CA Spectrum®

Common Access Card Authentication Solution Guide

Release 9.4

CA Technologies Product References

This guide references CA Spectrum®.

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Common Access Cards and CA Spectrum Authentication

This section contains the following topics:

Introduction to Common Access Cards (CACs)

Within secure environments, the use of a single point of entry is required for easy access management. Without a single point of entry, administrators of secure environments must manage several programs with different security levels and requirements in addition to user access. Common Access Cards (CACs) provide a single point of entry by requiring the use of the CAC for access to all controlled resources.

How CACs Work

Each CAC contains certificates that are issued by certificate authorities. A managing authority, such as the ActivIdentity® ActivClient®, controls access to the CAC certificates. Managing authorities prevent the certificates that are contained within the CACs from being used outside of the CAC without first verifying the CAC owner.

The managing authority verifies the card owner by prompting the user of the CAC for a Personal Identification Number (PIN). If the PIN is verified, the managing authority allows access to the CAC Certificates.

The presentation of a CAC Certificate, however, is not sufficient to gain access to a resource. The CAC Certificate must first be checked for both authenticity and validity.

Certificate authenticity is checked by building a certificate path from the CAC Certificate through any intermediate certificates to a trusted root certificate. A chain of trust thus links the user certificate to the trusted root certificate. If this chain is properly built, the certificate is authentic. Certificate authorities provide intermediate and root certificates to administrators for this purpose.

Once a certificate is verified as authentic, validity checks are required. Certificate authorities can revoke CAC Certificates. Revocation invalidates the certificate, which renders the CAC that holds the certificate useless. This verification can be accomplished in *one* of the following two ways:

- Certificate Revocation Lists (CRLs) are the most common way to verify that a CAC is valid and are the industry standard.

  CRLs are flat files that contain the serial numbers of revoked certificates. They become outdated frequently because of constant additions. As a result, they expire at predetermined times and must be refreshed. CRLs also consume a great deal of memory and must be placed on the local file system. Generally administrators choose this option when they have no access to an OCSP server/responder.

- On-line Certificate Status Protocol (OCSP) eliminates the load times of CRLs by abstracting the information that is stored within them into a database.

  An OCSP server accepts requests to verify certificates. OCSP servers and responders are rarely outdated because administrators can revoke a certificate at any time. OCSP can be placed on a separate server from CA Spectrum.

Once a certificate has been verified as both authentic and valid, the CAC can be accepted.

How CA Spectrum CAC Authentication Works

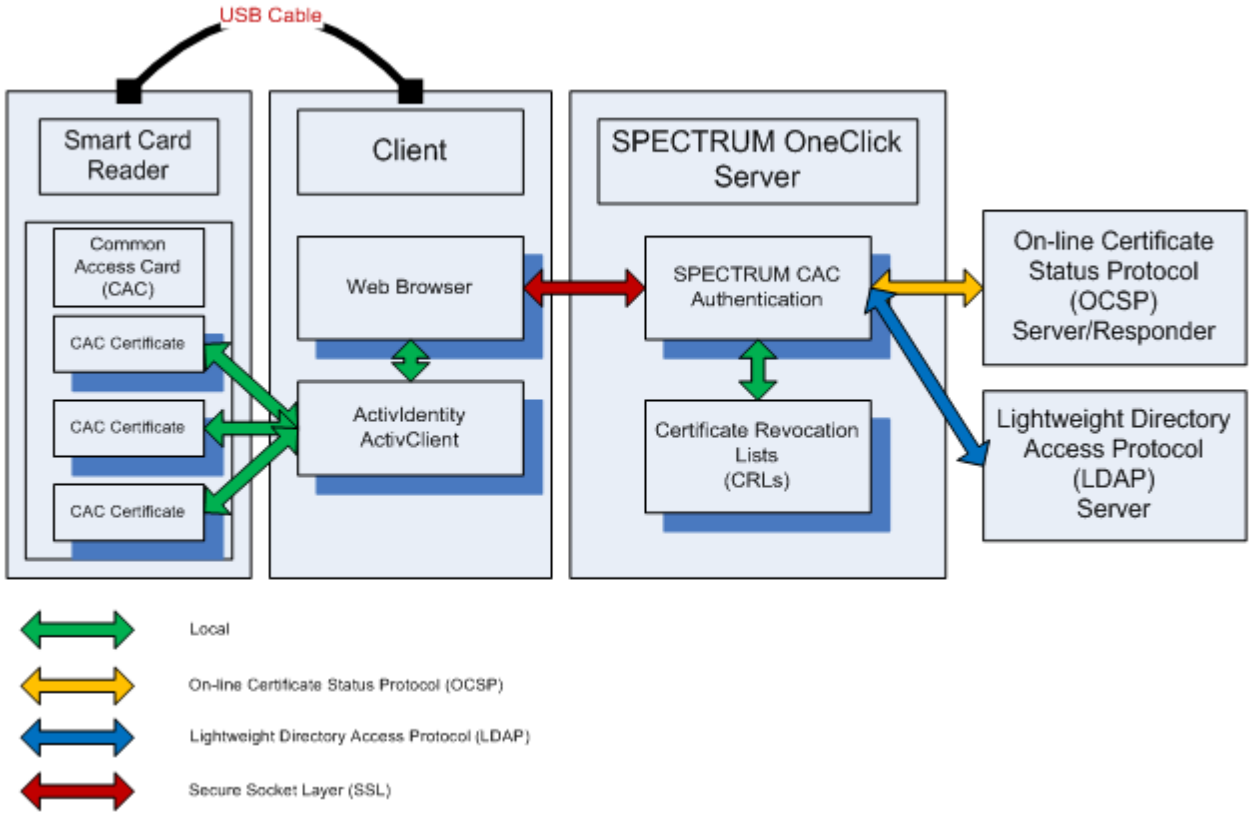
CA Spectrum CAC Authentication works by leveraging SSL, the Java PKIX Library, and any middleware that exposes PKSC11 to provide a complete CAC authentication solution.

