TECHNICAL DOCUMENTATION

XpressConnect
Enrollment System

Integration Module for Microsoft CA Setup Guide

Software Release 4.2

December 2015

Summary: This document describes the deployment requirements for the Integration Module for Microsoft CA, how to configure the Enrollment System for the Integration Module, how to download the Integration Module, and how to configure the web server. This guide also includes information for testing and troubleshooting the system.

Document Type: Configuration

Audience: Network Administrator

+1 303.647.1495 | +44 (01) 161.261.1400 | support@cloudpath.net | ©2015 Cloudpath Networks, Inc. | www.cloudpath.net

XpressConnect Enrollment System Integration Module for Microsoft CA Setup Guide

Software Release 4.2

December 2015

Integration Module for Microsoft CA
Setup Guide

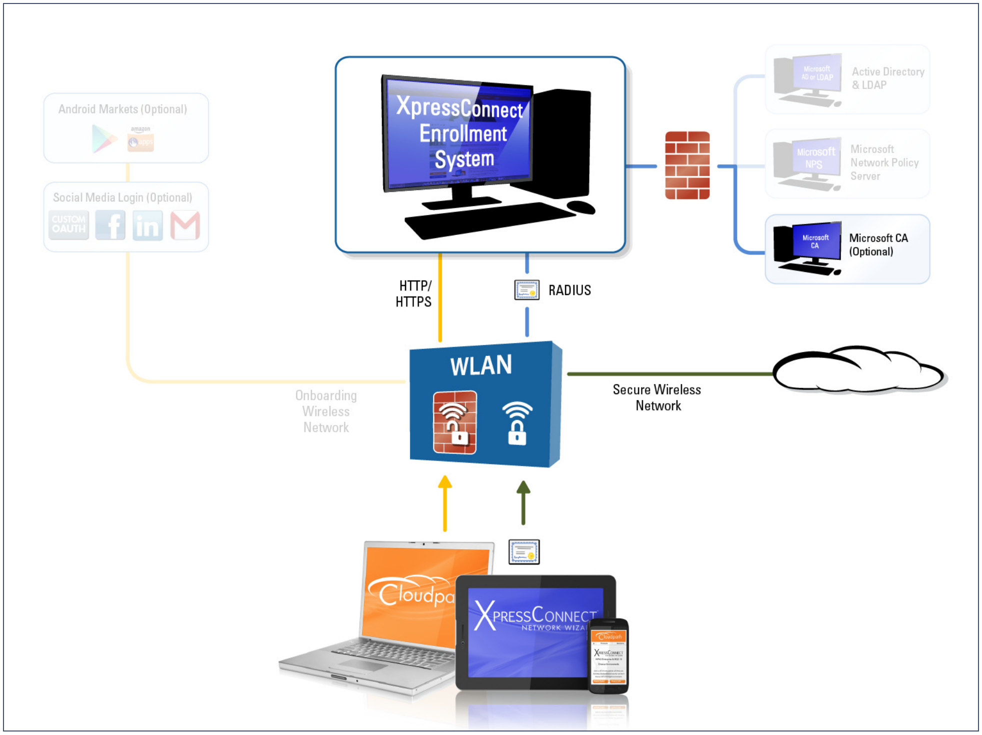
Overview

To implement certificate-based authentication on your WPA-2 Enterprise and 802.1X network, through EAP-TLS, you must set up a certificate infrastructure, which includes a certificate authority (CA) for issuing client certificates.

The XpressConnect Integration Module for Microsoft CA allows XpressConnect to request TLS client certificates from your existing Microsoft CA infrastructure.

While configuring a user's device, XpressConnect prompts the user for credentials. It then generates a CSR, authenticates to the CA, and sends the CSR to the CA via the Integration Module. The Integration Module, in coordination with the CA, authenticates the user and, if valid credentials are provided, signs a certificate for the user. The characteristics of the certificate generated are dictated by the certificate template utilized. The certificate is then streamed back to the XpressConnect Wizard, which installs it and configures the SSID to utilize it.

