Publish Certificate Revocation Lists for ISE on a Microsoft CA Server Configuration Example

TAC **Document ID: 115758**

Contributed by Justin Teixeira, Cisco TAC Engineer.
Feb 15, 2013

Contents

Introduction

This document describes the configuration of a Microsoft Certificate Authority (CA) server that runs Internet Information Services (IIS) to publish Certificate Revocation List (CRL) updates. It also explains how to configure Cisco Identity Services Engine (ISE) (versions 1.1 and later) to retrieve the updates for use in certificate validation. ISE can be configured to retrieve CRLs for the various CA root certificates it uses in certificate validation.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine Release 1.1.2.145
- Microsoft Windows® Server® 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Configurations

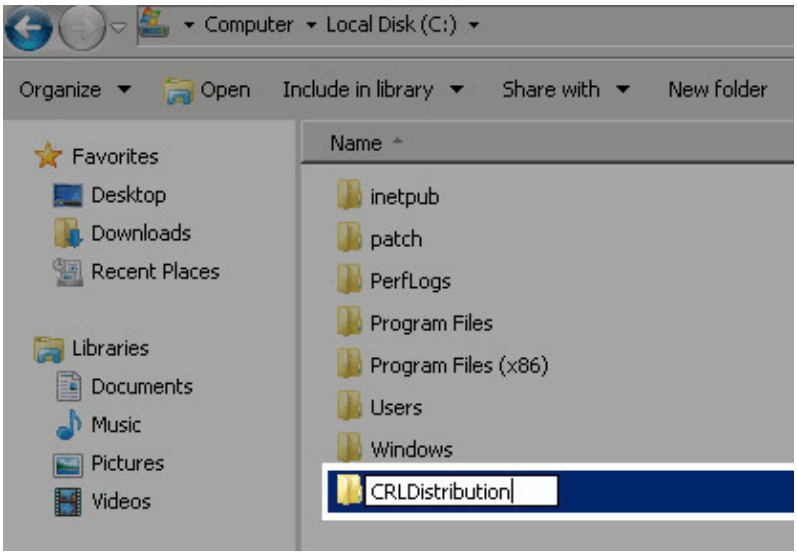
This document uses these configurations:

- Section 1. Create and Configure a Folder on the CA to House the CRL Files
- Section 2. Create a Site in IIS to Expose the New CRL Distribution Point
- Section 3. Configure Microsoft CA Server to Publish CRL Files to the Distribution Point
- Section 4. Verify the CRL File Exists and is Accessible via IIS
- Section 5. Configure ISE to use the New CRL Distribution Point

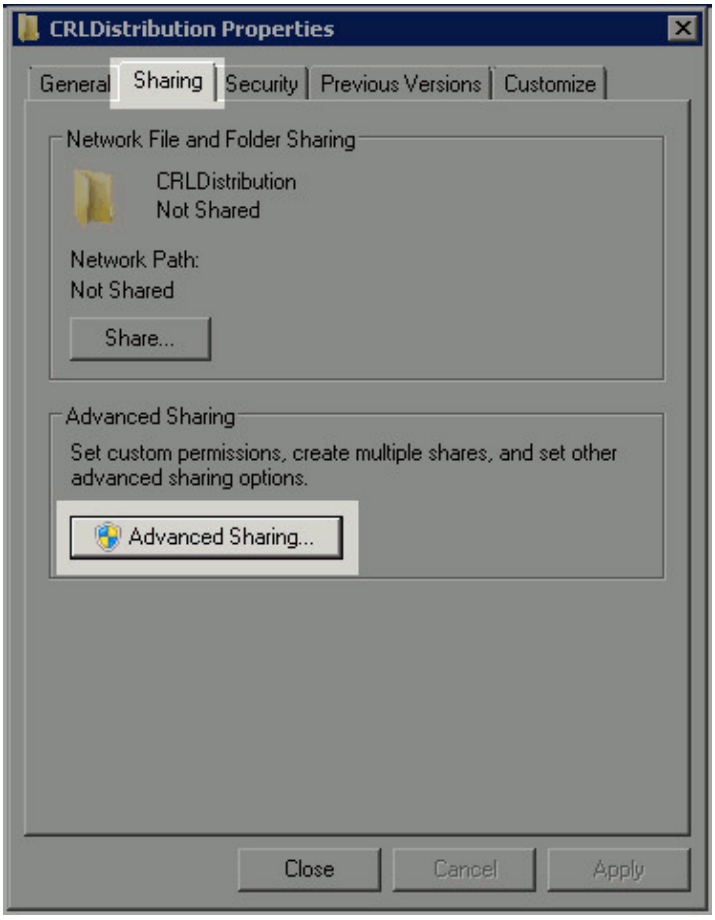
Section 1. Create and Configure a Folder on the CA to House the CRL Files

The first task is to configure a location on the CA server to store the CRL files. By default, the Microsoft CA server publishes the files to C:\Windows\system32\CertSrv\CertEnroll\ . Rather than use this system folder, create a new folder for the files.

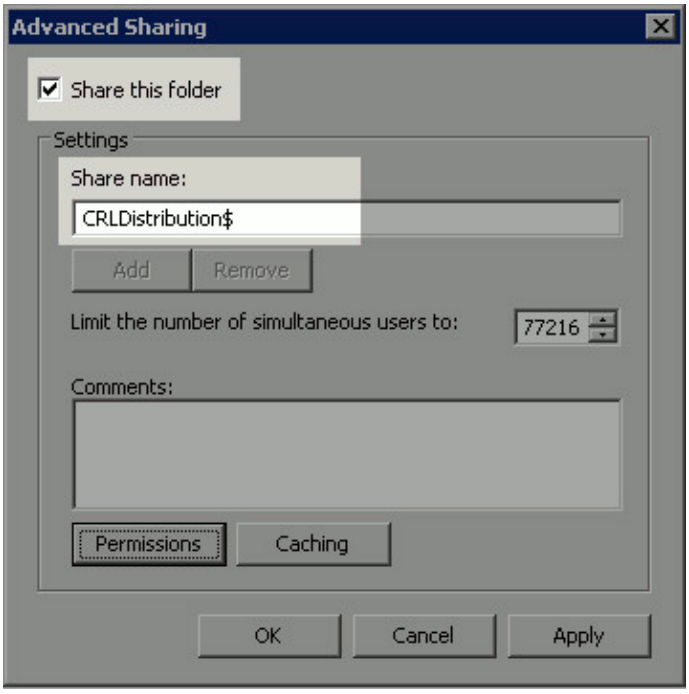
1. On the IIS server, choose a location on file system and create a new folder. In this example, the folder C:\CRLDistribution is created.



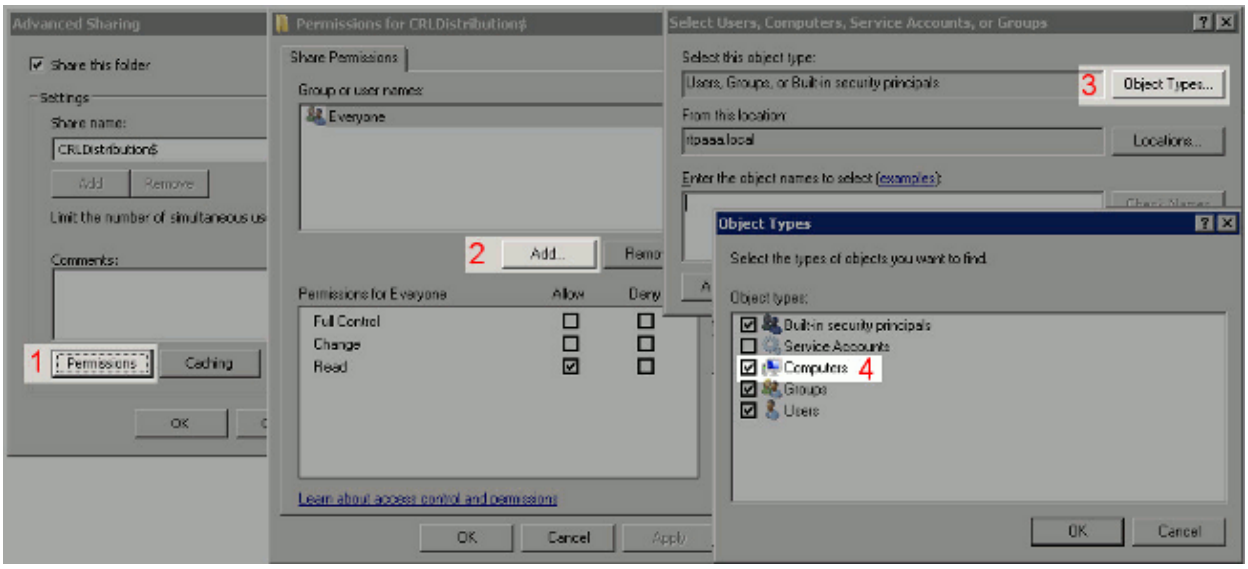
2. In order for the CA to write the CRL files to the new folder, sharing must be enabled. Right−click the new folder, choose **Properties**, click the **Sharing** tab, and then click **Advanced Sharing**.