Note: ActivIdentity ActivClient is an example of middleware that exposes PKSC11. We use this client to illustrate the CA Spectrum CAC authentication solution throughout this guide.

As part of SSL negotiation (if SSL is configured), clients that are connecting to the OneClick web server with ActivIdentity ActivClient installed have their CAC Certificates made available for authenticating automatically. Each user provides a CAC PIN to ActivIdentity. Once the PIN is verified, ActiveIdentity releases the CAC Certificate to the OneClick server. CA Spectrum CAC Authentication verifies that the uploaded CAC Certificate is authentic and valid. Verification consists of building a certificate path and validating the certificate against either Certificate Revocation Lists (CRLs) or an Online Certificate Status Protocol (OCSP) Server.

SSL negotiation is now complete. If LDAP for CAC has been configured, the directory is queried using a unique identifier that is derived from the CAC Certificate. The unique identifier acts as a key to acquire a username to enable login. If LDAP is not used, the user is prompted for a username and password to log in to CA Spectrum.

The following image shows the architecture for CA Spectrum CAC Authentication.



Supported Platforms

CA Spectrum CAC Authentication is available on the OneClick client for the Microsoft Windows and Red Hat Enterprise Linux platforms that CA Spectrum supports. CA Spectrum CAC Authentication can be configured on the OneClick server for all CA Spectrum-supported platforms.

Note: CA Spectrum CAC Authentication for the OneClick client on the Oracle Solaris platform is not supported. If you require CAC Authentication on Solaris, contact CA Support to open a product Enhancement Request.

The following list displays the tested combinations of OneClick client on Windows and the OneClick servers running on Windows, Red Hat Enterprise Linux, and Oracle Solaris platforms:

OneClick Clients: ■ Windows 7 64-bit ■ Windows XP 32-bit ■ Windows 2008 64-bit	**OneClick Servers:** ■ Windows 7 64-bit ■ Red Hat Enterprise Linux 5.9 (Server) 64-bit ■ Solaris 5.10 32-bit ■ Windows XP 32-bit
Middleware on Windows: HID Global ActivIdentity® ActivClient® 6.2 and 7.0	**Java Runtime Environment (JRE) versions:** JRE 1.6 and 1.7
Web Browser: Microsoft Internet Explorer version 8.0	

Note: The table summarizes the platform combinations that we tested. Our testing was constrained by our available resources. Other combinations might also be supported. For more information, contact CA Support.

Chapter 2: Configure CA Spectrum for SSL and CAC Authentication

This section contains the following topics:

How to Configure CA Spectrum for SSL and CAC Authentication

Note: The command-line actions that you perform during this process must be executed using the installation owner account. This account owns the CA Spectrum files.

To configure CA Spectrum for SSL and CAC Authentication, use the following process:

1. Gather and record the appropriate security certificate information (see page 12).
2. Verify that ActivIdentity ActivClient™, or other middleware that can expose PKSC11, has been installed on any client that will access OneClick.

   Note: For specific information about installing middleware, see the instructions for the middleware product.
3. Install CA Spectrum on your server and then reboot.

   Note: For more information about installing CA Spectrum, see the *Installation Guide*.
4. Add CA Spectrum users (see page 15).
5. Add Intermediate and Root certificates to CA Spectrum (see page 16).
6. Configure the secure socket on the OneClick server (see page 17).
7. Configure CAC Authentication from the OneClick client (see page 19).
8. Enable CA Spectrum CAC Authentication (see page 24).
9. Verify that CAC is functional. Log in to the CAC Authentication web page and launch the OneClick Console on Windows.
10. (Optional) Configure Linux clients (see page 26).

Gather Security Certificates and Information

Before you can start setting up CA Spectrum CAC Authentication, verify that you have the appropriate security certificates and security information readily available to you. Start by gathering the required certificate and security information.

