expired certificate as the reason for the error. The expired certificate is the DST Root CA X3 certificate in the client's trust store, not the server certificate for the API servers, s-platform.api.opendns.com and fireeye.vendor.api.opendns.com.

Resolution

To remedy this issue, update the client's trust store to include the new SRG Root X1 certificate, which can be downloaded from the Let's Encrypt website. (This page also provides websites for testing your clients.) Consult the documentation for your client or operating system to obtain instructions on viewing and updating your client's trust store. If an official update package or automatic update mechanism is available then this is typically preferable to manually updating the trust store.

If manually updating the trust store with the new SRG Root X1 certificate, then we also recommend removing the expired DST Root CA X3 certificate, in case your client's validation path-building code is problematic. An official update of the trust store from the provider of your client or operating system can add the SRG Root X1 and remove the DST Root CA X3 certificate.