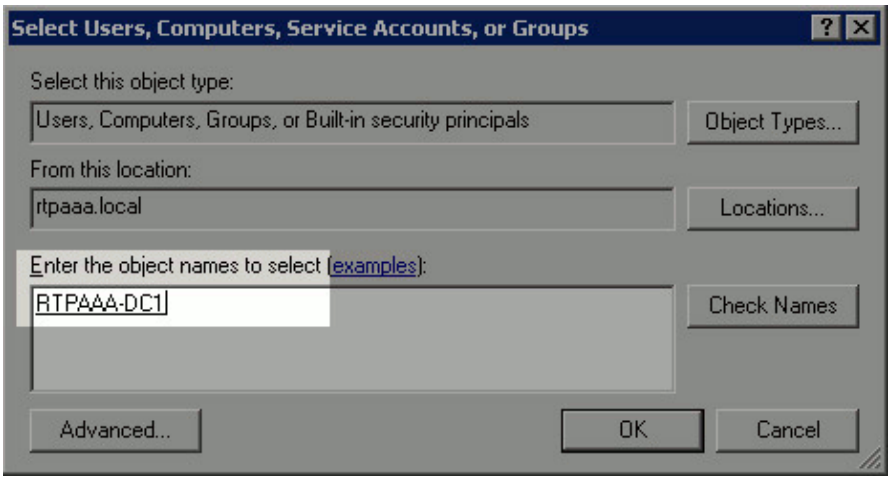
3. In order to share the folder, check the **Share this folder** check box and then add a dollar sign ($) to the end of the share name in the Share name field to hide the share.



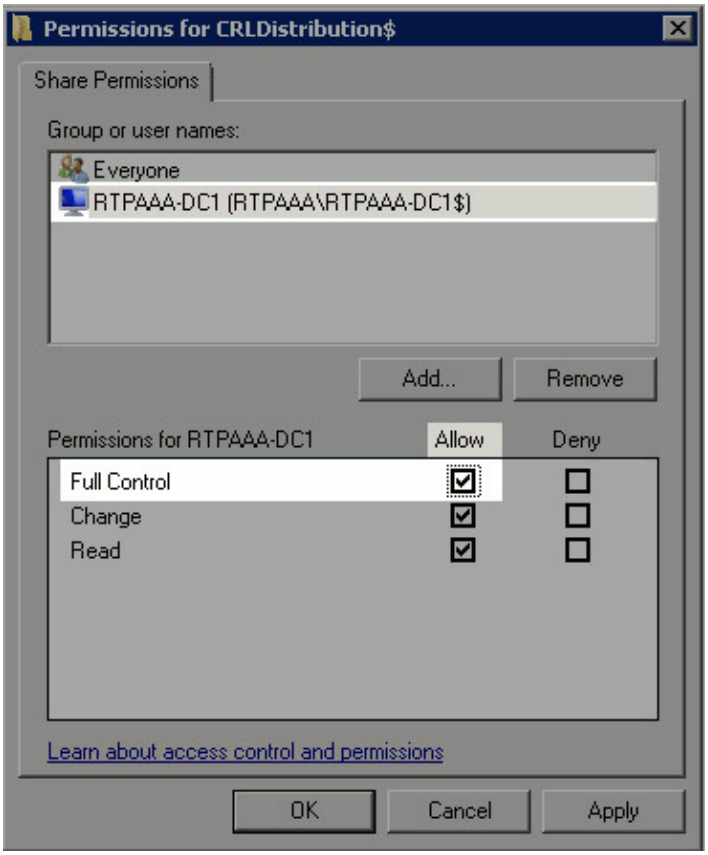
4. Click **Permissions** (1), click **Add** (2), click **Object Types** (3), and check the **Computers** check box (4).



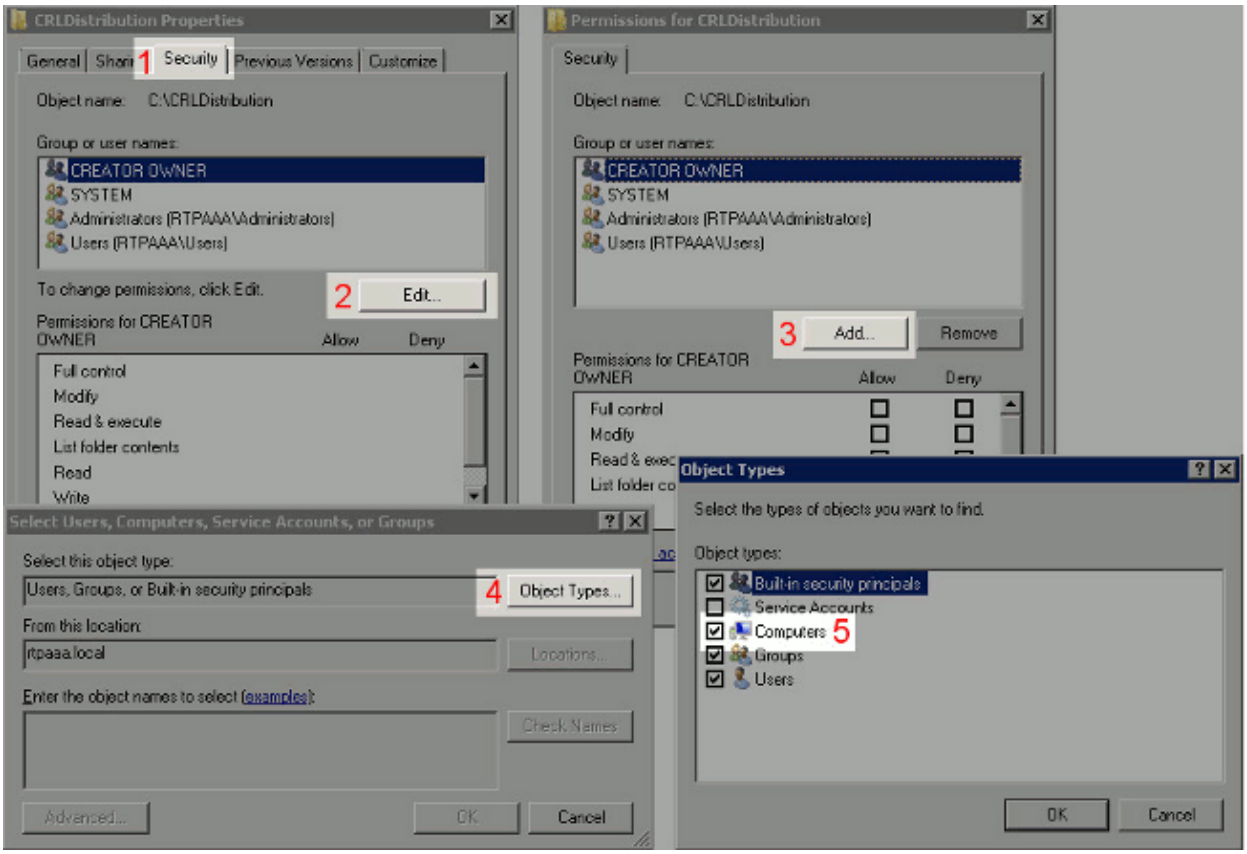
5. In order to return to the Select Users, Computers, Service Accounts, or Groups window, click **OK**. In the Enter the object names to select field, enter the computer name of the CA server and click **Check Names**. If the name entered is valid, the name refreshes and appears underlined. Click **OK**.



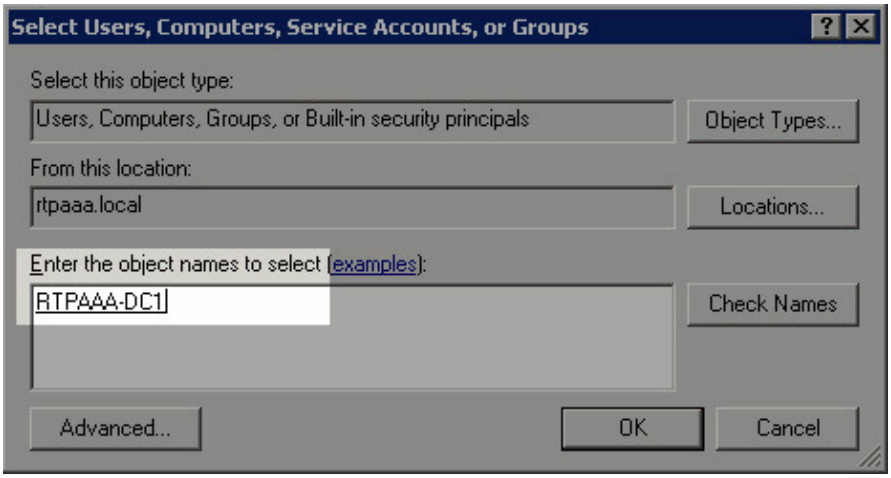
6. In the Group or user names field, choose the CA computer. Check **Allow** for Full Control to grant full access to the CA. Click **OK**. Click **OK** again to close the Advanced Sharing window and return to the Properties window.