FIGURE 1. XpressConnect Integration Module for Microsoft CA


Android Markets (Optional)
amazon
Social Media Login (Optional)
CUSTOM OAUTH
XpressConnect Enrollment System
Microsoft AD or LDAP
Active Directory & LDAP
Microsoft NPS
Microsoft Network Policy Server
Microsoft CA
Microsoft CA (Optional)
HTTP/ HTTPS
RADIUS
WLAN
Secure Wireless Network
Onboarding Wireless Network
Cloudpath
XpressConnect Network Wizard

Note >>
The Integration Module for Microsoft CA is essentially a sibling to Microsoft Network Device Enrollment Service (NDES). Unlike Microsoft NDES, which assigns all certificates to the SCEP_ADMIN user account, the Integration Module assigns each issued certificate to the corresponding user account.

Integration Module Specifications

Recommendation

We recommend that you do not install the Integration Module on a domain controller. By default, you cannot run a web server on a domain controller unless you change policy settings. Also, users typically do not have LOGON_INTERACTIVE rights for domain controllers, as they do for other machines.

Deployment Requirements

- Install on a Windows Domain-joined Microsoft Windows 2008 R2 (IIS) or greater web server. Other servers in the network including the CA and DC can be Windows 2003.
- The web server must meet Microsoft's minimum system requirements.
- The web server should contain a valid certificate to enable HTTPS communication.
- Optionally, the Integration Module can be installed directly onto the CA or RA server.
- The Enrollment System must be able to interact with the CA via a URL. We strongly recommend that this URL be HTTPS to provide web server authentication and a secure communication over your network.
- The website that contains the CA's web interface should be configured for appropriate *Anonymous* authentication.
- To allow communication between the Enrollment Server and the CA, ensure that your firewall is configured for ports 80/443 (HTTP/HTTPS).

Deployment Process

Follow these steps to deploy the Integration Module for the XpressConnect Enrollment System.

- Configuring the Enrollment System, page 3
- Downloading the Integration Module, page 5
- Configuring the Web Server, page 6
- Testing the System, page 10

What You Need

You need the following information to setup the Integration Module for Microsoft CA:

- CA Host Name of the server with which the plug-in should communicate.
- CA Name, which is the primary label for the CA within the Certification Authority snap-in.
- Request Attributes for the certificate template.

Configuring the Enrollment System

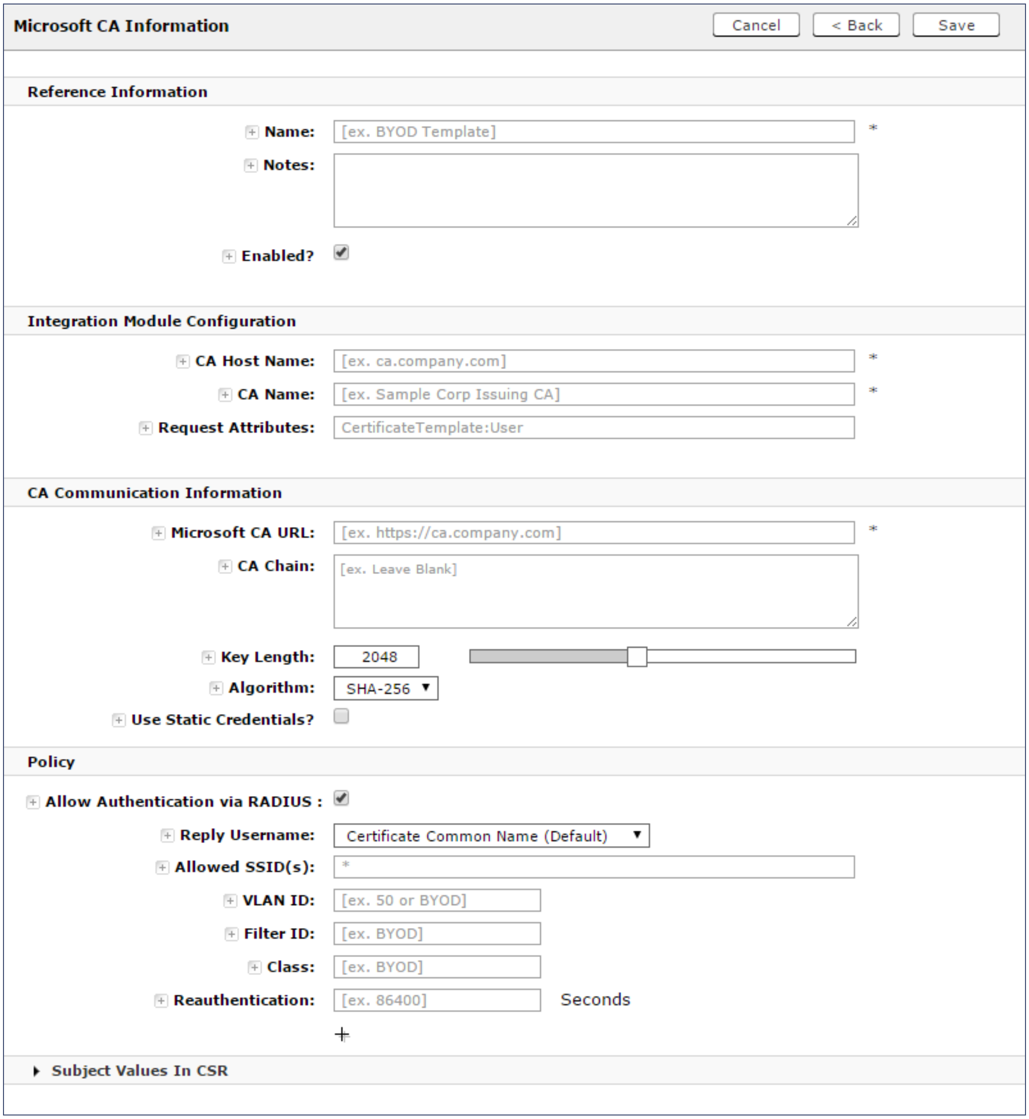
Use these steps to set up a certificate template for the Microsoft CA. The certificate template allows the certificates to be pulled from the Microsoft CA.

