Smart Card and certificate login support

OnCommand Insight

NetApp
October 24, 2024

Table of Contents

Smart Card and certificate login support

OnCommand Insight supports use of Smart Cards (CAC) and certificates to authenticate users logging in to the Insight servers. You must configure the system to enable these features.

After configuring the system to support CAC and certificates, navigating to a new session of OnCommand Insight results in the browser displaying a native dialog providing the user with a list of personal certificates to choose from. These certificates are filtered based on the set of personal certificates that have been issued by CAs trusted by the OnCommand Insight server. Most often, there is a single choice. By default, Internet Explorer skips this dialog if there is only one choice.

> For CAC users, smart cards contain multiple certificates, only one of which can match the trusted CA. The CAC certificate for `identification` should be used.

> For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):
>
> - How to configure Common Access Card (CAC) authentication for OnCommand Insight
> - How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
> - How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
> - How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
> - How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Configuring hosts for Smart Card and certificate login

You must make modifications to the OnCommand Insight host configuration to support Smart Card (CAC) and certificate logins.

Before you begin

- LDAP must be enabled on the system.
- The LDAP `User principal account name` attribute must match the LDAP field that contains a user’s ID.

> If you have changed *server.keystore* and/or *server.truststore* passwords using securityadmin, restart the *sanscreen* service before importing the LDAP certificate.

> For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):
>
> - How to configure Common Access Card (CAC) authentication for OnCommand Insight
> - How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
> - How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
> - How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
> - How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Use the `regedit` utility to modify registry values in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Change the JVM_Option `DclientAuth=false` to `DclientAuth=true`.
2. Back up the keystore file: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Open a command prompt specifying `Run as administrator`
4. Delete the self-generated certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Generate a new certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Generate a certificate signing request (CSR): `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. After the CSR is returned in step 6, import the certificate, then export the certificate in Base-64 format and place it in `"C:\temp" named servername.cer`.
8. Extract the certificate from the keystore:`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extract a private key from the p12 file: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Merge the Base-64 certificate that you exported in step 7 with the private key: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey`

```
"C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name
"servername.abc.123.yyy.zzz"
```

11. Import the merged certificate into the keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`

12. Import the root certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`

13. Import the root certificate into the server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`

14. Import the intermediate certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    Repeat this step for all intermediate certificates.

15. Specify the domain in LDAP to match this example.

1. Restart the server.

Configuring a client to support Smart Card and certificate login

Client machines require middleware and modifications to browsers to enable the use of Smart Cards and for certificate login. Customers who are already using Smart Cards should not require additional modifications to their client machines.

Before you begin

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

The following are the common client configuration requirements:

- Installing Smart Card middleware, such as ActivClient (see http://militarycac.com/activclient.htm)
- Modifying the IE browser (see http://militarycac.com/files/Making_AKO_work_with_Internet_Explorer_color.pdf)
- Modifying the Firefox browser (see https://militarycac.com/firefox2.htm)

Enabling CAC on a Linux server

Some modifications are required to enable CAC on a Linux OnCommand Insight server.

The Root CA must be imported into the truststore.

Steps

1. Navigate to `/opt/netapp/oci/conf/`
2. Edit `wildfly.properties` and change the value of `CLIENT_AUTH_ENABLED` to "True"
3. Import the “root certificate” that exists under `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Restart the server

Configuring Data Warehouse for Smart Card and certificate login

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins.

Before you begin

- LDAP must be enabled on the system.
- The LDAP `User principal account name` attribute must match the LDAP field that contains a user’s government ID number.

  The common name (CN) stored on government-issued CACs is normally in the following format: `first.last.ID`. For some LDAP fields, such as `sAMAccountName`, this format is too long. For these fields, OnCommand Insight extracts only the ID number from the CNs.

> ⓘ If you have changed *server.keystore* and/or *server.trustore* passwords using securityadmin, restart the *sanscreen* service before importing the LDAP certificate.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Use regedit to modify registry values in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Change the JVM_Option `-DclientAuth=false` to `-DclientAuth=true`.

   For Linux, modify the `clientAuth` parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Add certificate authorities (CAs) to the Data Warehouse trustore:

   a. In a command window, go to `..\SANscreen\wildfly\standalone\configuration`.

   b. Use the `keytool` utility to list the trusted CAs: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`
   See the SecurityAdmin documentation for more information about setting or changing the password for server_trustore.

   The first word in each line indicates the CA alias.

   c. If necessary, supply a CA certificate file, usually a `.pem` file. To include customer's CAs with Data Warehouse trusted CAs go to `..\SANscreen\wildfly\standalone\configuration` and use the `keytool` import command: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   my_alias is usually an alias that would easily identify the CA in the`keytool -list` operation.

3. On the OnCommand Insight server, the `wildfly/standalone/configuration/standalone-full.xml` file needs to be modified by updating verify-client to "REQUESTED" in `/subsystem=undertow/server=default-server/https-listener=default-https`to enable CAC. Log in to the Insight server and run the appropriate command:

OS	Script

Windows	<install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

After executing the script, wait until the reload of the wildfly server is complete before proceeding to the next step.

