Symantec™ Managed PKI®

Integration Guide for ActiveSync®

Symantec

Symantec™ Managed PKI® Integration Guide for ActiveSync®

Last updated March 28, 2013

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/contact/index.html#support4

Contents

Chapter 1

Integrating Managed PKI Certificates with Microsoft® ActiveSync®

Managed PKI certificates can be integrated with many common applications to enable secure communications and online access. This document describes how to integrate Managed PKI certificates with Microsoft® ActiveSync® to enable S/MIME (with or without userID and password authentication) using certificate mapping.

Pre-requisites

This integration has been qualified on the following platform:

- Microsoft Exchange ActiveSync® 14
- Windows® 2008 Server R2 64-bit Standard or Enterprise edition
- Microsoft Exchange® Server 2010
- Microsoft Internet Information Services® (IIS) 7.5

Integration Overview

Integrating Managed PKI certificates with ActiveSync consists of the following general steps:

- "Prepare for Certificate Mapping for ActiveSync" on page 1
- "Map Certificates" on page 5
- "Test ActiveSync" on page 7

Prepare for Certificate Mapping for ActiveSync

To prepare certificate mapping for ActiveSync, you configure ActiveSync and Exchange to enable certificate mapping for Active Directory (AD). Note the following special considerations:

- Your Exchange server and ActiveSync must be configured for userID and password.
- The Exchange server must be a member of a domain.
- The CDP for certificates issued by Managed PKI and which map to ActiveSync must be reachable without going through a proxy. If your client certificates are missing, the CDP is not available, or if the CRL cannot be accessed, certificate mapping will fail.
- To check if your CDP is not available, refer to the procedures in "Verifying if the CDP is Available" on page 9.

Note: If you are unable to reach the CRL without going through a proxy, you can set the web server to run as an administrator. Refer to the instructions at http://support.microsoft.com/kb/294305. However, running the web server as an administrator is not recommended.

Configure ActiveSync to Request Certificates

1. Open the Exchange Management console.
2. Click on **Server Configuration** → **Client Access** → **Exchange ActiveSync** → **Properties**.
3. Select the **Authentication** tab.

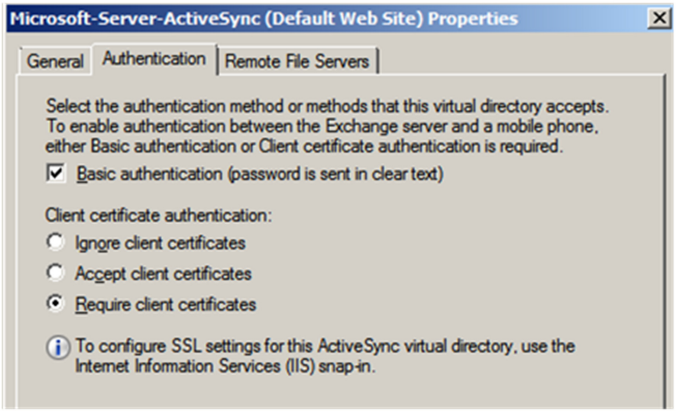

Figure 1-1 Microsoft-Server-ActiveSync Properties dialog box

- To enable certificate and userID/password authentication, select **Basic authentication (password is sent in clear text)** and **Require client certificates**.
- To enable certificate authentication only, select **Require client certificates**.

Configure ActiveSync to Map Certificates to Active Directory

1. The ability to map certificates to Active Directory is typically not enabled by default. You must enable this manually. Refer to the Active Directory documentation or Microsoft for instructions. Make sure that the following Authentication options are enabled:

a At the top level, enable **Active Directory Client Certificate** and **Anonymous Authentication**.