Create a Microsoft CA Certificate Template

Use these steps to set up a certificate template for the Microsoft CA. The certificate template allows the certificates to be pulled from the Microsoft CA.

1. Navigate to *Certificate Authority > Manage Templates.*
2. Click *Add Template* to create a new certificate template.
3. Select *Use a Microsoft Certificate Authority*. Click *Next*.

FIGURE 2. Microsoft CA Certificate Template Information



Microsoft CA Information

Reference Information

Name: [ex. BYOD Template] *

Notes:

Enabled? ☑

Integration Module Configuration

CA Host Name: [ex. ca.company.com] *

CA Name: [ex. Sample Corp Issuing CA] *

Request Attributes: CertificateTemplate:User

CA Communication Information

Microsoft CA URL: [ex. https://ca.company.com] *

CA Chain: [ex. Leave Blank]

Key Length: 2048

Algorithm: SHA-256

Use Static Credentials? □

Policy

Allow Authentication via RADIUS : ☑

Reply Username: Certificate Common Name (Default)

Allowed SSID(s): *

VLAN ID: [ex. 50 or BYOD]

Filter ID: [ex. BYOD]

Class: [ex. BYOD]

Reauthentication: [ex. 86400] Seconds

Subject Values In CSR

4. On the *Microsoft CA Information* page, enter the *Name* and *Notes* for the certificate template, and *Enable* it for use.

5. Enter the *Integration Module Configuration* settings. These are required fields.

   - CA Host Name - The DNS name of the CA server.
   - CA Name - The name of the CA, which appears in the Certificate Authority console.

Note >>

The *CA Name* should be the name of the CA as displayed in the Certificate Authority snap-in. On Windows, it also displays in the *Issued By* field when a certificate is viewed in the CertMgr.

- Request Attributes - The attributes used when querying the CA. This typically includes, at a minimum, the certificate template name. For example, *Certificate Template:User*.

6. Enter the *Communication Information* and *Save*. The Microsoft CA URL is a required field.

- Microsoft CA URL - Enter URL where the Microsoft CA is installed. You must enter the complete URL, for example, *https://msft-ca.testcompany.com*.

Tip >>

If using multiple certificate templates with the Microsoft CA, the CA URL should reflect the certificate template name. For example, if you create one certificate template for staff, and one for guests, the Microsoft CA URLs should be *https://msft-ca.testcompany.com/staff*, and *https://msft-ca.testcompany.com/guests,* respectively. See Multiple Certificate Templates.

