Active Directory Self-Service
SSL Configuration White Paper

General Information: info@cionsystems.com
Online Support: support@cionsystems.com
Contact Notes:

For technical support or feature requests, please contact us at Support@CionSystems.com or 425.605.5325

For sales or other business inquiries, we can be reached at Sales@CionSystems.com or 425.605.5325

If you’d like to view a complete list of our Active Directory Management solutions, please visit us online at www.CionSystems.com

Disclaimer

The information in this document is provided as information only. No warranty on the accuracy of the information, express or implied, No license, express or implied, to any intellectual property right is granted by this document or in connection with the sale of CionSystems products. EXCEPT AS SET FORTH IN CIONSYSTEMS' LICENSE AGREEMENT FOR THIS PRODUCT, CIONSYSTEMS INC. ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL CIONSYSTEMS INC. BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CIONSYSTEMS INC. HAS BEEN ADVISED IN WRITING OF THE POSSIBILITY OF SUCH DAMAGES. CionSystems may update this document without notice.

CionSystems Inc
16625 Redmond Way,
Ste M106
Redmond, WA 98052
425.605.5325

This guide is provided for informational purposes only, and the contents may not be reproduced or transmitted in any form or by any means without written permission.

Trademarks

CionSystems, CionSystems Inc., the CionSystems Inc. logo, CionSystems Active Directory Self-Service are trademarks of CionSystems. Other trademarks and registered trademarks used in this guide are property of their respective owners.
# Table of Contents

SSL Installation Procedure ........................................................................................................ 4  
1. Introduction .......................................................................................................................... 4  
2. Prepare a certificate signing request ..................................................................................... 4  
   2.1 If the Server Certificate button is not available or button is disabled ......................... 6  
3. Request a certificate from certificate vendor or Submit a certificate Request ............ 13  
   3.1 Procedure 1: .................................................................................................................. 13  
   3.2 Procedure 2: .................................................................................................................. 18  
4. Install the certificate ............................................................................................................. 20  
5. Install necessary intermediate certificate ............................................................................. 23  
6. Issue a Certificate .................................................................................................................. 24  
7. Checking the require secure channel .................................................................................... 26  
8. Test ........................................................................................................................................ 27
SSL Installation Procedure

1. Introduction
SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. A browser requests a secure page (usually https://). This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) - a data file also containing your details. You should then submit the CSR. During the SSL Certificate application process, the Certification Authority will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL. Your web server will match your issued SSL Certificate to your Private Key. Your web server will then be able to establish an encrypted link between the website and your customer's web browser.

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals.

Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

CionSystems active directory self-service application is a web based application. You can configure the application to use https instead of default http connection by following the below process. These steps are same as you would take for protecting any website.

Note: This document describes a generic process for configuring web based application along with a way to obtain generic certificates. For your specific needs you need to contact the certificate authorities or certificate vendor to obtain the right certificate for your needs.

2. Prepare a certificate signing request
1. Choose start button and click on run
2. Now enter “inetmgr” and click on ok

3. IIS Manager window will open
4. Open the site window you want to protect. Here we are selecting default website
5. Right click on the selected site and click on properties option and it will open the selected site properties window
6. From property window, select the directory security tab
7. Click the button labeled server certificate to start the webserver.

**Note:** If the Server Certificate button is not available or button is disabled. Follow the below process. If Server Certificate button is available or button is enabled then follow step 8.

2.1 If the Server Certificate button is not available or button is disabled

**SYMPTOMS:** When you try to generate a certificate request by using the Internet Information Services (IIS) Certificate Wizard from the properties of a site, the **Server Certificate** button may be unavailable or you may receive an error message similar to the following:

**Error:** The Instruction at "0X64e6a38e" referenced memory at 0X00000000. The memory could not be "read".

Note: You may also see the IIS Manager close without error.

**CAUSE:** The Xenroll.dll file is not properly registered.

**RESOLUTION:** Xenroll.dll is located in the \Winnt\System32 directory.
**Note:** Winnt is your %windir% directory. Follow these steps to reregister Xenroll.dll:

1. Open Windows Explorer, expand the **Winnt** directory, and then click the **System32** directory.
2. Click **Start**, click **Run**, and then type Regsvr32 in the text box.
3. In Windows Explorer, locate Xenroll.dll in the \Winnt\System32 directory, and then drag Xenroll.dll into the text box that is described in step 2.
4. Click **OK**. A message box states that the Xenroll.dll registration is successful.