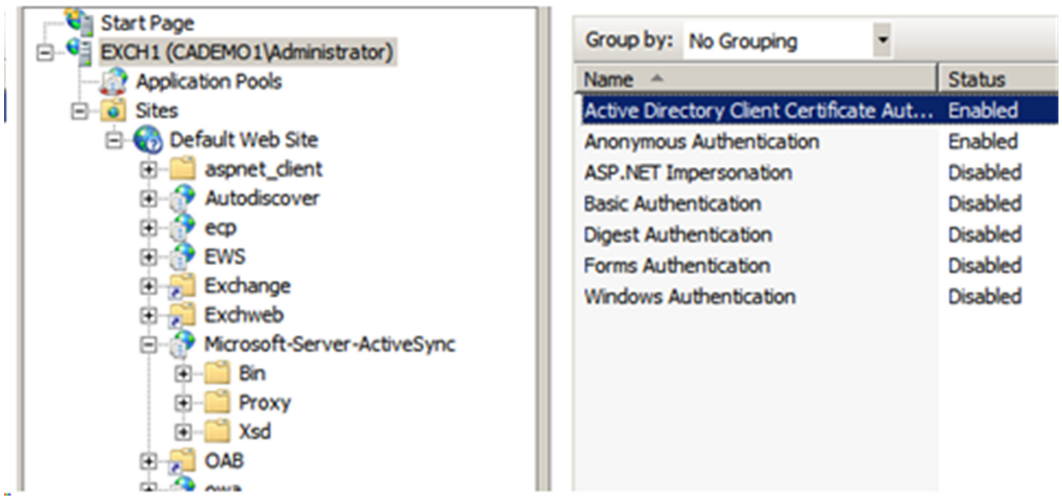

Figure 1-2 Top-level authentication method settings

b At the Microsoft-Server-ActiveSync level:

- Enable basic authentication for certificate and userID/password authentication.
- Disable all authentication methods for certificate only authentication.

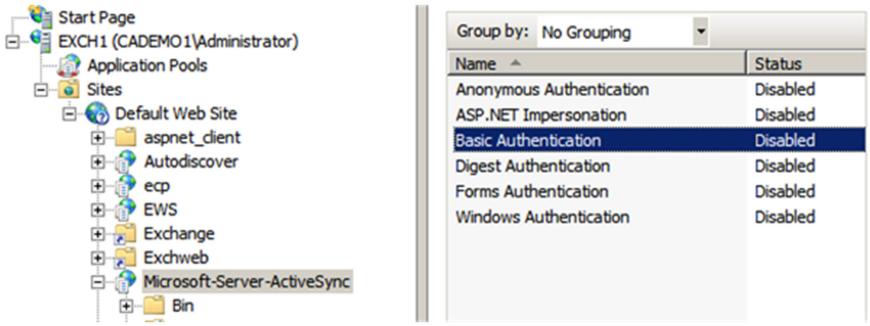

Figure 1-3 Microsoft-Server-ActiveSync-level authentication method settings

2 Using a POWERSHELL, run the following commands to enable mapping to occur at the ActiveSync level. This can be done manually or programmatically.

```
C:\Windows\SysWOW64\inetsrv\appcmd.exe unlock config /section:client
CertificateMappingAuthentication
```

The command will return the following response:

```
Unlocked section "system.webServer/security/authentication/client
CertificateMappingAuthentication" at configuration path "MACHINE/
WEBROOT/APPHOST".
```

```
C:\Windows\SysWOW64\inetsrv\appcmd.exe set config "Default Web Site/
Microsoft-Server-ActiveSync" -section:clientCertificateMapping
Authentication /enabled:true
```

The command will return the following response:

```
Applied configuration changes to section "system.webServer/security/
authentication/clientCertificateMappingAuthentication" for "MACHINE/
WEBROOT/APPHOST/Default Web Site/Microsoft-Server-ActiveSync" at
```

```
configuration commit path "MACHINE/WEBROOT/APPHOST/Default Web Site/
Microsoft-Server-ActiveSync"
```

3 Restart the World Wide Web Publishing Service. From the **Start** menu, click **Administrative Tools**→ **Services** → **World Wide Web Publishing Service** → **Restart**.

Configure IIS and ActiveSync to Trust a Third Party CA

Complete the following steps on the system that hosts Exchange and ActiveSync to establish a trust relationship with the IIS server.