- CA Chain - Specify the CA Chain. The client configuration must include the root, and if applicable, the intermediate CAs. The certificates should be concatenated together in PEM format.
- Key Length - The key length, as dictated by the CA, for certificate signing requests.
- Algorithm - The algorithm, as dictated by the CA.
- Use Static Credentials - By default, the system uses user-provided credentials when interacting with the Microsoft CA. Check this box if you want to configure static username and password to use when interacting with the Microsoft CA.

7. Specify policy information for the RADIUS server. If enabled, the RADIUS server will contain policy information for this certificate template.

- Reply Username - The RADIUS server replies with the username based on the CN of the certificate but, additional options are available.
- Allowed SSID - Enter a regex, which defines the SSID(s) from which devices are allowed to authenticate.
- RADIUS Attributes - Specify a VLAN, Filter ID, Class, Reauthentication interval, or use the plus icon to add custom attributes.

8. Use the *Specify Subject Values In CSR* settings if you want to configure the subject of the CSR destined for Microsoft CA when the template is set to "Supply in request".

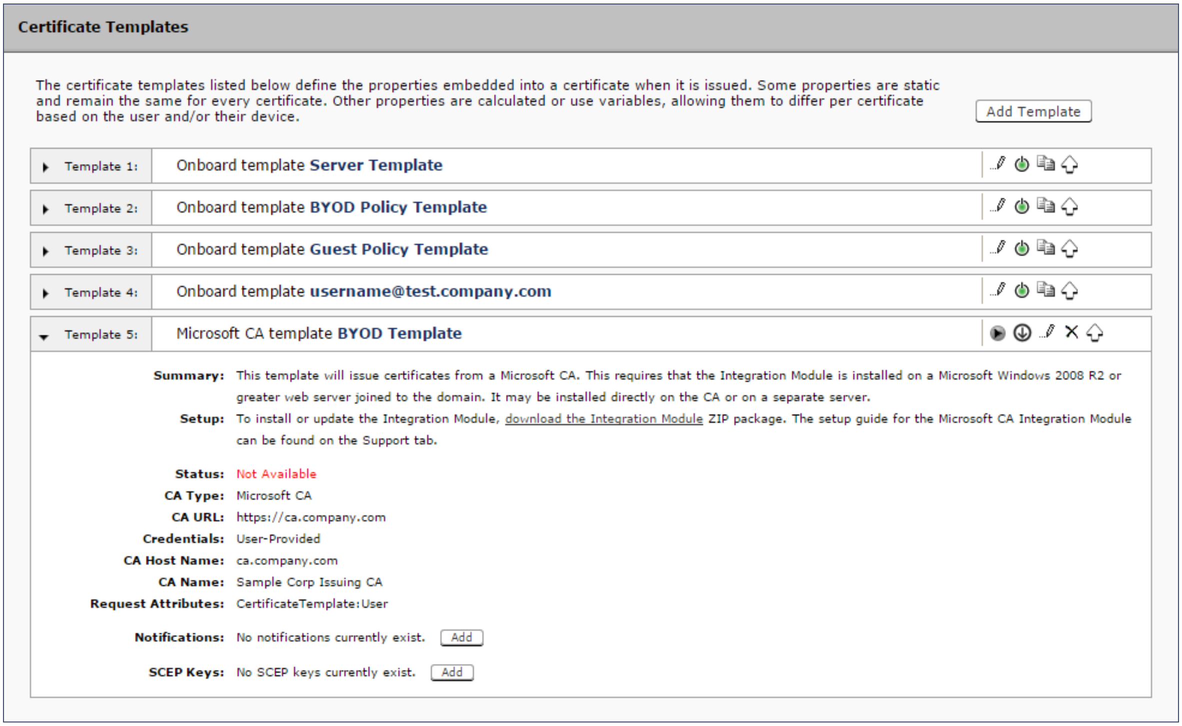
Downloading the Integration Module

The Integration Module for Microsoft CA is downloaded from the Enrollment System *Certificate Templates* page. It downloads as a compressed Zip file.

1. Go to *Certificate Authority* > *Certificate Templates*.

2. On the *Certificate Templates* page, click the download icon ⬇ to download the Integration Module.

FIGURE 3. Download Integration Module for Microsoft CA



Certificate Templates

The certificate templates listed below define the properties embedded into a certificate when it is issued. Some properties are static and remain the same for every certificate. Other properties are calculated or use variables, allowing them to differ per certificate based on the user and/or their device.