4. Restart the OnCommand Insight server.

Configuring Cognos for Smart Card and certificate login (OnCommand Insight 7.3.10 and later)

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins for the Cognos server.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.10 and later.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Add certificate authorities (CAs) to the Cognos trustore.

   a. In a command window, go to `..\SANscreen\cognos\analytics\configuration\certs\`

   b. Use the `keytool` utility to list the trusted CAs: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>

   The first word in each line indicates the CA alias.

   a. If no suitable files exist, supply a CA certificate file, usually a `.pem` file.

   b. To include customer's CAs with OnCommand Insight trusted CAs, go to `..\SANscreen\cognos\analytics\configuration\certs\`.

   c. Use the `keytool` utility to import the `.pem` file: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` is usually an alias that would easily identify the CA in the `keytool -list` operation.

   d. When prompted for a password, enter the password from the */SANscreen/bin/cognos_info.dat* file.

   e. Answer `yes` when prompted to trust the certificate.

2. To enable CAC mode, do the following:

   a. Configure CAC logout page, using the following steps:

      - Logon to Cognos portal (user must be part of System Administrators group i.e. cognos_admin)
      - (Only for 7.3.10 and 7.3.11) Click Manage -> Configuration -> System -> Security
      - (Only for 7.3.10 and 7.3.11) Enter cacLogout.html against Logout Redirect URL -> Apply
      - Close browser.

   b. Execute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

   c. Start IBM Cognos service. Wait for Cognos service to start.

3. To disable CAC mode, do the following:

   a. Execute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

   b. Start IBM Cognos service. Wait for Cognos service to start.

   c. (Only for 7.3.10 and 7.3.11) Unconfigure CAC logout page, using the following steps:

      - Logon to Cognos portal (user must be part of System Administrators group i.e. cognos_admin)
      - Click Manage -> Configuration -> System -> Security
      - Enter cacLogout.html against Logout Redirect URL -> Apply
      - Close browser.

Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.10 and later)

You can add SSL certificates to enable enhanced authentication and encryption for your Data Warehouse and Cognos environment.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.10 and later.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

You must have admin privileges to perform this procedure.

Steps

1. Stop Cognos using the IBM Cognos Configuration tool. Close Cognos.
2. Create backups of the `..\SANScreen\cognos\analytics\configuration` and `..\SANScreen\cognos\analytics\temp\cam\freshness` folders.
3. Generate a Certificate Encryption Request from Cognos. In an Admin CMD window, run:
   a. cd `"\Program Files\sanscreen\cognos\analytics\bin"`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Note: here -H and -I are to add subjectAltNames like dns and ipaddress.
   c. For <password>, use the password from the */SANscreen/bin/cognos_info.dat* file.
4. Open the `c:\temp\encryptRequest.csr` file and copy the generated content.
5. Input the encryptRequest.csr content and generate certificate using CA signing portal.
6. Download the chain certificates by including root certificate by using PKCS7 format

   This will download fqdn.p7b file
7. Get a cert in .p7b format from your CA. Use a name that marks it as the certificate for the Cognos Webserver.
8. ThirdPartyCertificateTool.bat fails to import the entire chain, so multiple steps are required to export all certificates. Split the chain by exporting them individually as follows:
   a. Open the .p7b certificate in "Crypto Shell Extensions".
   b. Browse in the left pane to "Certificates".
   c. Right-click on root CA > All Tasks > Export.
   d. Select Base64 output.
   e. Enter a file name identifying it as the root certificate.

   f. Repeat steps 8a through 8e to export all of the certificates separately into .cer files.

   g. Name the files intermediateX.cer and cognos.cer.

9. Ignore this step if you have only one CA certificate, otherwise merge both root.cer and intermediateX.cer into one file.

   a. Open root.cer with NotePad and copy the content.

   b. Open intermediate.cer with NotePad and append the content from 9a (intermediate first and root next).

   c. Save the file as chain.cer.

10. Import the certificates into the Cognos keystore using the Admin CMD prompt:

    a. cd “Program Files\sanscreen\cognos\analytics\bin”

    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer

    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer

    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer

11. Open the IBM Cognos Configuration.

    a. Select Local Configuration-→ Security -→ Cryptography -→ Cognos

    b. Change “Use third party CA?” to True.

    c. Save the configuration.

    d. Restart Cognos

12. Export the latest Cognos certificate into cognos.crt using the Admin CMD prompt:

    a. cd "`C:\Program Files\SANscreen"

    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias encryption

    c. For <password>, use the password from the */SANscreen/bin/cognos_info.dat* file.

13. Back up the DWH server trustore at`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Import the “c:\temp\cognos.crt” into DWH trustore to establish SSL communication between Cognos and DWH, using the Admin CMD prompt window.

    a. cd "`C:\Program Files\SANscreen"

    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password> -alias cognos3rdca

    c. For <password>, use the password from the */SANscreen/bin/cognos_info.dat* file.

15. Restart the SANscreen service.

16. Perform a backup of DWH to make sure DWH communicates with Cognos.

17. The following steps should be performed even when only the “ssl certificate” is changed and the default Cognos certificates are left unchanged. Otherwise Cognos may complain about the new SANscreen certificate or be unable to create a DWH backup.

    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`

    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore”`

```
-storepass <password> -alias “ssl certificate”
```

c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

Typically, these steps are performed as part of the Cognos certificate import process described in How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Copyright information

Trademark information