Follow these steps:

1. Import the certificate for the OneClick server as follows:
   - (Optional) Generate a self-signed certificate for the OneClick server (see page 13) if you do not already have one.
   - (Optional) Import an existing self-signed certificate for the OneClick server (see page 14).
   - (Optional) Import an existing private key and certificate for the OneClick server (see page 14).
2. Gather root and intermediate certificates for the CACs.
3. Determine the method that you plan to use for CAC verification. Record the information that is indicated for your selection as appropriate:

   OCSP AIA

   Retrieves the parameters of the OCSP server from the certificate on the Common Access Card from the “AIA extension” of the certificate. The OCSP responder certificate is required.

   OCSP Server

   Uses a URL to access the OCSP server and a certificate for the specified server. The OCSP responder certificate and the OCSP responder URL are required.

   CRL Directory

   Uses a path to the directory which contains CRL files. The full path to the directory containing CRLs is required.

   CRL URL

   Specifies a list, separated by spaces, of full URLs to the CRL files that are provided by the web server. The full URL to each CRL is required.

   CRL Distribution Point

   Specifies that CA Spectrum retrieves the information about the web location of the CRL files from the certificate itself.

   Note: For more information about these options, see How CACs Work (see page 7).

4. (Optional) If you are using Lightweight Directory Access Protocol (LDAP), collect the following information:
   - Hostname
   - Port
   - Base distinguished name
   - User distinguished name
   - User password
   - EDIPI attribute name
   - LDAP server certificate (if you plan to enable SSL)
   - Field name to map ID to
   - Field from which to extract the CA Spectrum Username

   For mapping from the certificate to LDAP:

   - Decide whether ID information on the card certificate (EDIPI or another type of the ID) will come from the subject, alternative name, or rfc822 name.
   - Create a parsing rule to extract ID information from the card.

Generate a Self-Signed Certificate

If you do not already have a certificate, generate a self-signed certificate on the OneClick server.

Follow these steps:

1. Open a command prompt/shell and change the directory to: <*SPECROOT*>/Java/bin.
2. Run the "keytool" program with the following arguments:

   ```
   -genkey -alias tomcatssl -keyalg RSA -keystore
   <SPECROOT>/custom/keystore/cacerts
   ```

3. Enter **changeit** for the -keystore password.

   Note: The word 'changeit' is the default password for the keystore.

4. Complete the fields. The following fields are not self-explanatory:

   First+Last name

   Specifies the fully qualified domain name of your OneClick server. For example, "myhostname.mydomain".

   Organizational Unit

   Specifies your company division. For example, Spectrum Engineering.

   Organization

   Specifies the company name. For example, CA Inc.

5. Verify that your information is correct, and type 'yes' to accept.
6. Press Enter to use the same password as the keystore.

Import an Existing Self-Signed Certificate for the OneClick Server

If you already have a certificate, you must import it for CA Spectrum CAC Authentication.

To import the existing certificate for CA Spectrum CAC Authentication

1. Change the directory to: <SPECROOT>/Java/bin.
2. Run the following command:

   `./keytool -importcert -alias tomcatssl -file` *`cert_file`* `-keystore <SPECROOT>/custom/keystore/cacerts`

   cert_file

   Specifies the existing OneClick certificate file.

3. Type **changeit** for the keystore password.
4. Press Enter to use the same password as the keystore.

Import an Existing Private Key and Certificate for the OneClick Server

Important! This procedure destroys your existing cacerts keystore and creates a new one with your private key and certificate. At present, you cannot force a private key into an existing keystore. This procedure is the only way to create a new keystore with a preexisting private key.

Follow these steps:

1. Gather the private key and the certificate files.
2. Change the directory to a temporary directory.

3. Execute the following command:

   ```
   openssl pkcs12 -export -inkey <private_key_file> -in <server_cert_file> -out mycert.pfx -name "default"
   ```

4. Change to the following directory:

   <*SPECROOT*>/Java/bin

5. Execute the following command:

   ```
   keytool -importkeystore -srckeystore <path_to_mycert.pfx> -srcstoretype pkcs12 -destkeystore <SPECROOT>/custom/keystore/cacerts -srcalias default -destalias tomcatssl -destkeypass changeit
   ```

   Your private key and server certificate are now stored in the keystore, which is located in the following directory:

   <*SPECROOT*>/custom/keystore/cacerts

Add CA Spectrum Users

You can add CA Spectrum users from the CA Spectrum Control Panel.

Note: For more information, see the *Administrator Guide*.

Follow these steps:

1. Open the CA Spectrum Control Panel using *one* of the following methods depending on the platform you are using:
   - Linux/Solaris: /usr/SPECTRUM/bin/SCP
   - Windows: Start, Program Files, CA, CA Spectrum Control Panel.
2. Click Start SpectroSERVER.

   The SpectroSERVER starts.
3. Select Control, Users from the main menu.

   The Users dialog opens.
4. Click Create to create the desired user.

   The Create dialog opens.
5. Type the user's name in the User Name field.