- Template 1: Onboard template **Server Template**
- Template 2: Onboard template **BYOD Policy Template**
- Template 3: Onboard template **Guest Policy Template**
- Template 4: Onboard template **username@test.company.com**
- Template 5: Microsoft CA template **BYOD Template**

Summary: This template will issue certificates from a Microsoft CA. This requires that the Integration Module is installed on a Microsoft Windows 2008 R2 or greater web server joined to the domain. It may be installed directly on the CA or on a separate server.

Setup: To install or update the Integration Module, download the Integration Module ZIP package. The setup guide for the Microsoft CA Integration Module can be found on the Support tab.

Status: Not Available
CA Type: Microsoft CA
CA URL: https://ca.company.com
Credentials: User-Provided
CA Host Name: ca.company.com
CA Name: Sample Corp Issuing CA
Request Attributes: CertificateTemplate:User

Notifications: No notifications currently exist. Add

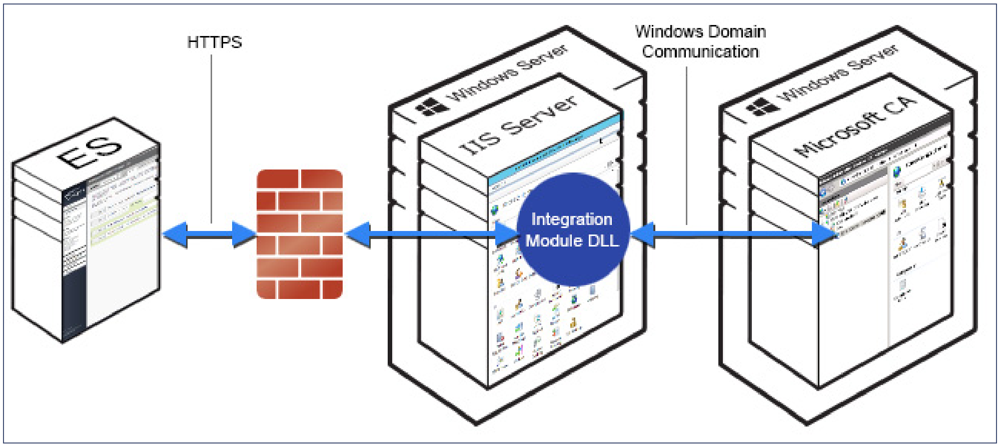
SCEP Keys: No SCEP keys currently exist. Add

Configuring the Web Server

The Integration Module is placed in IIS on a Windows 2008 or Windows 2012 Server. The server may or may not be on the same server as the CA, but it must be on the same domain as the CA. At a minimum, the web server must have the *ASP.NET* role services installed.

The following diagram illustrates how the different systems work together, including the communication ports between the components, and where the different pieces of data reside.

FIGURE 4. Example of ES with Microsoft CA in a Network



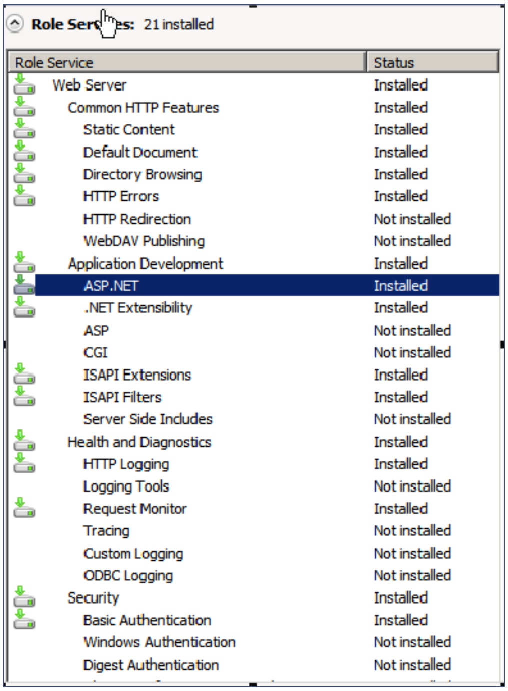
Use the steps outlined in the following sections to set up your IIS server.