If registering the Xenroll.dll file does not resolve this issue, register the following additional files by using the same steps:

- \%systemroot%\system32\inetsrv\certmap.ocx
- \%systemroot%\system32\inetsrv\certwiz.ocx

Close the IIS Properties window, and then open the Web site properties. Verify that you can create a certificate request.

**MORE INFORMATION:** The Certwiz.ocx control wizard calls the Xenroll.dll dynamic-link library (DLL) when you click **Server Certificate**.

**Steps to reproduce the behavior**

1. Open Windows Explorer, expand the Winnt directory, and then click the System32 directory.
2. Click **Start**, click **Run**, and then type Regsvr32 /u in the text box.
3. In Windows Explorer, locate Xenroll.dll in the \WINNT\System32 directory, and then drag Xenroll.dll into the text box that is described in step 2.
4. Click **OK**. A message box states that the Xenroll.dll unregistration is successful.
5. Open the IIS Service Manager Microsoft Management Console (MMC), right-click a Web site, and then click **Properties**.
6. In the site property window, click the **Directory Security** tab.
7. Click **Server Certificate** to open the IIS Certificate Wizard. You receive the error message that is described in the "Symptoms" section.

8. Click the server certificate to begin the process

![Welcome to the Web Server Certificate Wizard]

**Welcome to the Web Server Certificate Wizard**

This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

**Status of your Web Server**

Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certwizard will help you to create a new certificate for this Web Server or attach to an existing certificate.

To continue, click **Next**.

9. Click **Next**
10. The first screen of the wizard asks you to select the number of options. In this case we want to Create a new certificate.
11. Select the create new certificate option and click next.

12. It will open the “Delayed or immediate request “window
13. Now select the “Prepare the request now, but send it later” option and click next.
14. Type the name of the certificate and click next

15. Enter the organization and organization unit name and click next
16. Type the common name of your certificate and click on next.
17. Enter the details of your country and state, city and click next

18. Enter the file name with .cer extension and click next
19. Request file summary will open and now click next

20. Click on finish.
Now you have completed the web server certificate wizard. A certificate request was created and saved to the file location c:\certreq.cer

Now go to the saved file path and open the file with notepad there we can find the CSR associated with the certificate request and it will be like this

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSDCCArECAQAwbTELMAkBGA1UEBhMCVVMxExAAMwIBAgYIKwYBBQUHAgEYDQgECDQgGCSqGSM49
...}
-----END NEW CERTIFICATE REQUEST-----

Copy the above encrypted data from notepad. Next process is to request the certificate from certificate authority. Follow the below process to request the certificate.

3. Request a certificate from certificate vendor or Submit a certificate Request

3.1 Procedure 1:
To submit a certificate request, follow these steps:

1. Open a browser, and then open http://YourWebServerName/certsrv/.
2. Select Request a Certificate, and then click Next.
3. Select Advanced Request, and then click Next.
4. Select the center option, Submit a Certificate Request using a Base64, and then click Next.

5. In Notepad, open the request document that you created in the first procedure section, "Create a Certificate Request".
6. Copy the contents of the document.

NOTE: If you save the document with the default name and location, it is located at C:\Certreq.txt.

7. Paste the contents of the document in the Base64 Encoded Certificate Request text box of the Web form.

8. Click Submit.

9. If Certificate Server is set to Always Issue the Certificate, you are immediately directed to the Certificate Issued page. The address bar reads: http://YourWebServerName/certsrv/certfnsh.asp

On this page, you can download the Web server certificate immediately. To do so, follow these steps on the Certificate Issued page:

- Click the top link, Download Certification Authority Certificate (do not click Download Certification Authority Certificate path).
- When you are prompted, select Save this file to disk and save the certificate to your desktop or another location that you will remember.
- Now, go straight to the "Install the Certificate" section.
10. If Certificate Server is set to Set the certificate request status to pending, you will receive the following "Certificate Pending" message:

“Certificate Pending. Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested. Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate.”