   Note: If you are using LDAP, user names in CA Spectrum must exactly match those in LDAP.
6. Type a password in the New Password and Confirm New Password fields.

   Note: This password is only used if LDAP is not enabled.

7. Click OK.

   The Create dialog closes.

8. Click Close.

   The CA Spectrum user is created.

Add Intermediate and Root Certificates to CA Spectrum

Use the SSL Certificates administration page to load root and intermediate certificate authority certificates for the CACs.

Note: For more information, see the *Administrator Guide*.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.

2. Click SSL Certificates in the left side panel.

   The SSL Certificates page opens.

3. Load the root or intermediate certificate authority Certificates for the CACs in the 'File with Certificate' field.

4. Enter an appropriate alias name of your choice.

5. Click Save.

   Note: Restarting the OneClick server is not required after you load each separate certificate. You can wait until you have loaded all of the desired certificates.

6. Repeat Steps 3-5 for every certificate you want to load.

7. (Optional) Load the Online Certificate Status Protocol (OCSP) Responder Certificate if you are using (OCSP).

   Note: Record the name of the certificate alias that is associated with this certificate. The alias name is a requirement for a later step.

8. (Optional) Load the LDAP certificate if you are using SSL to connect to the LDAP server.

9. Click Restart OneClick Server after you have loaded all of the appropriate certificates.

Configure the Secure Socket on the OneClick Server

As a final step in configuring the OneClick web server for SSL, configure the secure socket on the OneClick web server host.

Follow these steps:

1. Shut down the OneClick web server:

   Linux or Solaris

   As root: <*$SPECROOT*>/tomcat/bin/stopTomcat.sh

   Windows

   Enter the following command from a command prompt:

   ```
   C:\> net stop spectrumtomcat
   ```

2. Open <*$SPECROOT*>/tomcat/conf/server.xml in a text editor.

3. Locate the following section in the server.xml file:

   ```
   <!-- Define a SSL Coyote HTTP/1.1 Connector on port 443 -->
       <!--
       <Connector
              port="443" minProcessors="5" maxProcessors="75"
              enableLookups="true" disableUploadTimeout="true"
              acceptCount="100" debug="0" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS"
              keystoreFile="<SPECROOT>/custom/keystore/cacerts"
              keystorePass="changeit">
        </Connector>
       -->
   ```

   By default the <Connector> element in the section is commented out.

   Note: The preceding XML fragment is Windows-specific. This example specifies 443 as the default port where the OneClick web server listens for SSL communications. You can omit the port from the URL for accessing the OneClick home page:

   ```
   https://<fully_qualified_host_name>/spectrum
   ```

   On a UNIX-based installation, the OneClick web server is not run as root, and the default port is 8443 (it must be greater than 1024).

4. Specify the port number in the web browser when you enter the URL to access the OneClick home page:

   ```
   https://<fully_qualified_host_name>:8443/spectrum
   ```

5. Remove the comments around the Connector definition. Make the definition active by deleting the “<!--” and “-->” tags that surround this section.
6. Replace <*$SPECROOT*> with the actual path as follows:

   Linux

   /usr/SPECTRUM

   Windows

   C:/win32app/SPECTRUM
7. Change clientAuth to “true”.

   Note: Changing this setting to "true" is a key component of the CA Spectrum Common Access Card solution. You can configure CA Spectrum for SSL without ClientAuth. However, this parameter must be set to "true" to enable CA Spectrum Common Access Card authentication. For more information, see the *Administrator Guide*.
8. Save and close the server.xml file.
9. Start the OneClick web server using one of the following commands, depending on the platform you are using:

   Linux or Solaris

   As root:

   <*$SPECROOT*>/tomcat/bin/startTomcat.sh

   Windows

   From a command prompt:

   ```
   C:\> net start spectrumtomcat
   ```

   The secure socket is now configured.

Configure CAC Authentication on the OneClick Client

After configuring CA Spectrum for SSL, configure CAC Authentication on the OneClick client. You can set up CAC Authentication by entering all of the relevant security information you have gathered.

Follow these steps:

1. Log in to the OneClick client that has ActivIdentity ActivClient installed.
2. Open the OneClick Administration pages using the SSL port as follows:
   - For Linux/Solaris, type **https://your_hostname:8443/**
   - For Windows, type **https://your_hostname/**
3. Provide your CAC Certificate.

   Note: The CAC certificate that you provide here is used to verify that the CAC Configuration is valid. For more information, see Enable CA Spectrum CAC Authentication.
4. (Optional) Accept the OneClick Server Certificate if prompted.
5. Enter the installation owner user name and password when prompted.

   Note: If you have not changed the password for the installation owner, it is *spectrum*.

   The OneClick home page opens.
6. Click Administration.

   The Administration Pages open.
7. Click CAC Configuration in the left side panel.

   The CAC Configuration page opens.

   Note: If you do not see a full web page here with options available, you did not use the SSL port. Repeat Steps 1 through 6.