Verify Role Services

Use this procedure to verify the role services in the Service Manager.

1. Open the Server Manager.
2. In the left tree view, expand *Roles* and select *Web Server (IIS)*.

FIGURE 5. Role Services Installed on the IIS



Role Services: 21 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Installed
HTTP Errors	Installed
HTTP Redirection	Not installed
WebDAV Publishing	Not installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Not installed
CGI	Not installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Not installed
Health and Diagnostics	Installed
HTTP Logging	Installed
Logging Tools	Not installed
Request Monitor	Installed
Tracing	Not installed
Custom Logging	Not installed
ODBC Logging	Not installed
Security	Installed
Basic Authentication	Installed
Windows Authentication	Not installed
Digest Authentication	Not installed

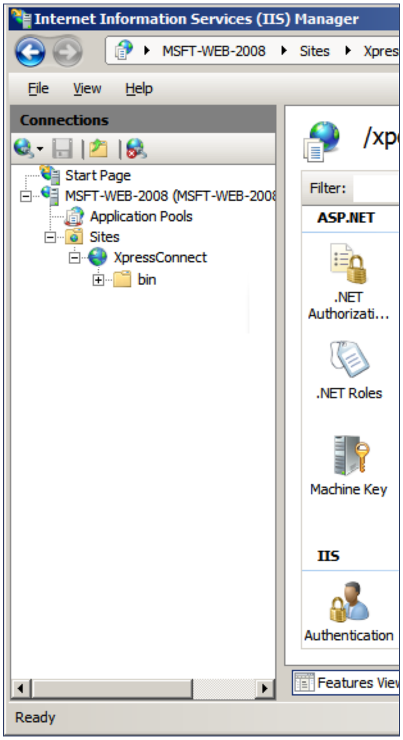
3. In the right window, scroll down to the *Role Services* section. In the list, locate *ASP.NET* and verify that it has the *Installed* Status.

Set Up the Integration Module Website

How to Add the Integration Module Website

1. On the file system, locate the folder where the Integration Module will reside. In most cases, the physical path is similar to *C:\inetpub\xpressconnect.*
2. Create this folder and unzip the downloaded plug-in file into it. The folder should contain the files *Default.aspx and Web.config*, among others.
3. In the IIS Manager, locate and select the *Sites* item in the left tree.
4. Right-click and select *Add Website…*
5. Name the site *XpressConnect*.

FIGURE 6. Site Structure in IIS Manager



6. Set the IP address, port and host name appropriately.
7. Set the physical path to the folder created above (for example *C:\inetpub\xpressconnect*), and click *OK*.

Multiple Certificate Templates

If using multiple certificate templates (for example one for staff, *https://msft-ca.testcompany.com/staff*, and one for guests, *https://msft-ca.testcompany.com/guests),* create a parent application for *https://msft-ca.testcompany.com,* and two child applications for staff and guests.

Note >>

The parent and child applications must be set up with *Anonymous* Authentication Type.

In multiple certificate template configurations, the parent application cannot contain the plug-in files (*Default.aspx, Web.config, etc.*). You must download the plug-in files into the corresponding child application directories.

For example, Download the plug-in files from the *staff* certificate template and place them in the *https://msft-ca.testcompany.com/staff* application directory, and download the plug-in files from the *guests* certificate template and place them in the *https://msft-ca.testcompany.com/guests* application directory.

Testing the System

Verify Communication Between the ES and the Microsoft CA

After the Integration Module is deployed, you can test the communication between the Enrollment System and the Microsoft CA. The query allows you to enter user credentials and verify interaction with the configured Microsoft CA.

1. From the *Certificate Templates* page, click the Test Integration Module icon ▶.
2. On the *Test Microsoft CA* page, enter user credentials to verify Microsoft CA interaction with the Enrollment System and *Continue*.

The *Microsoft CA Test* page displays the results of the query.

Troubleshooting

DNS

Verify that the Microsoft CA can resolve DNS.

CA Name

Verify that CA name is correct. The CA name is case-sensitive.