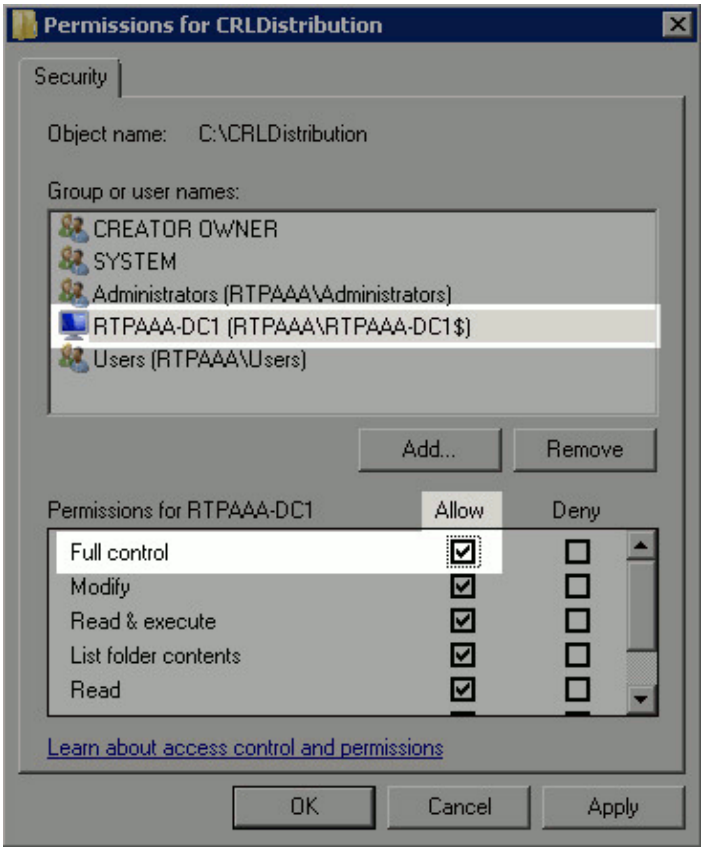
7. In order to allow the CA to write the CRL files to the new folder, configure the appropriate security permissions. Click the **Security** tab (1), click **Edit** (2), click **Add** (3), click **Object Types** (4), and check the **Computers** check box (5).



8. In the Enter the object names to select field, enter the computer name of the CA server and click **Check Names**. If the name entered is valid, the name refreshes and appears underlined. Click **OK**.



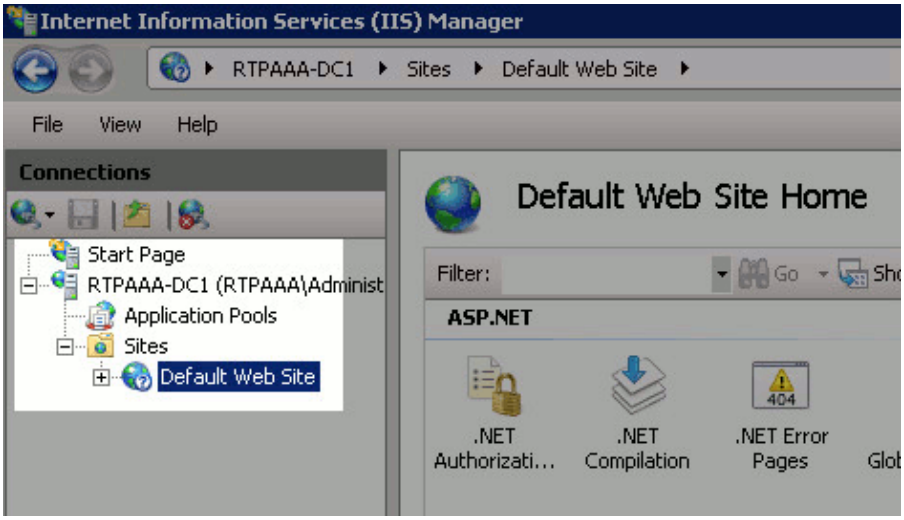
9. Choose the CA computer in the Group or user names field and then check **Allow** for Full control to grant full access to the CA. Click **OK** and then click **Close** to complete the task.



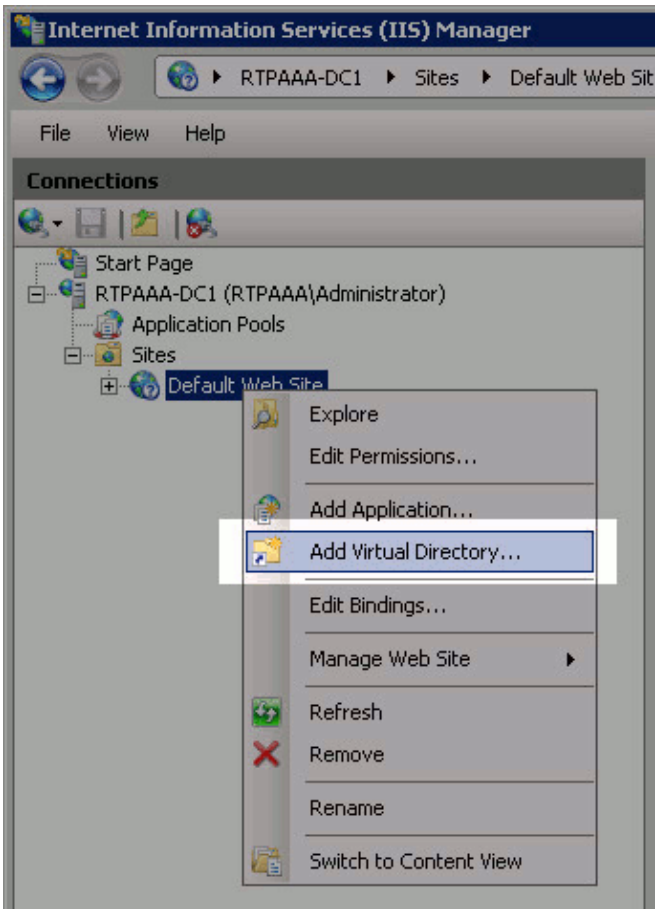
Section 2. Create a Site in IIS to Expose the New CRL Distribution Point

In order for ISE to access the CRL files, make the directory that houses the CRL files accessible via IIS.

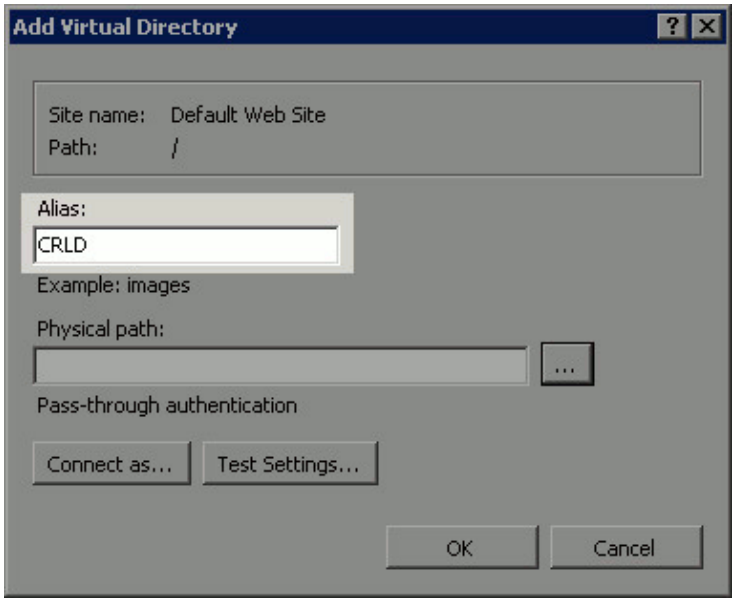
1. On the IIS server taskbar, click **Start**. Choose **Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left pane (known as the Console Tree), expand the IIS server name and then expand **Sites.**



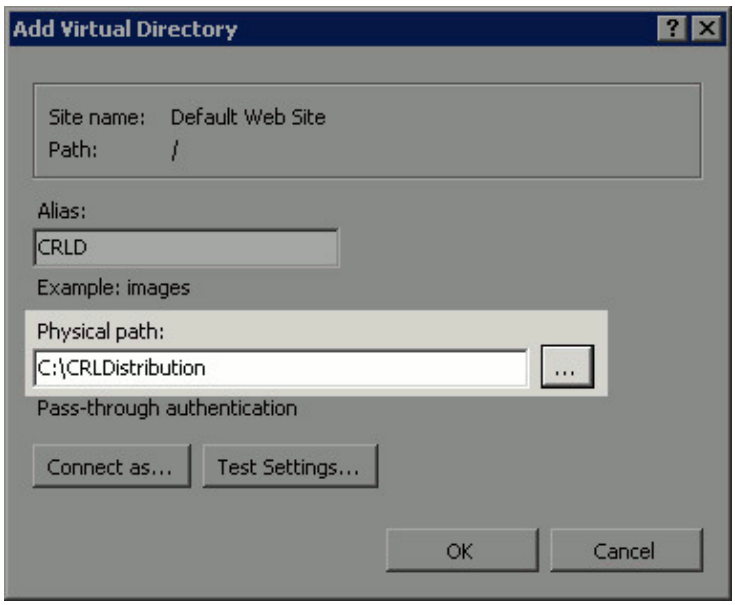
3. Right−click **Default Web Site** and choose **Add Virtual Directory**.



