Niagara 4.13 Feature Preview - Certificate Enhancements and Web View

May 11, 2023

Q&A

1. Will 4.13 be the next LTS build?

   4.15 will be the next LTS.

2. Is there a way to automate the cert application to the panel (JACE es3s/es3r)?

   Probably need a little clarity on what you are asking, but if I "think" I understand what you are asking, we have provisioning job steps that can be used to generate and install certs to stations. In addition, we are in development of a feature that can handle auto re-signing of certs. This feature is not available yet.

3. Is it possible to import a 3-part certificate directly in to the "User Trust Store" and the "User Key Store" without making a certificate request from Niagara first?

   Yes, you can import keypairs with cert into the key store and certs into the user trust store that are generated externally (like with openssl). Our updated dialogs make openssl on Windows easier. Outside Niagara hint: Keystore Explorer.

   Of course, the best desired case is to generate the keypair on the station/JACE so that the private key is never actually shared, but there are some cases (IT requirements, etc.) where you may need to be provided the private key.

4. Do I need a PEM-fil with both the cert and the private key? Is what you are saying is not safe?

   It's a little messy. I'm not going to say its "not safe". But it is less desirable because now you have to trust the entire handling of the containing file from generation to importing. If someone can access that file enroute to importing, they could "steal" the private key and use it to man-in-the-middle you or replace it with their own.

   When you generate the pem file, you CAN encrypt the private key in the file (PEM standard) so that it's harder, but still not as good as not exposing the private key at all.

5. In a non-DNS environment, is it possible to add IP address to the certificate? Is it selectable or do you need to enter "IP:"

   Yes, when you create a Subject Alternative Name, you can set an IP address and it will be added as an IP name instead of a DNS name.

   This also works with the AX cert creation dialog but kind of automatically as it "detects" that it's an IP address and switches the SAN type.

   When you edit it in the web view, there is an option to set/add the SAN type. There are other types of SANS too like email (nothing to with TLS handshake, but part of the spec). In the AX dialog, it basically does a regex check under the hood the determine it.

6. We generate our own certs and get is signed by CA for each store but right now we are applying them to store by store manually. We would like to find out how we can script it to install the certs automatically at each store panel.?

   Provision steps will help A LOT with this and the new cert signing service features that are coming will make it easier to maintain them once configured.

7. I have this client, who has provided their own root cert. and they make the cert, and got it signed. What do I need from them? Do I have to send something to them at all?

   If they are their own CA (which is fine), you will need to import the root CA cert into the User Trust Store. This is not uncommon for internal networks and IT departments.

   If they are also provided the keypair and signed cert, you will need those as well and import them into the user key store.

8. What it's the got form them was, this 2 types, cert.pem and a key.prv , but it's the can 't import that in Niagara

   If you open the prv file, if it looks like a text file

   *** RSA PRIVATE KEY ****

   {blab}{blah}{blah}

   then create 1 file with both the contents of the pem and the prv file.

   If the prv file doesn't look something like that, then you may need to use a tool to convert it. If you find that it's the latter, let us know. We are working on support for importing other types.

9. It is exactly that type *** RSA PRIVATE KEY **** , and i have tried to put the 2 types in to one file with notesblok, and saved it as an pem file, and when i try to import it in "User Key Store" it popup and ask for the password for the privtekey, and when i enter it and click "ok" nothing happens.

   Hmm. If you need to or are willing to, please reach out to support to see if there is "bug" there. Seems odd.

10. Will the host continue to allow a connection after the Certificate has expired but has a self-signed cert and has a chain of trust in the User Trust Store? example: Supervisor to JACE?

    It will fail validation because it's now expired but can be "continued" by adding it to the allowed host table. Not desirable.

11. Do you adhere to the new browser rules regarding no certificate over 2 years?

    We default to 1 year, but as the administrator, you can set it to whatever you want. That being said, we "should" add a warning to the generation and sec dashboard when the expiration is greater that 2 years. Good idea.

12. Where is the Certificate Management Wizard?

    When commissioning a station (from niagarad), you can right click on the platform and there is an option for cert management wizard like commissioning wizard.

13. Will this new method allow certificate and authority creation on a System behind a secure firewall that does not allow the certificate to determine date/time from the Web? Cannot reach the Web for TLS.

    Validation of the cert is done by the "client" receiving the cert, so as long as the client has a reasonably accurate clock, it should be ok.