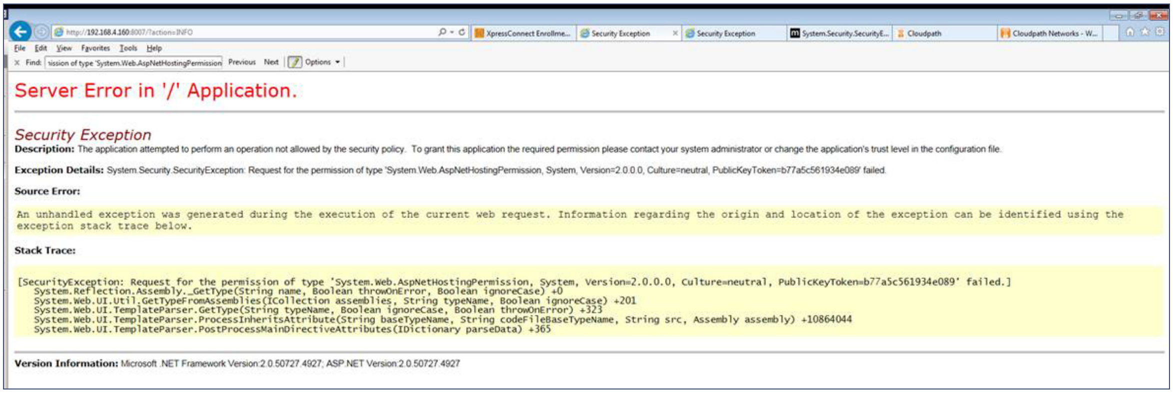
ASP.NET Installed on the IIS Server

If the Application Settings icon does not appear on the IIS server, Verify that ASP.NET is installed on the IIS server. The entire ASP.NET icon set, which includes *Application Settings*, will not display if ASP.NET is not installed.

ASP Hosting Permissions

If you receive the following *Security Exception* error when trying to access http://site/?action=INFO, this typically indicates that the web server cannot use the files.

FIGURE 7. Security Exception Error


http://192.168.4.160:8007/?action=INFO
XpressConnect Enrollme...
Security Exception
Security Exception
System.Security.SecurityE...
Cloudpath
Cloudpath Networks - W...
File Edit View Favorites Tools Help
Find: ission of type 'System.Web.AspNetHostingPermission
Previous
Next
Options

Server Error in '/' Application.

Security Exception

Description: The application attempted to perform an operation not allowed by the security policy. To grant this application the required permission please contact your system administrator or change the application's trust level in the configuration file.