1 Open the Microsoft Management Console (MMC).

2 Click **File** → **Add/Remove Snap-in...**.

3 Select the Certificate snap-in for the Computer account on the local computer and click **OK**.

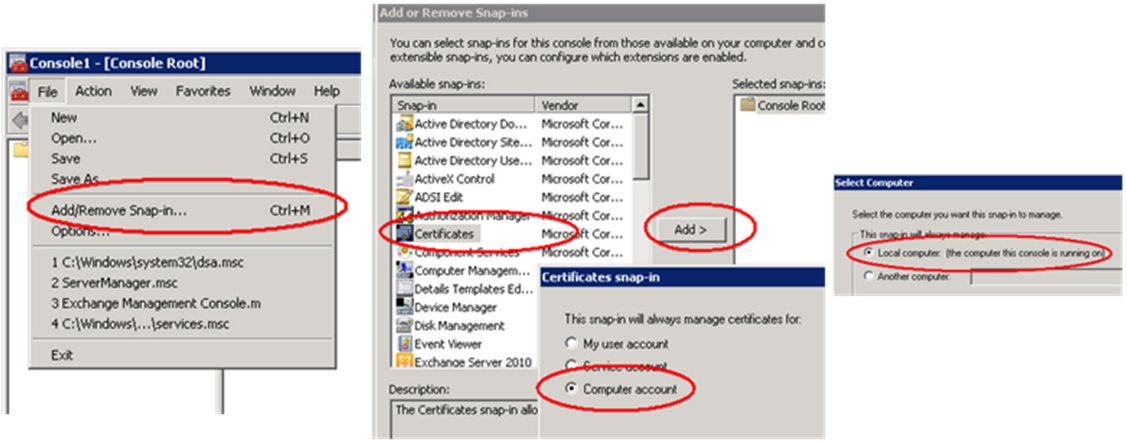

Figure 1-4 Selecting the Certificate snap-in for the Computer account on the local computer

4 Double-click **Certificates (Local Computer)**.

5 Double-click **Trusted Root Certificate Authorities**.

6 Right-click on the **Certificates** folder under **Trusted Root Certification Authorities** and click **All Tasks**.

7 Select **Import**.

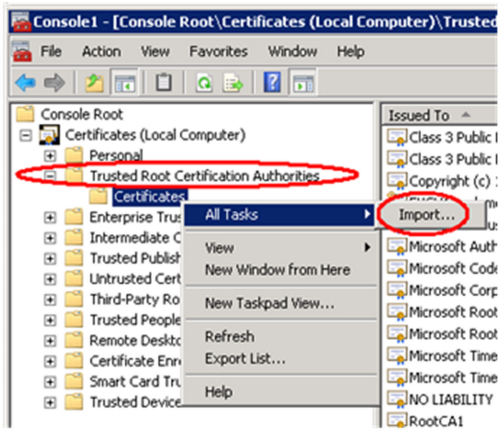

Figure 1-5 Importing the trusted CAs

8 Follow the prompts to install the trusted root CAs.

9 Repeat Step 1, "Open the Microsoft Management Console (MMC)." through Step 8, "Follow the prompts to install the trusted root CAs." for any intermediate CAs, except import them to the **Intermediate Certification Authorities** → **Certificates** branch rather than the **Trusted Root Certification Authorities** → **Certificates** branch.

Map Certificates

There are two ways to map certificates with Microsoft. You can implement one or both of these methods.

- Alternative Security Identities: This method is the most reliable method of mapping and works with any client authentication certificate. There is no need for specific fields in the certificate to be managed (no need to set UPN in SubjectAltName for example). Both One-to-One and Many-to-One mapping methods are available, which allows greater flexibility. Many-to-One also facilitates mapping many certificates to a single service account.

  Symantec has qualified this method with all versions of ActiveSync.

- Universal Principal Name (UPN) Mapping: This method allows certificates that include a UPN field in their Subject Alternative Name to map to the Universal Principal Name for the user. If you do not have a UPN in your certificate that matches the corresponding user's Universal Principal Name, then you must use the Alternative Security Identities method for certificate mapping.

  Symantec has qualified this method with ActiveSync 14 and 14.1.

Certificate Mapping Option 1 - Alternative Security Identities

1 Open the Active Directory Users and Computers snap-in. From the **Start** menu, click **Administrative Tools** → **Active Directory Users and Computers**.

