Upcoming Citrix Access Gateway (CAG) Certificate Updates
Impact to Firefox and Safari Browser Users

Introduction

The Citrix Access Gateway (CAG) remote access solution is a collaborative effort between Service Delivery and Engineering (SDE) and Network Security Operations Center (NSOC). SSL certificates are used to encrypt traffic from the end device over the internet to the CAG; these certificates are being renewed and will utilize a new Certificate Authority (CA) for verification. The new CA is not currently part of the Mozilla Firefox trusted certificate store. This causes an error page to display when accessing the CAG login screen using Mozilla Firefox. Macintosh users will experience the same issue with Firefox and Safari.

The CAG webpage will receive the updated certificates beginning January 27th through February 7th. At that time Firefox users will receive an error message advising "This Connection is Untrusted". There are a few different solutions available to resolve this error message listed in the *Available Solutions* section below.

Background

The VA is moving to a new CA managed by the Federal Public Key Infrastructure Management Authority. In the past, certificates were issued using a Cybertrust CA. This CA is being sunsetted, thus all new SSL certificates are being issued by the Federal Common Policy CA. The vendor Mozilla has been engaged by the Federal Public Key Infrastructure Management Authority to have their certificate store updated with the new Federal Common Policy CA, but a date for this to be completed has not been determined.

Available Solutions

#1 Add the certificate as an exception

When the "This Connection is Untrusted" error page appears, use this solution to only add an exception for that specific CAG site.

1. Navigate to the CAG Login Screen using Firefox
2. Expand the section **I Understand the Risks**
3. Click the **Add Exception…** button
4. A new pop-up window appears, click **Confirm Security Exception**

FAQ: *https://rescue.vpn.va.gov/FAQ/Default.aspx?ShortName=CAG266*

#2 Add the Federal Common Policy CA certificates manually

Adding the Federal Common Policy CA certificate resolves the issue for all websites that are issued certificates from the Federal Common Policy CA. This is the best method to use; this ensures that all other sites that are navigated to that use the Federal Common Policy do not display an untrusted error.

1. Use a browser and connect to the RESCUE Media site https://rescue.vpn.va.gov
2. Navigate to ***Citrix (CAG) > Media***
3. Under the section ***Citrix Software***, download the **Federal Common Policy** Certificate (if you performed Steps 1-3 using the Firefox browser, skip to #10)
4. Launch Firefox and open **Options**
5. Choose the **Advanced** tab, then the **Certificates** sub-tab

6. Click the **View Certificates** button
7. Ensure the **Authorities** tab is chosen, click **Import…**
8. Browse to the folder that the Federal Common Policy Certificate was downloaded to
9. Choose the **Federal Common Policy.cer** and click **Open**
10. Check the box next to "Trust this CA to identify websites"
11. Click **OK**
12. To verify the Federal Common Policy certificate is now in the certificate store scroll down to U.S. Government under Certificate Name
13. Click **OK** on all open screens
14. Browse to the CAG Login page and the error should no longer be presented

FAQ: *https://rescue.vpn.va.gov/FAQ/Default.aspx?ShortName=CAG267*

#3 Use an alternate browser
Use either Internet Explorer or Chrome (which use the same certificate store) - the Federal Common Policy CA has already been added to the trusted certificate authorities.

#4 Macintosh Users Keychain update
Macintosh users need to install the complete certificate chain of trust to resolve the issue. Refer to the following FAQ for information on installing the certificates.

FAQ: *https://rescue.vpn.va.gov/FAQ/Default.aspx?ShortName=CAG268*

Access the following links for additional information
Firefox Bugzilla Case: https://bugzilla.mozilla.org/show_bug.cgi?id=478418
RESCUE Media Site: https://rescue.vpn.va.gov

Points of Contact

National Service Desk*
Local: 916-692-7460 Option 1
Toll Free: 1-855-NSD-HELP (1-855-673-4357) Option 6, Option 1
If you are unable to call the NSD, you may report a problem via email: NSD.VPNSecurity@va.gov

**The NSD Specialty Team is available 24x7 to assist you with any issues you may be experiencing with any of VA's remote access solutions, including the CAG. If you are experiencing any issues, now or in the future that the Remote Access FAQs available on the RESCUE Media Site do not address, please contact the NSD to ensure your issue is resolved. If you are experiencing an issue and haven't opened up a ticket on it recently, please do so at your earliest convenience.*