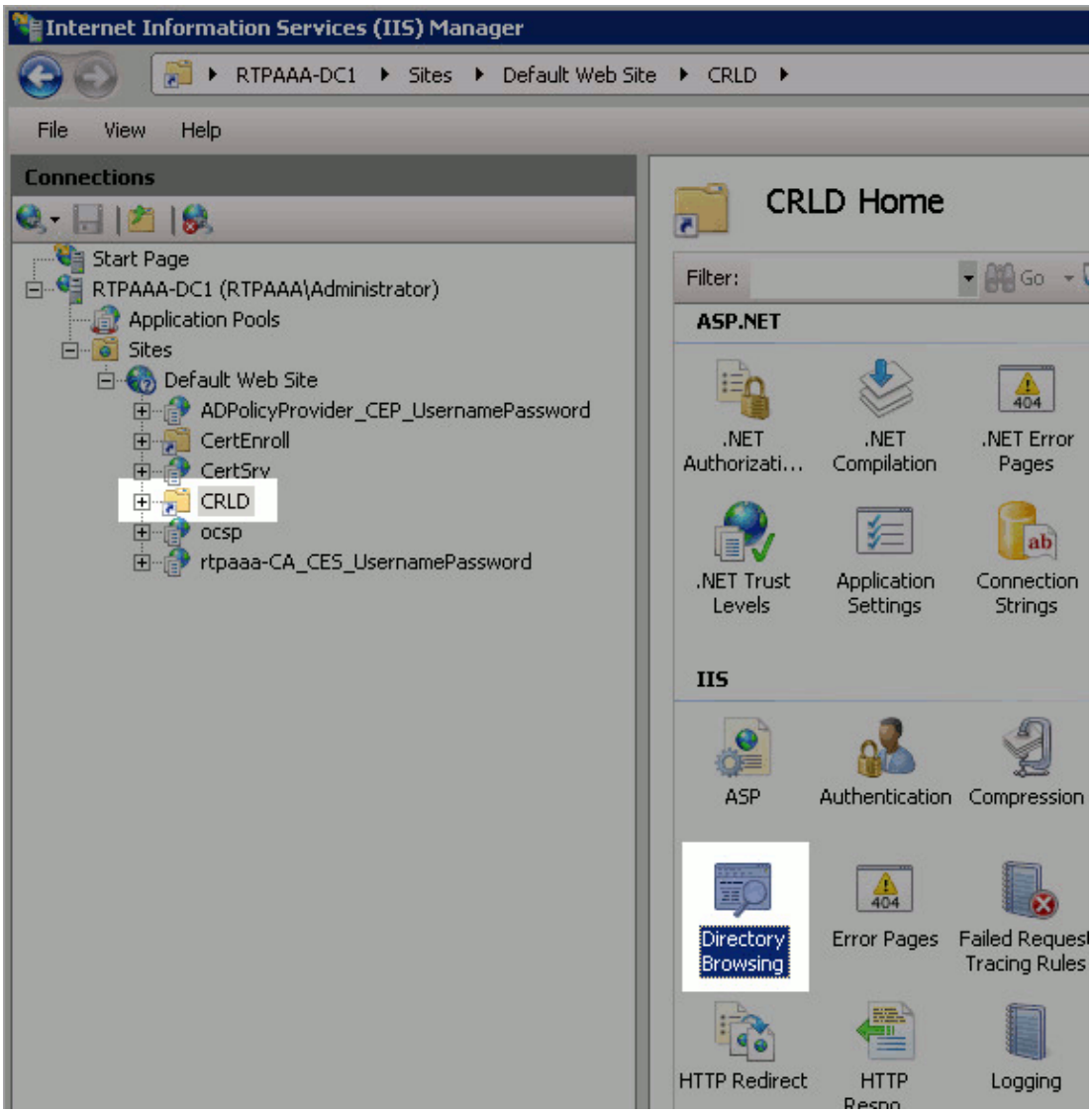
4. In the Alias field, enter a site name for the CRL Distribution Point. In this example, CRLD is entered.



5. Click the ellipsis (. . .) to the right of the Physical path field and browse to the folder created in section 1. Select the folder and click **OK**. Click **OK** to close the Add Virtual Directory window.

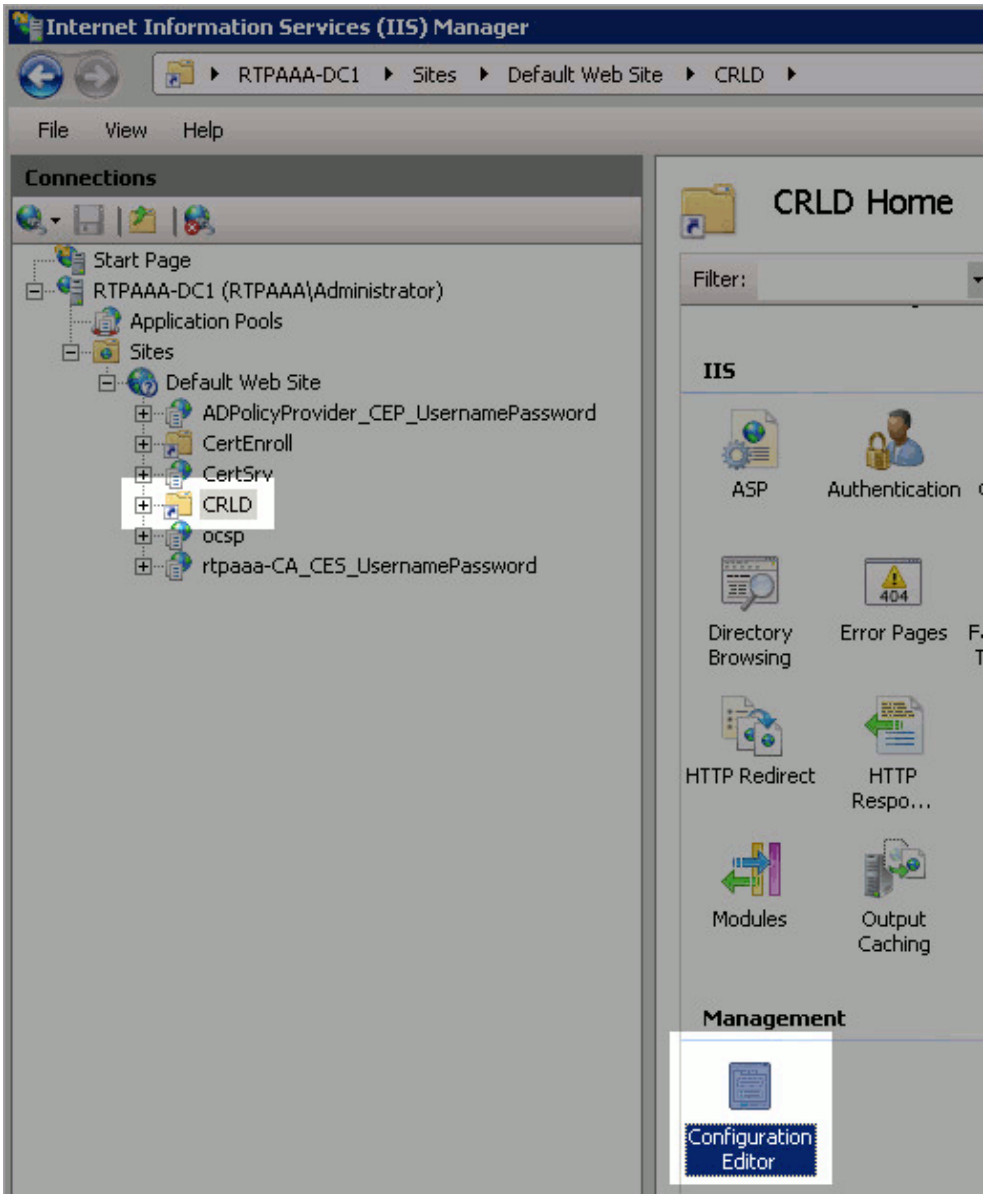


6. The site name entered in step 4 should be highlighted in the left pane. If not, choose it now. In the center pane, double−click **Directory Browsing**.

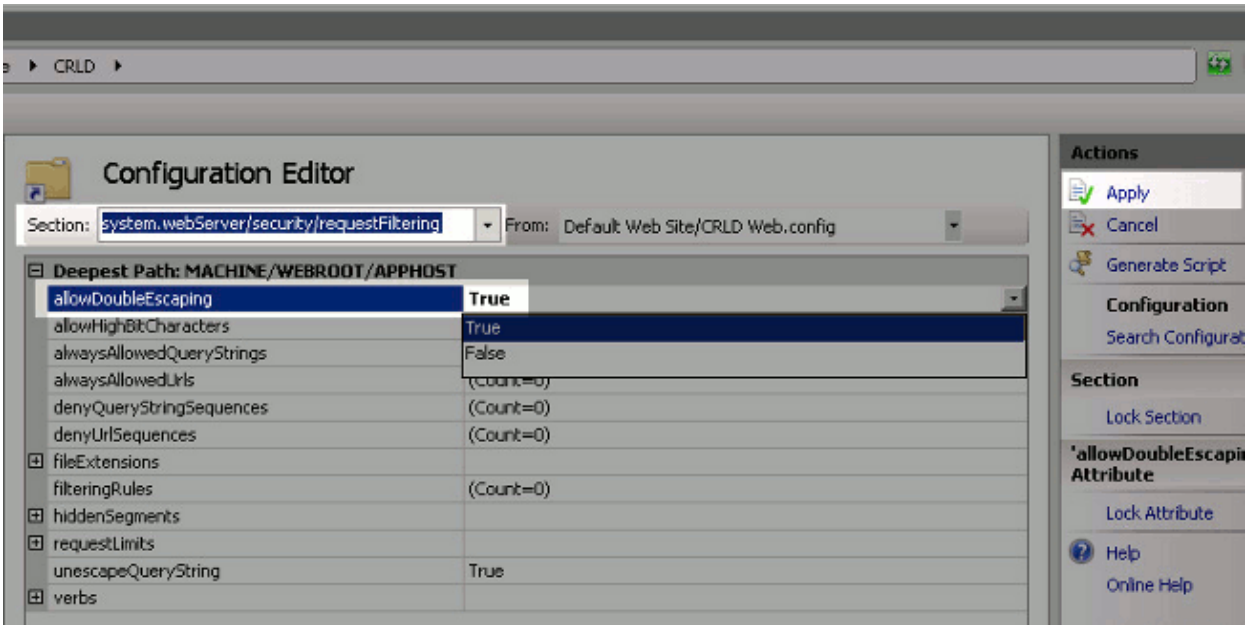


7. In the right pane, click **Enable** to enable directory browsing.

8. In the left pane, choose the site name again. In the center pane, double−click **Configuration Editor**.



9. In the Section drop−down list, choose **system.webServer/security/requestFiltering**. In the allowDoubleEscaping drop−down list, choose **True**. In the right pane, click **Apply**.