2 Select **View** → **Advanced Features**.

3 Navigate to your end user (under **Users**).

4 Right-click on the user's name and select **Name Mappings**.

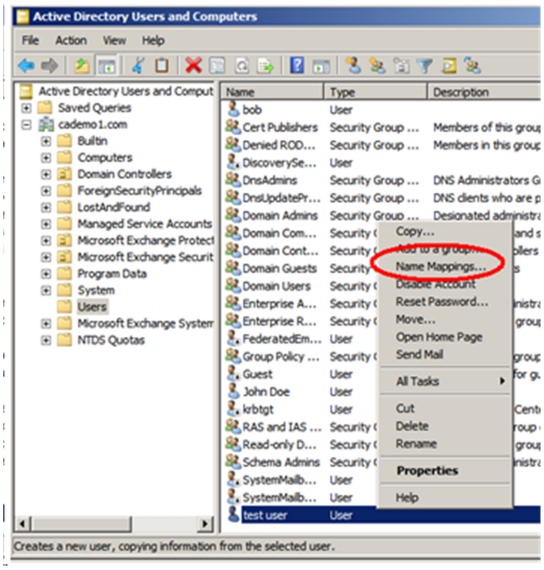

Figure 1-6 Selecting Name Mappings for an end user

5 The Security Identity Mapping dialog box appears. Click **Add** and navigate to the certificate that you want to map to this user (the certificate should be in x509 format).

6 Select how you want the certificate to be mapped:

- To have this certificate map to one user, select the **Use Issuer for alternate security identity** and **Use Subject for alternate security identity** checkboxes. This is the default.
- To map additional certificates to this user, click **Add** and map another certificate, making sure that the **Use Issuer for alternate security identity** and **Use Subject for alternate security identity** checkboxes are selected for each certificate added.
- If you want all certificates from this issuer to map to this user, unselect the **Use Subject for alternative security identity** checkbox. You might use this when you want all certificates from a private root to map to a single service account.

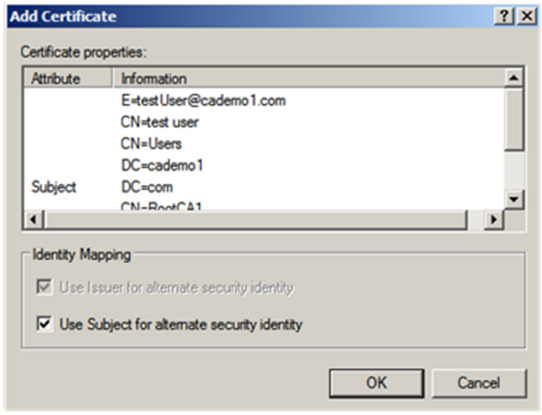

Figure 1-7 Mapping a single certificate to a single user

Certificate Mapping Option 2 - UPN mapping

Configure your domain to recognize your Certificate Authority as being authorized to issue certificates that include the UPN value:

1. Obtain a copy of your root CA certificate (.cer) and copy it to your domain controller (this is typically not the same machine that hosts Exchange and ActiveSync).
2. Issue the following command when logged in as Domain Administrator on the Primary Domain Controller:

   ```
   certutil -dspublish -f YourRoot.cer NTAuthCA
   ```

   Where YourRoot.cer is the filename of the root CA that you want to authorize to use the UPN mapping.

   It may take some time for this change to replicate across all systems on the domain.

- You can verify if an individual system has recognized this update by examining the following registry location:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates\NTAuth\Certificates

  Double-click on the certificates under this branch and look for one that includes the subject DN of YourRoot.cer.

- You can immediately force the update on any system in the domain by running the gupdate /force command on that system.