CAC Configuration Page

Use the CAC Configuration page to configure OneClick to use Common Access Cards (CAC) for authentication.

Choose CAC Option

Specifies whether to enable or disable the CAC authentication solution.

Disable CAC

Disables CAC authentication.

Enable CAC

Enables CAC authentication.

The Trusted Keystore section contains the following fields:

Trusted Keystore password

Specifies the password to use for accessing the Trusted Keystore: **changeit**.

Re-enter Trusted Keystore password

Confirms the password for accessing the Trusted Keystore.

The Revocation System section specifies how you want CA Spectrum to determine whether a CAC has been revoked. Select *one* of the following options:

Enable OCSP AIA

Instructs CA Spectrum to retrieve the parameters of the OCSP server from the certificate on the Common Access Card from the “AIA extension” of the certificate.

Enable OCSP Server

Specifies that the user must provide a URL to access OCSP server and a certificate for this server.

Enable CRL Directory

Specifies that a path to the directory that contains CRL files is required.

Enable CRL URL

Specifies a list, separated by spaces, of full URLs to the CRL files that the web server provides.

Enable CRL Distribution Point

Specifies that CA Spectrum retrieves the information about the web location of the CRL files from the certificate itself.

The OCSP AIA Connectivity section appears when you select Enable OCSP AIA in the Revocation System section. This section contains the following option:

Test OCSP AIA

Verifies that OCSP AIA is working properly.

The OCSP Server Connectivity section appears when you select Enable OCSP Server in the Revocation System section. This section contains the following options:

OCSP Server URL

Specifies the complete URL for accessing the OCSP Responder. The complete URL is used because many OCSP Responders are servlets running on a larger OCSP server.

OCSP Server Certificate Alias

Specifies the certificate for the specified OCSP server.

Test OSCAP Server

Tests the connection to the OCSP server based on the credentials that you entered.

The Certificate Relocation Lists appears when you select Enable CRL Directory or Enable CRL URL in the Revocation System section. It contains the following settings, depending on the CRL option that you selected:

CRL Directory

Specifies the full path to the directory that contains the CRL files for verifying user certificates.

CRL URL

Specifies a list of full URLs, separated by spaces, to the CRL files that the web server provides.

Test CRL Availability

Attempts to load the CRLs in the specified directory.

The LDAP Username Lookup section contains the following settings:

Enable LDAP

Enables LDAP.

LDAP Server Hostname

Specifies the host name of an LDAP server that contains users that correspond to user certificates.

LDAP Server Port

Specifies the port number for accessing the LDAP server.

Enable SSL

Enables secure connecting to the LDAP server using SSL.

Note: Load the LDAP server certificate if you enable SSL.

LDAP Base DN

Specifies the LDAP base distinguished name.

LDAP User DN

Specifies the distinguished name (DN) of the user that is used to query the LDAP server.

LDAP User Password

Specifies the password of the user that is used to query the LDAP server.

Re-enter LDAP User Password

Confirms the LDAP user password.

Certificate's EDIPI Field

Specifies the source for user ID information. Select *one* of the following options, which describe the format in which EDIPI is stored in the CAC certificate:

- Subject
- SubjectUniqueId
- AltName.otherName
- AltName.rfc882Name

EDIPI Extraction Rule

Specifies the rule to use to extract EDIPI from the CAC certificate field.

Type: Java regular expression

Example: The default value for this field is as follows:

```
"CN=\w*\.\w*\.(\d+),";
```

This string defines a rule that matches a string that resembles the following example:

```
CN=aaaa.bbbbbb.1233454,xxxxxxxxxxxxxxxx
```

- Literal “CN=”
- Any word (possibly empty) \w*
- Literal “.”
- Any word (possibly empty) \w*
- Literal “.”
- Integer number (non-empty) \d+

- Literal “,”
- Anything can follow.

Note: Regex *capturing group* must be defined in the regular expression. CA Spectrum uses the first defined group in the expression to extract unique user ID information. More information about capturing groups is available on the Internet.

LDAP EDIPI Attribute Name

Specifies the name of the LDAP field that is used to store EDIPI (or other unique identifier) information.

LDAP Username Attribute Name

Specifies the name of the LDAP field that is used to store CA Spectrum user name information.

LDAP Referral Setting

Specifies how OneClick handles LDAP referrals.

follow

(Default) Instructs OneClick to automatically follow any referrals.

throw

Instructs OneClick to throw an exception for each referral. The request is likely to fail with an "Unprocessed Continuation Reference(s)" error.

ignore

Instructs OneClick to ignore referrals. The request is likely to fail with an "Unprocessed Continuation Reference(s)" error.

Note: LDAP Referral Setting is hidden by default on the CAC Configuration page. To display this field and change its value, see Modify LDAP Referral Setting (see page 23).

Test LDAP Server

Attempts to connect to the LDAP server using the credentials that you supplied.