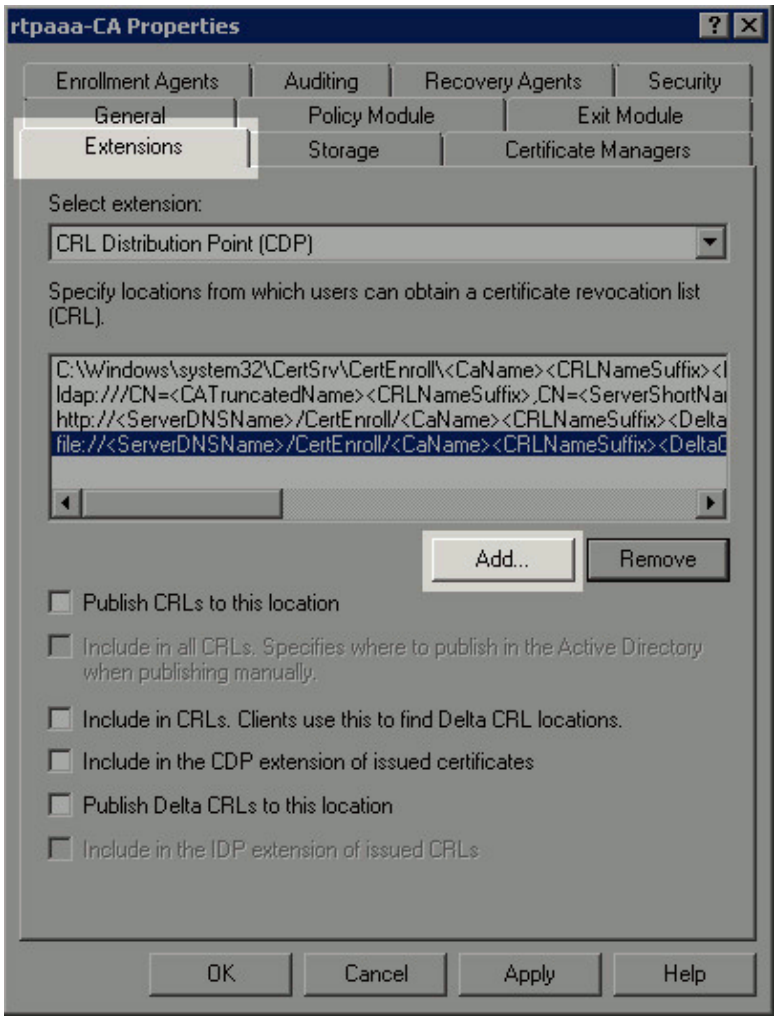


The folder should now be accessible via IIS.

Section 3. Configure Microsoft CA Server to Publish CRL Files to the Distribution Point

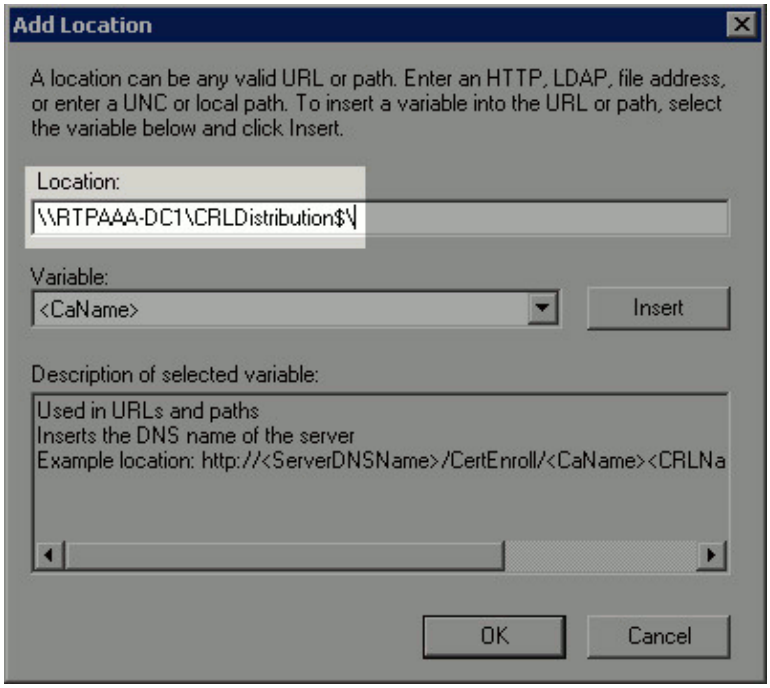
Now that a new folder has been configured to house the CRL files and the folder has been exposed in IIS, configure Microsoft CA server to publish the CRL files to the new location.

1. On the CA server taskbar, click **Start**. Choose **Administrative Tools > Certificate Authority**.
2. In the left pane, right−click the CA name. Choose **Properties** and then click the **Extensions** tab. In order to add a new CRL distribution point, click **Add**.

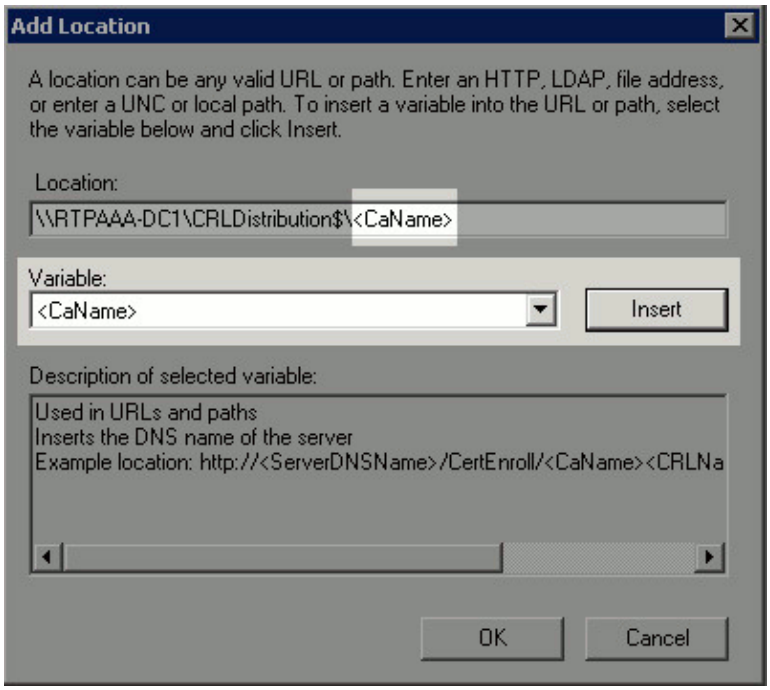


3. In the Location field, enter the path to the folder created and shared in section 1. In the example in section 1, the path is:

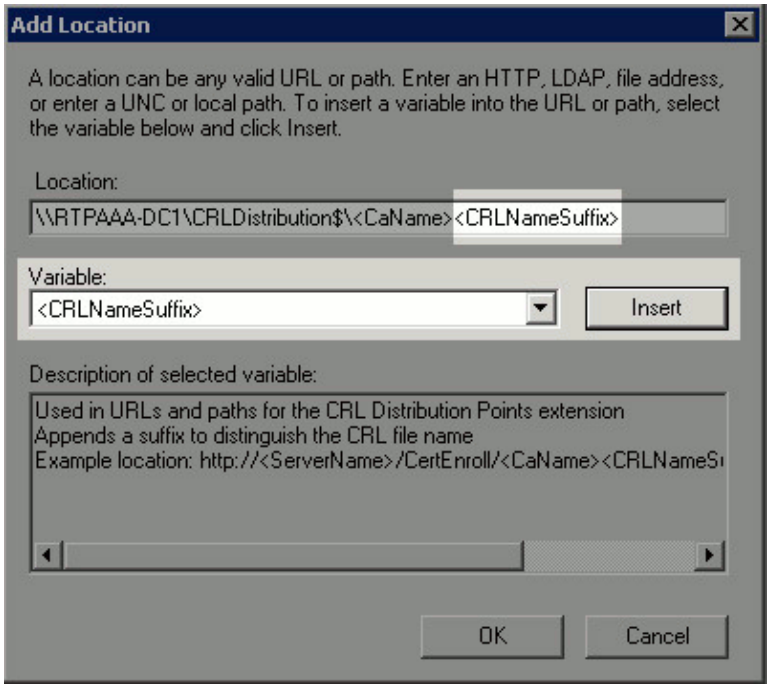
```
\\RTPAAA-DC1\CRLDistribution$\
```



4. With the Location field populated, choose **<CaName>** from the Variable drop−down list and then click **Insert.**

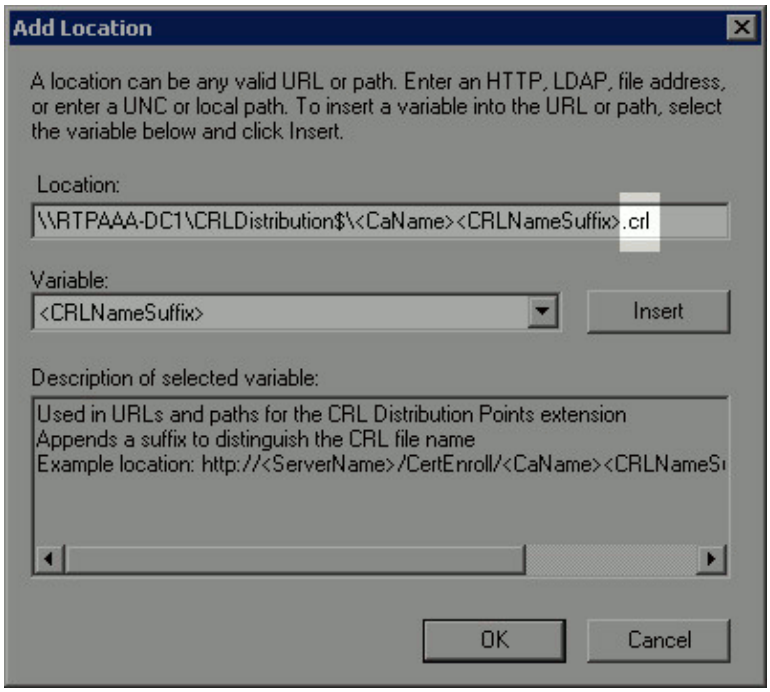


5. From the Variable drop−down list, choose **<CRLNameSuffix>** and then click **Insert**.

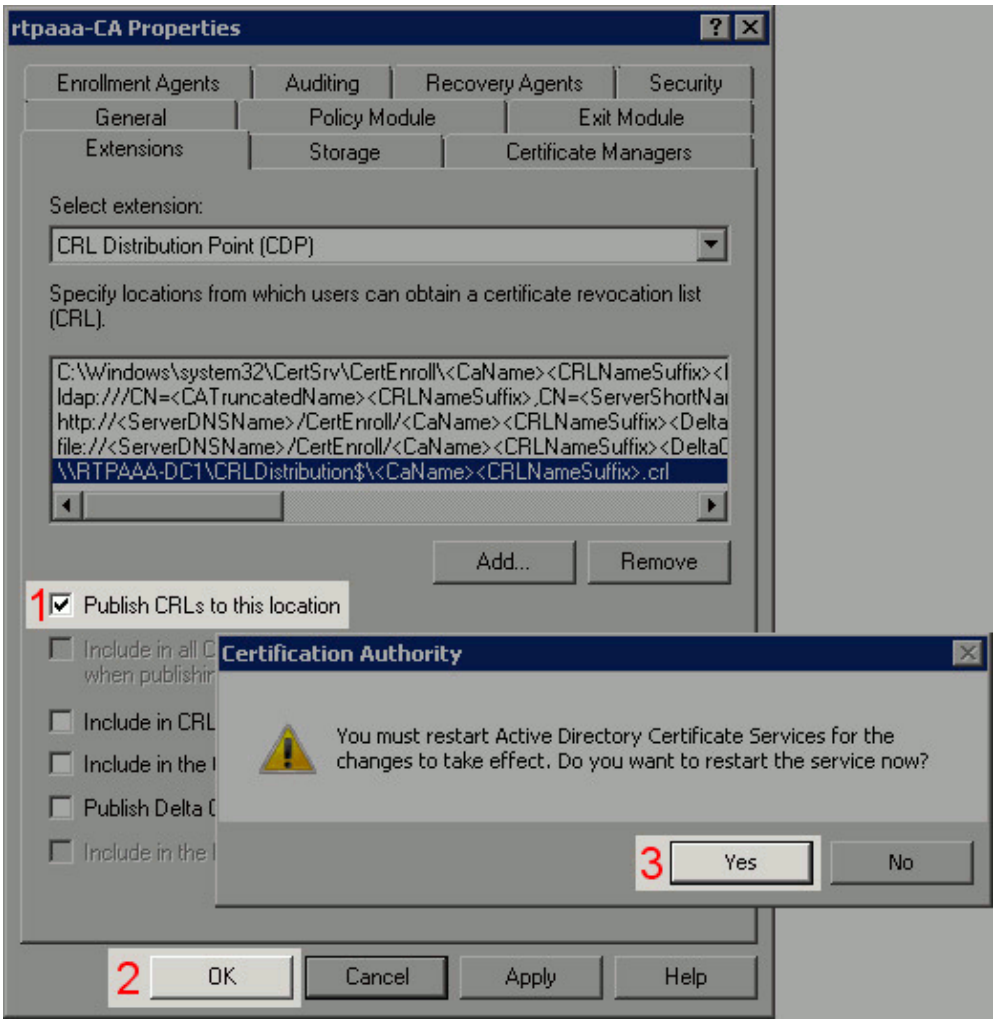


6. In the Location field, append .crl to the end of the path. In this example, the Location is:

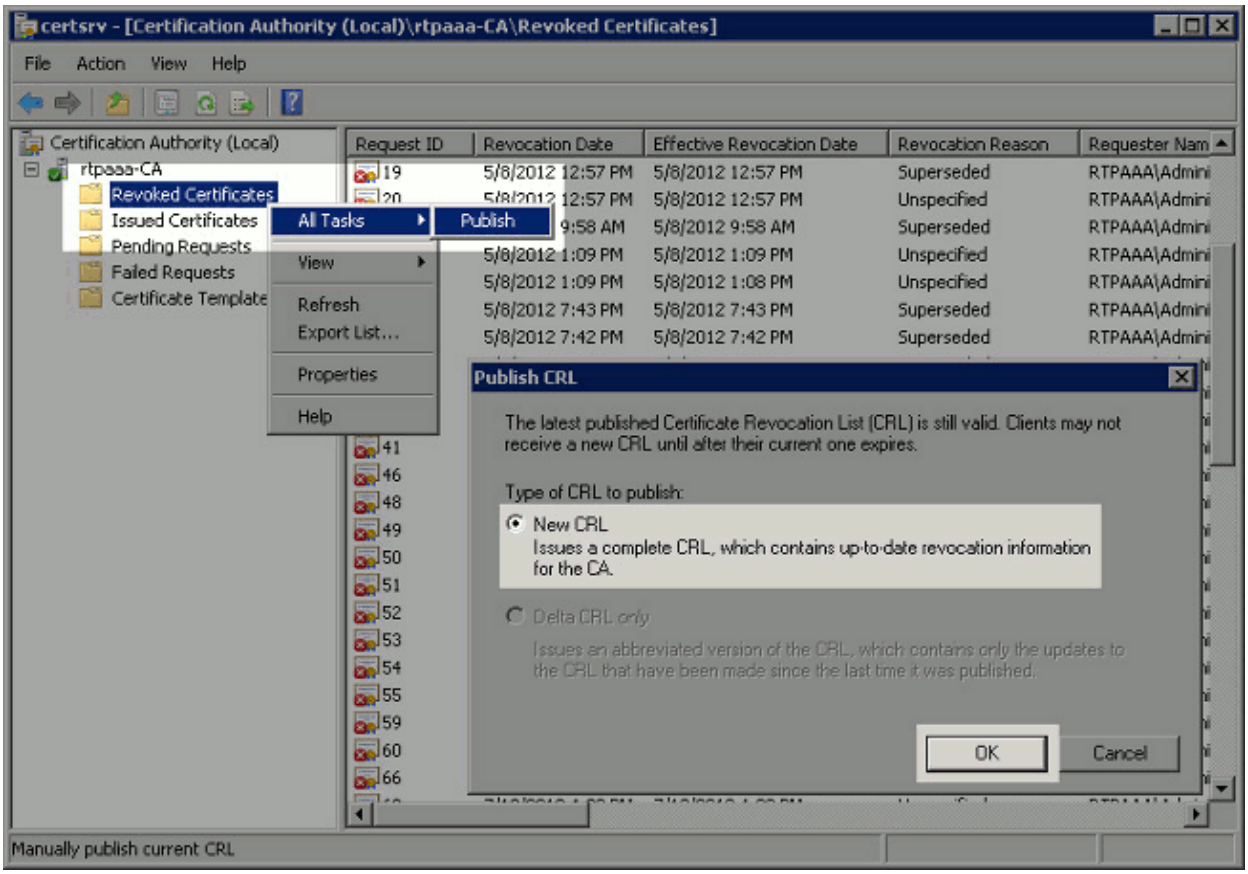
```
\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl
```



7. Click **OK** to return to the Extensions tab. Check the **Publish CRLs to this location** check box (1) and then click **OK** (2) to close the Properties window. A prompt appears for permission to restart Active Directory Certificate Services. Click **Yes** (3).