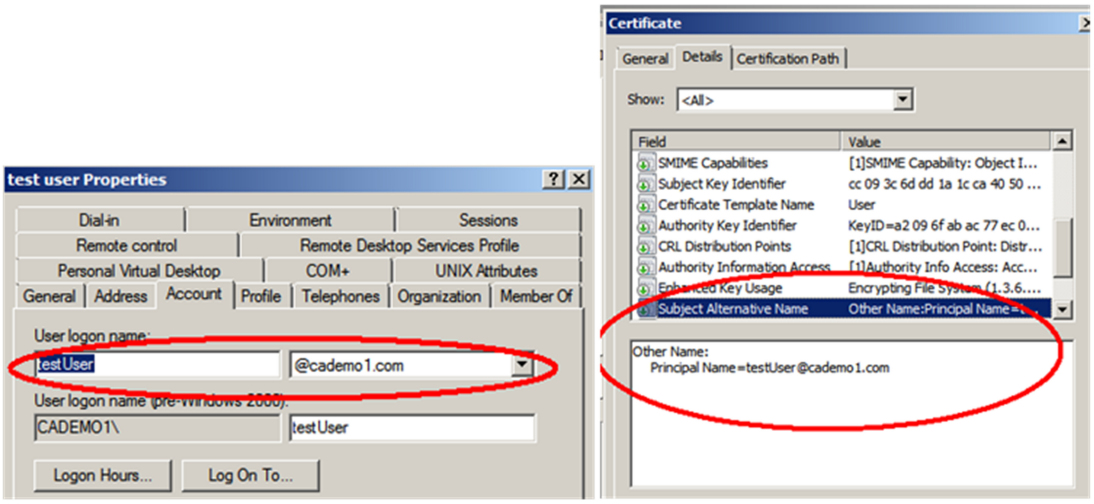

Figure 1-8 Verifying if the root CA has been recognized by a user's system

Test ActiveSync

Testing your configuration requires two steps:

- "Test Certificate Mapping" on page 7
- "Test with an ActiveSync Emulator" on page 8

Test Certificate Mapping

Complete the following steps to test if the certificate mapping is configured correctly.

1. Select a user that has an Exchange mailbox for which certificate mapping has been configured.
2. Use the private key for the user's certificate to install the certificate into Internet Explorer.
3. Using Internet Explorer, navigate to https://<ExchangeServer>/Microsoft-Server-ActiveSync (for example, https://exch1.cademo1.com/Microsoft-Server-ActiveSync.)

   You are prompted to select or confirm a certificate. This should be the user certificate added in previous step. (If not, verify that you set the correct root and intermediate CAs as trusted in "Configure IIS and ActiveSync to Trust a Third Party CA" on page 4.
4. Select the certificate. You may see an error page with a message similar to the following:

   ```
   HTTP Error 505.0 - Http Version Not Supported

   This page cannot be displayed because the HTTP version is not supported.
   ```

You can safely ignore this error.

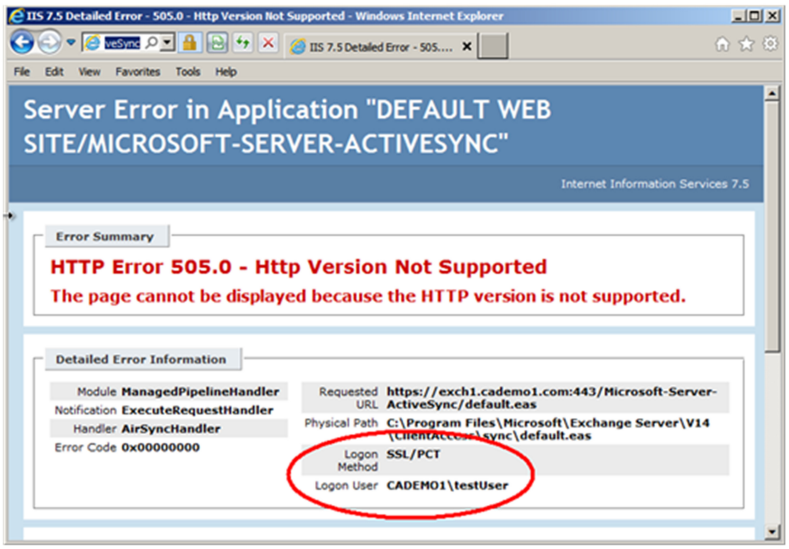

Figure 1-9 Verifying the Logon User

5 Verify that the Logon User matches the expected user in the certificate mapping (see Figure 1-7). If the Logon User is Anonymous or To be determined, verify that you have configured your certificate mapping correctly in "Map Certificates" on page 5. Also:

- Make sure you issue the appcmd.exe commands as described in "Configure ActiveSync to Map Certificates to Active Directory" on page 2.
- Make sure you can reach the CRL that is published in the CDP without having to go through a proxy.

Test with an ActiveSync Emulator

Using an ActiveSync emulator, test that the configuration works end-to-end. This example test uses the Exchange ActiveSync MD (EAS MD) available at http://mobilitydojo.net/downloads.