Modify LDAP Referral Setting

The LDAP Referral Setting specifies how OneClick handles LDAP referrals. When an LDAP server cannot locate a requested object, the server returns a referral to the client. The referral directs the request to another server to locate the object. By default, OneClick automatically follows referrals to obtain the requested information.

You can also specify to ignore referrals or to throw an exception for each referral. The LDAP Referral Setting is hidden by default on the CAC Configuration page. To modify its value, change the configuration file to display the field.

Follow these steps:

1. Open <*$SPECROOT*>/tomcat/webapps/spectrum/WEB-INF/cac/cac-config.jsp in a text editor.
2. Uncomment the LDAP Referral Setting display code:
   a. Add "-->" after <!-- BEGIN HIDDEN REFERRAL SETTING SECTION
   b. Add "<!--" before END HIDDEN REFERRAL SETTING SECTION -->
3. Save and close the file.
4. Refresh the CAC Configuration page.

   The LDAP Referral Setting field appears.
5. Select a value from the LDAP Referral Setting drop-down list, and click Save.

   The new LDAP Referral Setting takes effect.

Enable CA Spectrum CAC Authentication

After you have configured CA Spectrum CAC Authentication on the OneClick server (see page 19) and have finished setting up security, you can enable it from the CAC Authentication page.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.
2. Click CAC Configuration in the left panel.

   The CAC Configuration page opens.
3. Click Enable CAC.

   The available configuration options for enabling CAC are displayed.
4. Enter the keystore password in the keystore password fields.

   Note: If you have not changed the keystore password, it is *changeit*.

5. Select one of the following options in the Revocation System section. These options specify how CA Spectrum determines whether a CAC has been revoked. Complete the resulting fields:

   Enable OCSP AIA

   Instructs CA Spectrum to retrieve the parameters of the OCSP server from the certificate on the Common Access Card from the "AIA extension" of the certificate.

   Enable OCSP Server

   Specifies that the user must provide a URL to access the OCSP server and a certificate for this server.

   Enable CRL Directory

   Specifies that a path to the directory that contains CRL files must be specified.

   Enable CRL URL

   Specifies a list, separated by spaces, of full URLs to the CRL files that are provided by the web server.

   Enable CRL Distribution Point

   Specifies that CA Spectrum retrieves the information about the location of the CRL files from the certificate itself.

   The CAC Configuration page changes to display the fields that relate to the option that you selected. For more information, see CAC Configuration Page (see page 20).

6. (Optional) If you are using LDAP, select the Enable LDAP check box, and complete the fields as described in CAC Configuration Page (see page 20).

7. Click the individual test buttons to test your information.

8. Click Save to save your selections.

   A full test of your CAC configuration options runs. If the test is successful, the CAC information is saved, and the OneClick server restarts.

   If you are using CRLs, they are loaded immediately after the restart. Depending on the number of CRLs and their size, this process can take several minutes. During this time, attempts to access the server using a web browser do not always provide feedback.

9. (Optional) Track the progress of the load operation by viewing one of the following logs:

   - *$SPECROOT*/tomcat/logs/catalina.out for Linux/Solaris
   - *$SPECROOT*/tomcat/logs/stdout.log for Windows

More information:

Gather Security Certificates and Information (see page 12)
Add Intermediate and Root Certificates to CA Spectrum (see page 16)

Configure Linux Clients

If any users are accessing CA Spectrum from Linux clients, configure those clients for CA Spectrum CAC Authentication.

Follow these steps:

1. Run mkoctar script on the OneClick server by doing the following:
   a. Set the environment variable SPECROOT to the SPECTRUM root directory.
   b. Navigate to <*$SPECROOT*>/tomcat/webapps/spectrum/
   c. Run the following command:

      ./mkoctar –servercert <*oneclick_certificate_alias*> -cert <*root_alias*> -cert <*int_alias_1*> -cert <*int_alias_2*>

      –servercert <oneclick_certificate_alias>

      Specifies the alias for the OneClick web server certificates. If you created a self-signed certificate, the OneClick certificate alias is "tomcatssl".

      -cert <root_alias>

      Specifies the alias for the root certificate, as defined in Add Intermediate and Root Certificates to CA Spectrum (see page 16).

      -cert <int_alias_1>

      Specifies the alias for the first intermediate certificate, as defined in Add Intermediate and Root Certificates to CA Spectrum (see page 16).

      -cert <int_alias_2>

      Specifies the alias for the second intermediate certificate, as defined in Add Intermediate and Root Certificates to CA Spectrum (see page 16).

   d. (Optional) Run the following command if you see a Permission Denied error:

      chmod +x mkoctar

   e. (Optional) Run the following command to view additional options:

      ./mkoctar -h

   This command produces the file "oc.tar" in the same directory. You can now copy oc.tar to a temporary directory on Linux clients that will access OneClick.