8. In the left pane, right−click **Revoked Certificates**. Choose **All Tasks > Publish**. Ensure that New CRL is selected and then click **OK.**



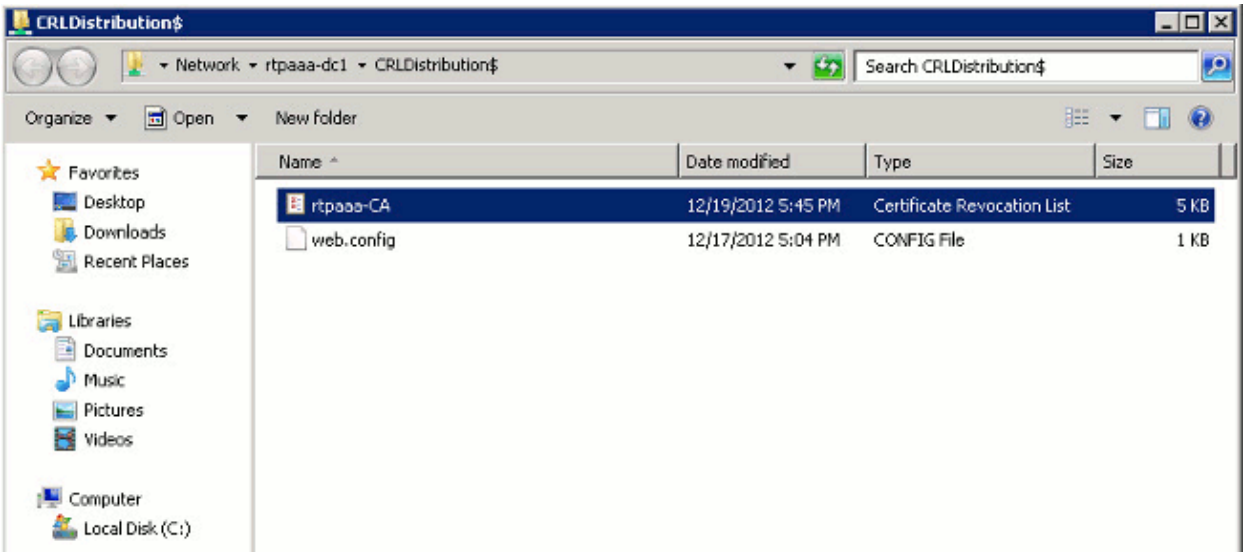
The Microsoft CA server should create a new .crl file in the folder created in section 1. If the new CRL file is created successfully there will be no dialog after OK is clicked. If an error is returned in regards to the new distribution point folder, carefully repeat each step in this section.

Section 4. Verify the CRL File Exists and is Accessible via IIS

Verify the new CRL files exist and that they are accessible via IIS from another workstation before you start this section.

1. On the IIS server, open the folder created in section 1. There should be a single .crl file present with the form <CANAME>.crl where <CANAME> is the name of the CA server. In this example, the filename is:

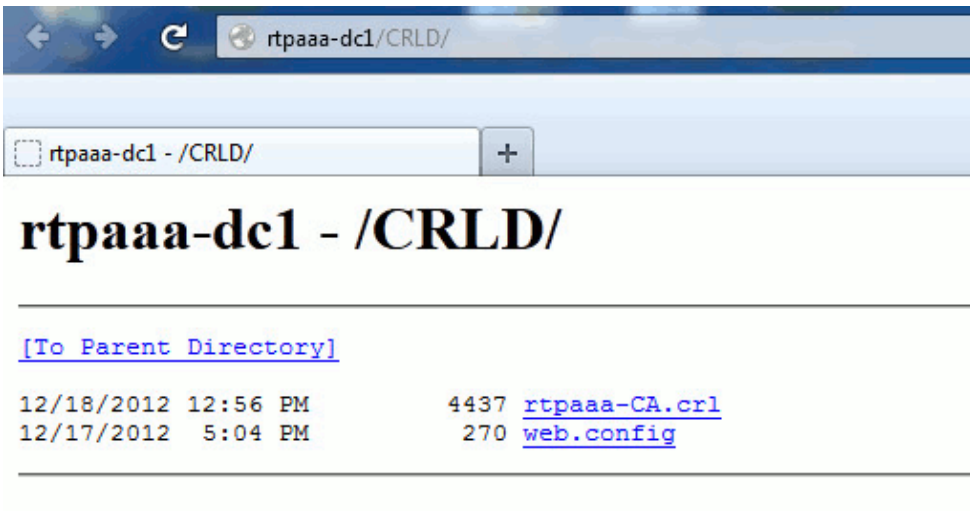
```
rtpaaa-CA.crl
```



2. From a workstation on the network (ideally on the same network as the ISE primary Admin node), open a web browser and browse to http://<SERVER>/<CRLSITE> where <SERVER> is the server name of the IIS server configured in section 2 and <CRLSITE> is the site name chosen for the distribution point in section 2. In this example, the URL is:

   ```
   http://RTPAAA-DC1/CRLD
   ```

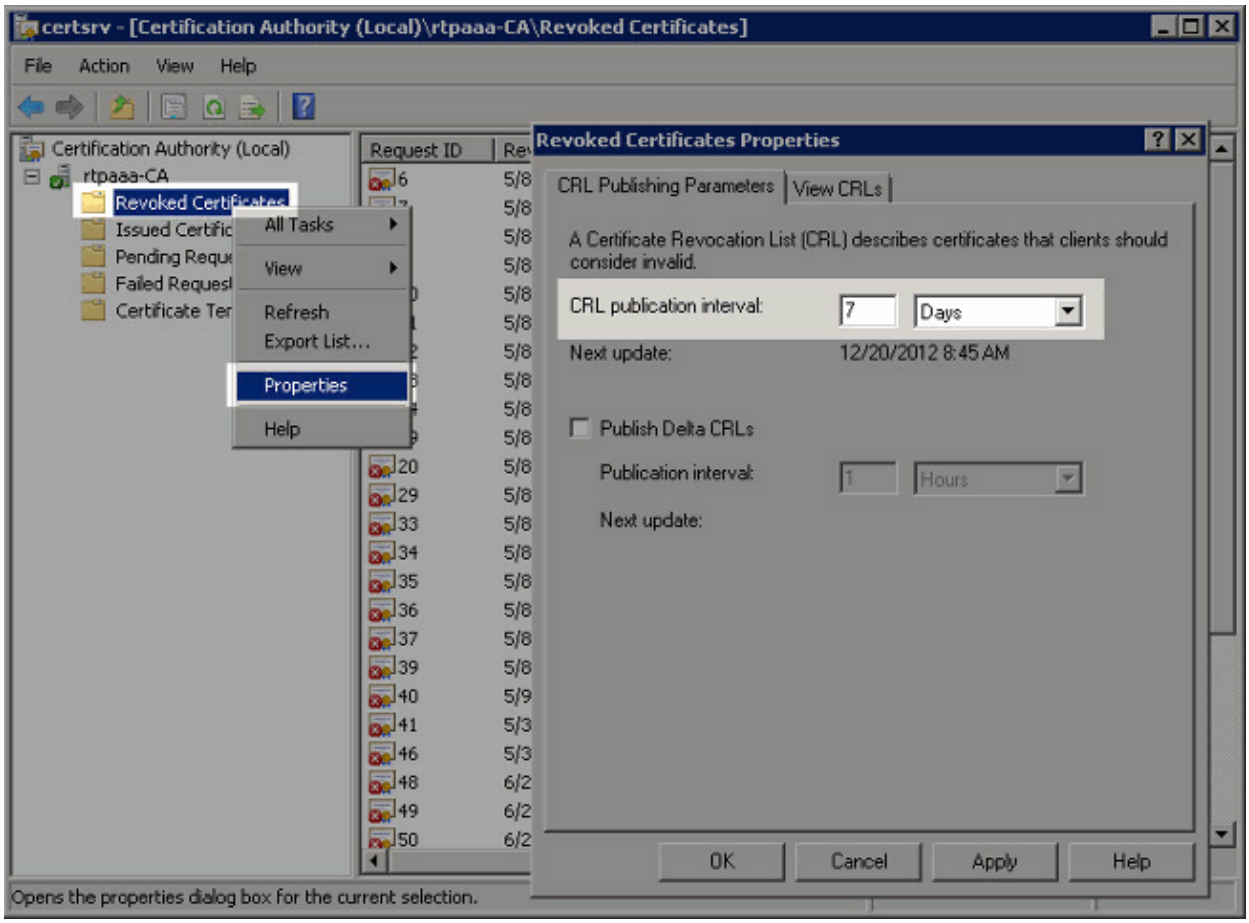
   The directory index displays, which includes the file observed in step 1.



Section 5. Configure ISE to use the New CRL Distribution Point

Before ISE is configured to retrieve the CRL, define the interval to publish the CRL. The strategy to determine this interval is beyond the scope of this document. The potential values (in Microsoft CA) are 1 hour to 411 years, inclusive. The default value is 1 week. Once an appropriate interval for your environment has been determined, set the interval with these instructions:

1. On the CA server taskbar, click **Start**. Choose **Administrative Tools > Certificate Authority**.
2. In the left pane, expand the CA. Right−click the **Revoked Certificates** folder and choose **Properties.**
3. In the CRL publication interval fields, enter the required number and choose the time period. Click **OK** to close the window and apply the change. In this example, a publication interval of 7 days is configured.



You should now confirm several registry values, which will help determine the CRL retrieval settings in ISE.

4. Enter the **certutil −getreg CA\Clock*** command to confirm the ClockSkew value. The default value is 10 minutes.

   Example output:

   ```
   Values:
       ClockSkewMinutes        REG_DWORS = a (10)
   CertUtil: -getreg command completed successfully.
   ```

5. Enter the **certutil −getreg CA\CRLov*** command to verify whether the CRLOverlapPeriod has been manually set. By default the CRLOverlapUnit value is 0, which indicates that no manual value has been set. If the value is a value other than 0, record the value and units.