1 Select **Trust all Certificates**.

2 Enter the userID in the **Username** field, but leave the **Password** field blank.

3 Select **Use Client Certificate (Specify Path)** and enter the path to the certificate file.

- If you enter the path to a .cer file (where the private key is installed already in CAPI), leave the **Certificate password (if applicable)** field blank.
- If you enter the path to a .pfx file, enter the password for the file in the **Certificate password (if applicable)** field.

4 Click **Basic Connectivity Test** or **Full Sync Test**, as appropriate. You will be prompted to select which MS-APProtocol Version you want to test if you run the Full Sync Test. All tests should pass.

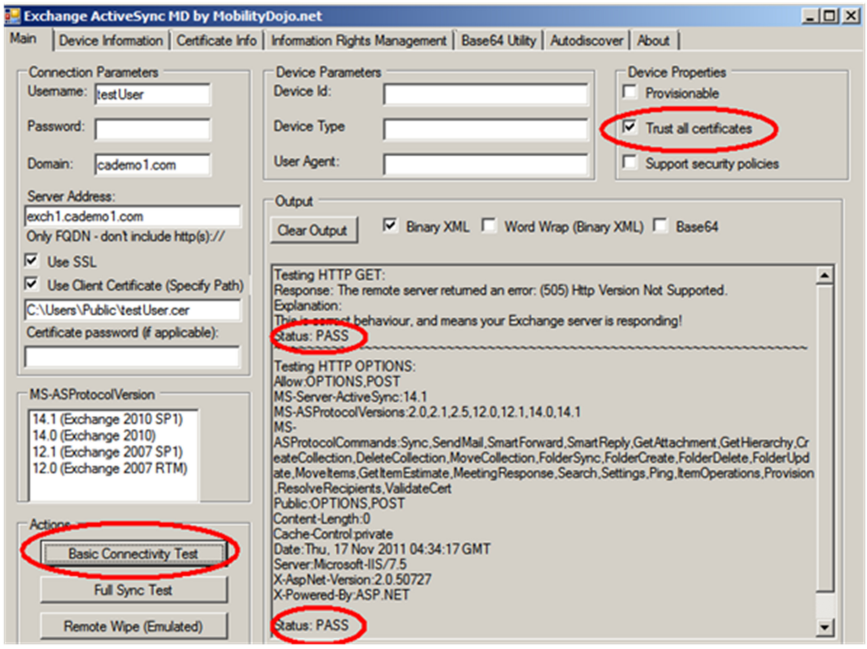

Figure 1-10 Testing with the Exchange ActiveSync MD emulator

Verifying if the CDP is Available

Complete the following steps to verify if the CDP is available:

1 Enroll for and pick up a sample client certificate. The CRL Distribution Points will be listed in the certificate. Open the certificate to view the details.

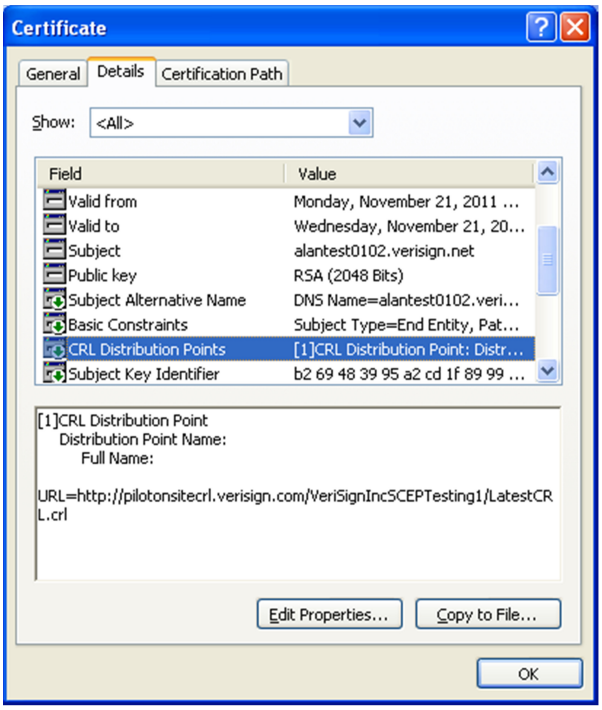

Figure 1-11 Certificate view showing CRL Distribution Points

2 Select **CRL Distribution Points**.

3 Copy and paste the URL into a browser.

If you are prompted to download the CRL, you have successfully reached the CDP from your browser.

Index

U

W