2. On the Linux client, extract oc.tar as follows:

   Note: For performance and security reasons, extract this file to a local disk, not to a network drive.

   a. Run the following command:

      tar xvf oc.tar

   b. Edit the line in card.config.Linux that begins with "library=". Change it to point to the ActivIdentity pkcs library. For example, change it to the following line:

      ```
      library =
      /usr/local/ActivIdentity/ActivClient/lib/libacpkcs211.so
      ```

   c. Run the runoc script to launch OneClick. Take *one* of the following steps:

      - LDAP: Run the following command:

        ./runoc

      - Non-LDAP: Run the following command:

        ./runoc –noldap

      When it is first run, runoc installs a JRE in the current directory.

Note: Users are always prompted for their CAC Personal Identification Number (PIN). If you are not using LDAP, users are also prompted for their user name and password.

Chapter 3: Working with CA Spectrum CAC Authentication

This section contains the following topics:

About Working with CA Spectrum CAC Authentication

Once CA Spectrum CAC Authentication is enabled, the only visible change to the user interface is the new CAC Configuration page in the OneClick Administration pages.

Non-SSL access is completely disabled after CA Spectrum CAC Authentication has been enabled. Any attempts to access the server from a non-secured port will cause a redirection to the SSL port.

About Memory Consumption Using CA Spectrum CAC Authentication with CRLs

A single CRL can hold more than half a million revoked certificate serial numbers. Some environments require 20 or more CRLs to cover all potential user certificates. Loading this much data consumes a great deal of time and memory. For example, a set of CRLs that is approximately 100 MB on disk consumes about 1.5 GB of memory and takes several minutes to process.

Take this increased memory consumption into account when you decide where to install OneClick. An easy way to calculate the memory consumption is to take the total size of your CRLs and multiply by 15. One MB of CRLs consumes 15 MB of memory, and 50 MB consumes 750 MB of memory. If your total exceeds 400 MB, consider increasing the amount of memory that is available to OneClick. If your total exceeds 500 MB, OneClick typically requires increased memory to function.

Important! If your total CRL memory requirement exceeds 1 GB, do not run CA Spectrum CAC Authentication with CRLs on a Windows server.

The steps to take to increase the amount of memory that is available to the OneClick server are described in Configure OneClick Web Server Memory Settings (see page 30).

To alleviate the time impact on end users, CRLs are loaded while OneClick is initializing. Users of OneClick do not experience significant delays once OneClick is running. You can track the progress of the CRL load operation by viewing the OneClick log file at one of the following locations:

Linux/Solaris

<*SPECROOT*>/tomcat/logs/catalina.out

Windows

<*SPECROOT*>\tomcat\logs\stdout.log

Configure OneClick Web Server Memory Settings

By default, the maximum memory that the OneClick web server uses is 1024 MB. If the OneClick web server is using more than 75 percent of its configured maximum memory, consider increasing the maximum memory value.

If the web server runs out of memory, an OutOfMemory error appears in the following log files:

- tomcat/logs/stdout.log (for Windows)
- tomcat/logs/catalina.out (for Linux/Solaris).

You can change memory allocations on the Web Server Memory Administration page. Test with a modest adjustment, such as a 25% increase in the maximum memory allocation, to 1280 MB. The steps in this procedure are an optional method for addressing out-of-memory issues.

Note: Restart the OneClick web server for these changes to take effect.

Follow these steps:

1. Verify the OneClick web server memory usage:
   a. Click Administration in the OneClick home page.

      The Administration Pages open.

   b. Click Web Server Memory in the left panel.

      The Web Server Memory page opens.

   c. Check the OneClick Server Memory Usage field to verify if memory usage is greater than 75 percent of the configured maximum.

2. Configure the maximum OneClick web server memory usage:
   a. In the Maximum Memory the Server Can Use (In MB) field, enter the new value.

      Note: Do not set the maximum memory to a value larger than the available memory for the system.

   b. Click Save.

      A dialog prompts you to commit your changes and restart the OneClick web server.

   c. Click OK.

      Your changes are saved, and the OneClick web server is restarted.

Changes to Access Security

If any part of the CAC certificate verification process fails, the user cannot be granted access. Allowing a user to log in without a validated CAC would defeat the purpose of enabling CAC Authentication.

If LDAP is up, but a user name is not returned properly or the returned user name is not in CA Spectrum, the user cannot be granted access. This is because user access is still controlled by CA Spectrum, and allowing someone who has a valid CAC but an invalid user name to log in as anyone is not secure.

Chapter 4: Troubleshooting

This section contains the following topics:

Java Heap Size and OutOfMemory Errors

Symptom:

I am seeing errors such as "Java Heap Size" and "OutofMemory" when I use CA Spectrum CAC Authentication with CRLs.

Solution:

The memory of your OneClick server is set too low. Complete the following procedure to avoid seeing these errors.

1. Remove a few CRLs from your CRL directory.
2. Restart the OneClick server.
3. Increase the amount of memory available on the server as described in Configure OneClick Web Server Memory Settings (see page 30).
4. Try using CA Spectrum CAC Authentication again.

   Note: If you continue to get this error, you may not have enough memory to run CA Spectrum CAC Authentication with CRLs.