   Example output:

   ```
   Values:
       CRLOverlapPeriod      REG_SZ = Hours
       CRLOverlapUnits        REG_DWORD = 0
   CertUtil: -getreg command completed successfully.
   ```

6. Enter the **certutil −getreg CA\CRLpe*** command to verify the CRLPeriod, which was set in step 3.

   Example output:

   ```
   Values:
       CRLPeriod      REG_SZ = Days
       CRLUnits        REG_DWORD = 7
   CertUtil: -getreg command completed successfully.
   ```

7. Calculate the CRL Grace Period as follows:

a. If CRLOverlapPeriod was set in step 5: OVERLAP = CRLOverlapPeriod, in minutes;

   Else: OVERLAP = (CRLPeriod / 10), in minutes
b. If OVERLAP > 720 then OVERLAP = 720
c. If OVERLAP < (1.5 * ClockSkewMinutes) then OVERLAP = (1.5 * ClockSkewMinutes)
d. If OVERLAP > CRLPeriod, in minutes then OVERLAP = CRLPeriod in minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes

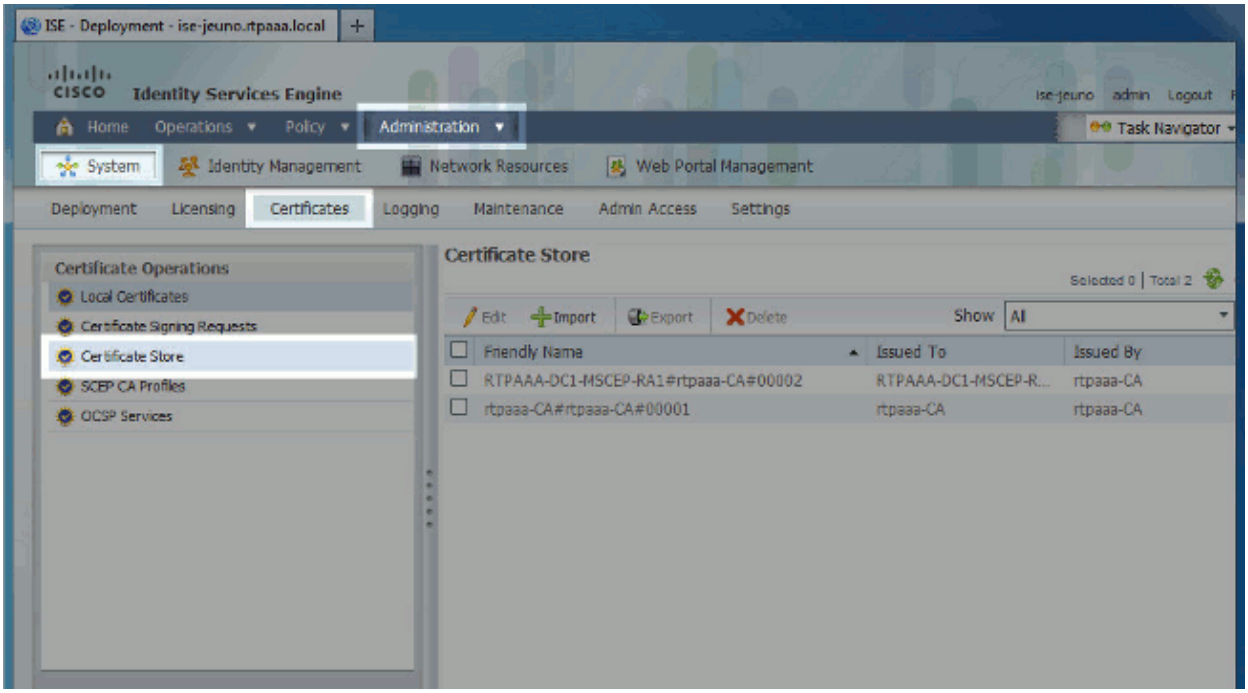
Example:

```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
CRLOverlapPeriod was not set.

a. OVERLAP = (10248 / 10) = 1024.8 minutes
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```

The grace period calculated is the amount of time between when the CA publishes the next CRL and when the current CRL expires. ISE needs to be configured to retrieve the CRLs accordingly.

8. Log in to the primary Admin node and choose **Administration > System > Certificates**. In the left pane, select **Certificate Store**.



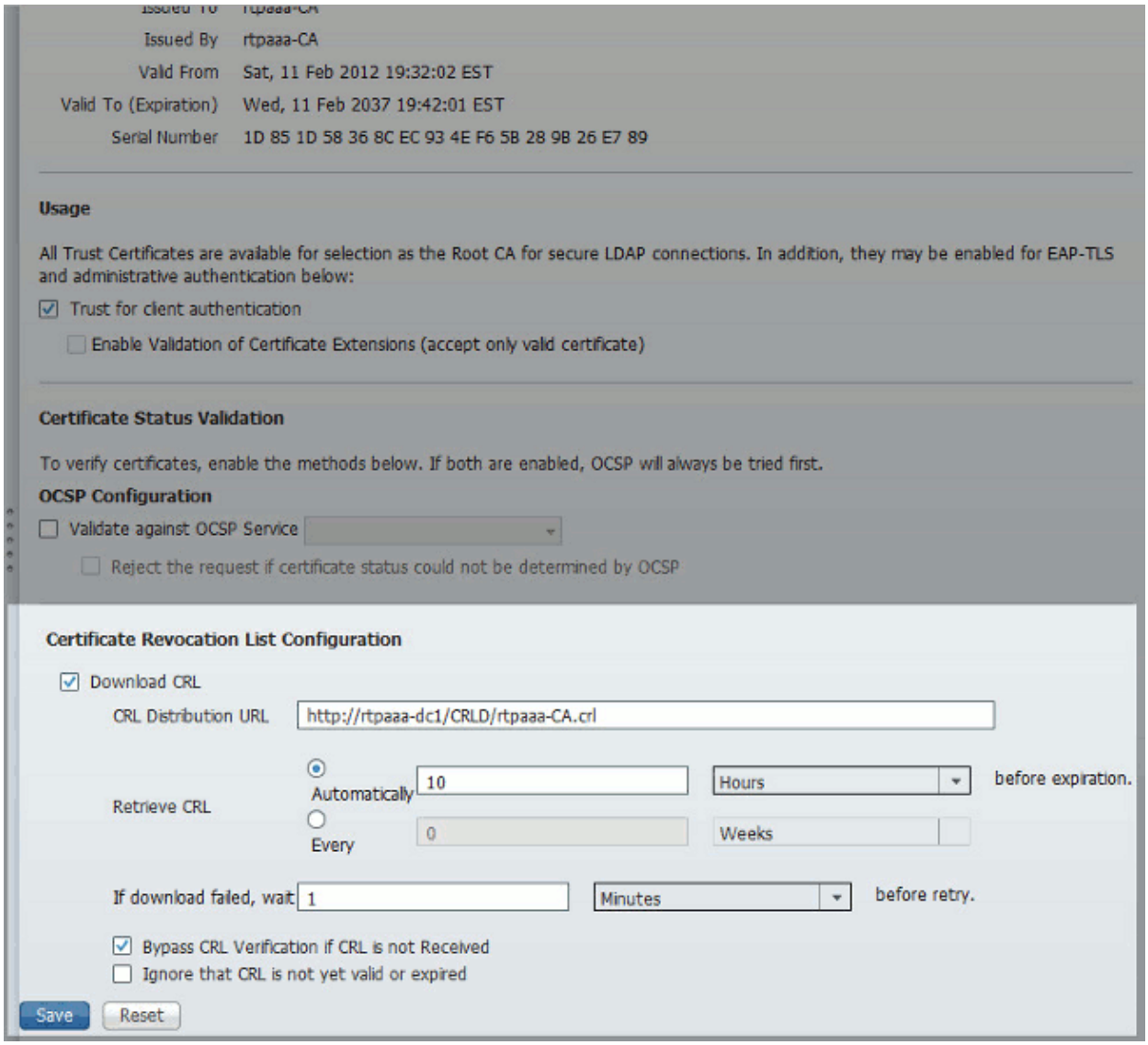
9. Check the Certificate Store check box next to the CA certificate for which you intend to configure CRLs. Click **Edit**.
10. Near the bottom of the window, check the **Download CRL** check box.
11. In the CRL Distribution URL field, enter the path to the CRL Distribution Point, which includes the .crl file, created in section 2. In this example, the URL is:

```
http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
```

12. ISE can be configured to retrieve the CRL at regular intervals or based on the expiration (which, in general, is also a regular interval). When the CRL publish interval is static, more timely CRL updates are obtained when the latter option is used. Click the **Automatically** radio button.
13. Set the value for retrieval to a value less than the grace period calculated in step 7. If the value set is longer than the grace period, ISE checks the CRL distribution point before the CA has published the next CRL. In this example, the grace period is calculated to be 730 minutes, or 12 hours and 10

minutes. A value of 10 hours will be used for the retrieval.

14. Set the retry interval as appropriate for your environment. If ISE cannot retrieve the CRL at the configured interval in the previous step, it will retry at this shorter interval.
15. Check the **Bypass CRL Verification if CRL is not Received** check box to allow certificate−based authentication to proceed normally (and without a CRL check) if ISE was unable to retrieve the CRL for this CA in its last download attempt. If this check box is not checked, all certificate−based authentication with certificates issued by this CA will fail if the CRL cannot be retrieved.
16. Check the **Ignore that CRL is not yet valid or expired** check box to allow ISE to use expired (or not yet valid) CRL files as though they were valid. If this check box is not checked, ISE considers a CRL to be invalid prior to their Effective Date and after their Next Update times. Click **Save** to complete the configuration.



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 15, 2013 Document ID: 115758