Exception Details: System.Security.SecurityException: Request for the permission of type 'System.Web.AspNetHostingPermission, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' failed.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the
exception stack trace below.
```

Stack Trace:

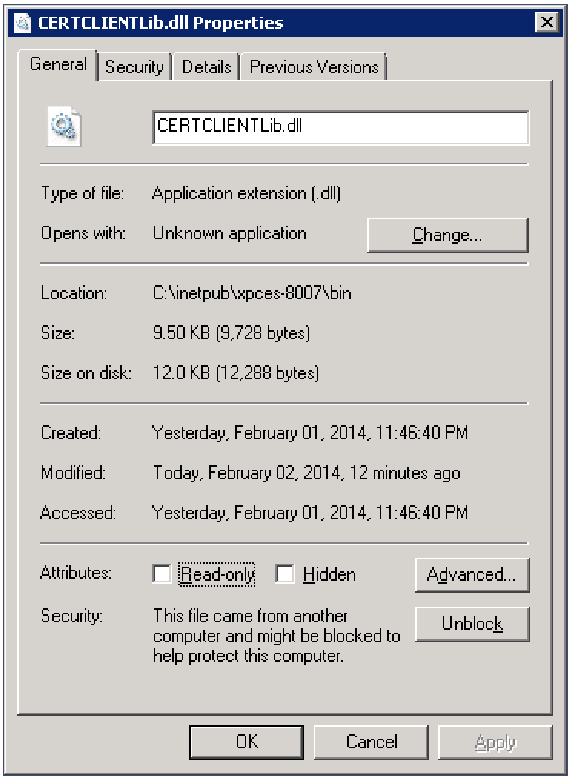
```
[SecurityException: Request for the permission of type 'System.Web.AspNetHostingPermission, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089' failed.]
   System.Reflection.Assembly._GetType(String name, Boolean throwOnError, Boolean ignoreCase) +0
   System.Web.UI.Util.GetTypeFromAssemblies(ICollection assemblies, String typeName, Boolean ignoreCase) +201
   System.Web.UI.TemplateParser.GetType(String typeName, Boolean ignoreCase, Boolean throwOnError) +323
   System.Web.UI.TemplateParser.ProcessInheritsAttribute(String baseTypeName, String codeFileBaseTypeName, String src, Assembly assembly) +10864044
   System.Web.UI.TemplateParser.PostProcessMainDirectiveAttributes(IDictionary parseData) +365
```

Version Information: Microsoft .NET Framework Version:2.0.50727.4927; ASP.NET Version:2.0.50727.4927

The key piece of information in this error message is *System.Web.AspNetHostingPermission*. When Internet Explorer encounters the files in the Integration Module zip files, it flags them as originating from the Internet, and blocks them.

To verify this, right-click one of the Integration Module files and view the *Properties*. With the *General* tab selected, in the *Security* section, you see a message: *This file came from another computer and might be blocked to help protect this computer*.

FIGURE 8. Integration Module Zip Files Properties



CERTCLIENTLib.dll

Type of file: Application extension (.dll)

Opens with: Unknown application

Location: C:\inetpub\xpces-8007\bin

Size: 9.50 KB (9,728 bytes)

Size on disk: 12.0 KB (12,288 bytes)

Created: Yesterday, February 01, 2014, 11:46:40 PM

Modified: Today, February 02, 2014, 12 minutes ago

Accessed: Yesterday, February 01, 2014, 11:46:40 PM

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

To correct this issue, check each file in the directory and *Unblock* any files that are listed as *Blocked*.

Restart the IIS Server

To apply these changes, the IIS Server must be restarted from the root node.

Note >>
Restarting the application does not apply the changes. You must restart the IIS server from the root node.

Terminology

TABLE 1. **Terminology**

Term	Definition
Certificate	A digital credential that provides information about the identity of an entity and is issued by a certification authority (CA).
Certificate Authority (CA)	An entity that issues and manages certificates, and guarantees the validity of the information in the certificate by signing the certificate with its own private key.
Certificate chain	A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate.
Certificate template	Certificate templates are used to generate certificates. A template defines the properties embedded into a certificate when it is issued.
Device Configuration	A concept used with the XpressConnect Enrollment System to group configuration settings. Each network contains a single configuration per operating system. A device configuration within XpressConnect represents a physical network within your environment.
HTTPS certificate	Also called an SSL certificate, or web server certificate, an HTTPS certificate allows you to host secure pages on your website.
Intermediate CA	A CA below another CA in a certificate chain is called an intermediate (or subordinate) CA. Intermediate CAs are trusted only if they have a valid certification path from a trusted root CA.
Role service (Windows Server)	Software programs that provide the functionality of a role. When you install a role, you can choose which role services the role provides for other users and computers in your enterprise.
Root CA	The trust anchor for a digital certificate hierarchy.
SSID	A unique identifier that wireless networking devices use to establish and maintain wireless connectivity.
Secure Wireless Network	A WPA2-Enterprise wireless network.
Server Certificate	The public portion of the certificate used by the RADIUS server. The server certificate does not contain the private key and is safe to distribute. The RADIUS server provides the server certificate to every device that attempts to connect.
TLS client certificate	The transport layer security (TLS) certificate submitted by the client’s web browser when the SSL protocol provides authentication during the login process. This certificate contains information about the client and about the organization that issued the certificate.

Additional Documentation

You can find detailed information in the Enrollment System configuration guides, located on the left-menu *Support* tab of the ES Admin UI.

About Cloudpath

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the XpressConnect Enrollment System and how it can simplify your wireless environment, visit www.cloudpath.net or contact a Cloudpath representative.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

Contact Information

General Inquiries:info@cloudpath.net

Support:support@cloudpath.net

Sales:sales@cloudpath.net

Media:media@cloudpath.net

Marketing:marketing@cloudpath.net

Phone:+1 303.647.1495 (US)
+1 866.472.6053 (US)
+44 (01) 161.261.1400 (UK)

Fax:+1 760.462.4569

Address:1120 W 122nd Ave, Suite 302
Westminster, CO 80234 USA