OneClick Client Locks Up After Authentication

Platform: Linux only

Symptom:

I am using CAC authentication for my OneClick clients, which I launch on a Linux server. After I invoke the runoc script, the client fails soon after startup. The OneClick client locks up and becomes unusable. Sometimes, I see a certificate error. I am forced to exit the application. After a few attempts, the client starts and runs as expected.

Solution:

This situation occurs when the SSL connection between the OneClick client and the Tomcat server times out before the SSL handshake has completed.

To resolve this issue, increase the timeout period that is set on the client and on the Tomcat server. On Linux, clients use a script (runoc) to launch OneClick. You can modify the -ssltimeout parameter in this script so that SSL has more time to complete the handshake. The longer timeout lets the handshake complete while the connection is still established.

First, reconfigure the server to use a five-minute connection timeout.

Follow these steps:

1. Navigate to *$TOMCAT_ROOT*/conf/
2. Open the file server.xml for editing, using your preferred text editor.
3. Locate the SSL Connector element in the file.
4. Change the connectionTimeout parameter to use a value equivalent to five minutes in milliseconds:

   `connectionTimeout="300000"`

   Note: The server setting is in milliseconds.
5. Restart the OneClick server so that the change takes effect.

Now launch the OneClick client using the new -ssltimeout parameter.

Follow these steps:

1. Navigate to the directory from which you launch the runoc script on the OneClick client. For example, /opt/CA_OC.
2. Invoke the runoc script, using the -ssl timeout parameter. For example, enter the following command:

   `./runoc –ssltimeout <value>`

   In this example, use a value of 300 (the equivalent of five minutes in seconds).

   Note: The client setting is in seconds.

   The OneClick client now has a five-minute timeout setting, which matches the timeout that you set on the tomcat server.

Poor OneClick Client Performance

Platform: Windows

Symptom:

The OneClick clients take a long time to start up. Once the clients have started, users experience long wait times for the user interface to react to mouse clicks and navigation tasks. They are so slow that we can hardly use them.

Solution:

This behavior results from the default setting for the "reuseConnections" Java System property, which is "false". In previous versions of CA Spectrum, the default value was "true". A change was made to facilitate out-of-the-box connectivity for users with web proxies or load balancers in their environment. Without reusing connections, SSL certificate verification is performed for every request from client to server. This work is expensive, in terms of round-trip times.

Change the value of the "reuseConnections" Java Runtime System property to "true".

To change the property setting, edit the oneclick.jnlp file.

Follow these steps:

1. Navigate to the following directory:

   `<$SPECROOT>/tomcat/webapps/spectrum/`

2. Open the oneclick.jnlp file for editing using your preferred text editor.
3. Add the following line, immediately below the "<resources>" line:

   `<property name="reuseConnections" value="true"/>`

4. Restart all open OneClick clients.

Poor OneClick Client Performance (Linux)

Platform: Linux

Symptom:

The OneClick clients take a long time to start up. Once the clients have started, users experience long wait times for the user interface to react to mouse clicks and navigation tasks. They are so slow that we can hardly use them.

Solution:

This behavior results from the default setting for the "reuseConnections" Java Runtime System property, which is "false". In previous versions of CA Spectrum, the default value was "true". A change was made to facilitate out-of-the-box connectivity for users with web proxies or load balancers in their environment. Without reusing connections, SSL certificate verification is performed for every request from client to server. This work is expensive, in terms of round-trip times.

Change the value of the "reuseConnections" Java runtime property from "false" to "true".

To change the property setting for Linux clients, edit the runoc script.

Follow these steps:

1. Navigate to the directory where you installed the runoc script.
2. Add "-DreuseConnections=true" to the last line of the script as follows:

   ```
   $JRE_HOME/bin/java -DreuseConnections=true -classpath
   ```

3. Save the script.
4. Restart all open OneClick clients.

Unable to Build Certificate Path

Symptom:

I am seeing the error "Unable to Build Certificate Path".

Solution:

This error occurs when SSL is set up, but the option for Client Authentication is not set to “true”. In this case when someone attempts to access a OneClick server with CA Spectrum CAC Authentication, they do not present a CAC certificate ahead of time. As a result, CA Spectrum CAC Authentication attempts to build a certificate path, but no certificates are available.

Refer to Configure the Secure Socket on the OneClick Server (see page 17). Verify that you have set clientAuth to “true”, and restart the OneClick server.

Unable to Determine Certificate Status

Symptom:

I am seeing the error "Unable to Determine Certificate Status".

Solution:

This error is usually presented when CRLs have expired. Acquire new CRLs from the Certificate Authority and replace the old CRLs. Then restart the OneClick server.

Certificate Has Been Revoked

Symptom:

I am seeing the error "Certificate Has Been Revoked".

Solution:

This error indicates that the CAC Certificate has been revoked. The revocation occurred either by an entry in a CRL or because the OCSP Responder has indicated that the certificate is no longer valid.

Index