Note: Save the provided certificate some where accessible. What you get back from a certificate vendor depends on the vendor you choose. Save this file to a location accessible from your web server. When you save the file make sure that it has .cer extension I have saved my file as “cion.cer”.
3.2 Procedure 2:

ipsCA, which provides free three months certificate. During this process need to provide the certificate company with information validating your or your company ID. Some consider this part as hassle but it is important part of over all SSL chain. After all you don’t want just anyone receiving a certificate that uses your company name. The certificate request process varies by Certificate Company.

Here is the URL to send the request for the certificate. By clicking this URL we will get a request form.

http://certs.ipsca.com/srvc/Free_SSL.asp?prim=1
1. Open the URL.
2. Click Type of certificate.
3. Fill customer contact information.
4. Open c:\certreq.cer with notepad
5. Paste the encrypted data included -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----
6. Click on submit.
7. Open your own Email ID.
8. You will get mail from Email ID: ssservers@ipsca.com
9. Copy the Request Ticket Number: 00006820782200924146708
10. Paste the Request Ticket Number in the above URL.
11. All the 1 to 7 CSR generation methods status will change from PENDING to DONE.
12. Download the file. Save with .cer extension.

Note: Once you complete the vendor’s certificate request form and you will need to wait for the SSL certificate to be delivered to your inbox.
4. Install the certificate

After making sure that your webserver can access the certificate file, you need to install the new certificate by completing the certificate process.

1. Open the Internet Information Services (IIS) Manager
2. In the IIS Manager expand the server (local computer)
3. Right click on the website to which want to install the received certificate and from shortcut menu choose the properties.
4. From the properties window select the directory security tab.
5. Click the server certificate button
6. From the first wizard screen, “Process the pending request and install the certificate”.

7. Click Next.
8. Provide the path and file name of the certificate which saved in step 3.
9. Click Next

10. Decide which port the website will use for website traffic
11. The summary screen will display the information which is found in certificate
12. Click next and click finish.
5. Install necessary intermediate certificate

Unless you are working with one of the big SSL players it is likely that you will need to install intermediate certificate that completes verification chain from your individual certificate up to a trusted root certificate. You can tell your server is ready by clicking the view certificate button.

13. Click on view certificate button
6. Issue a Certificate

In order to complete the certificate, you need to install an intermediary certificate that sits between a root certificate and a certificate you just installed

1. Choose start | Run and type “mmc”. This starts Microsoft management console.

2. From the management console select file | Add/Remove snap in.
3. In add/remove snap in window click add button.
4. In the add standalone snap in window, select certificates.
5. Click the add button
6. Choose computer account
7. Click Next
8. Make sure that local computer option is selected
9. Click finish
10. Close the add standalone snap in window
11. Click the ok button in add/remove snap in dialog to return to the MMC window
12. Expand the certificate option until you see the “Intermediate certification authorities”
13. Right click on Intermediate certification authorities and from the short cut menu choose All tasks | Import
14. This will start the SSL certificate import wizard
15. Click the browse button and locate the intermediate certificate file that you provided from the certificate provider.

**Certificate Import Wizard**

**File to Import**

Specify the file you want to import.

File name:

C:\Documents and Settings\Administrator\Desktop\cion.cer

**Note:** More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)
16. Click Next.
17. Choose "Place all certificates in the following store," making sure that "Intermediate Certification Authorities" is the selected store.

18. Click Next.
19. Click Finish. If everything goes as planned Windows will indicate that the import was successful. After completing the installation of intermediate certificate you should check the require secure channel in edit button under secure communication.

7. Checking the require secure channel
1. Click the Edit button in directory security tab

2. Check the option “Require secure channel” option

3. Click ok

4. Now again click on ok button in Directory security tab

8. Test

Once you complete, browse to the new site using https

Contact Notes:
For technical support or feature requests, please contact us at Support@CionSystems.com or 425.605.5325

For sales or other business inquiries, we can be reached at Sales@CionSystems.com or 425.605.5325

If you’d like to view a complete list of our Active Directory Management solutions, please visit us online at www.CionSystems.com

Disclaimer
The information in this document is provided in connection with CionSystems products. No license, express or implied, to any intellectual property right is granted by this document or in connection with the sale of CionSystems products. EXCEPT AS SET FORTH IN CIONSYSTEMS’LICENSE AGREEMENT FOR THIS PRODUCT, CIONSYSTEMS INC. ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL CIONSYSTEMS INC. BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF