Cloudpath

Cloudpath Enrollment System

Issuing Certificates From a Microsoft CA Configuration Guide

Software Release 5.0

December 2016

Summary: This document describes the deployment requirements for the Integration Module for Microsoft CA, which allows you to issue certificates from a Microsoft CA, how to configure Cloudpath 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

Cloudpath

Issuing Certificates from a Microsoft CA Configuration Guide

Software Release 5.0

December 2016

Issuing Certificates from a Microsoft CA Configuration Guide

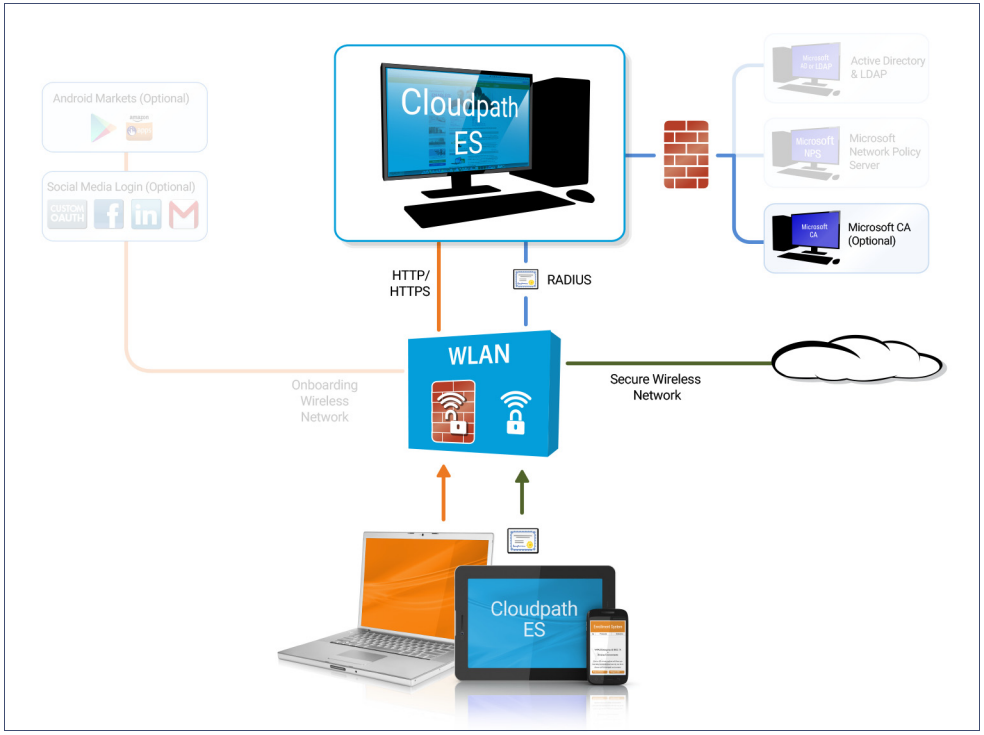
Overview

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

While configuring a user's device, Cloudpath 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 Cloudpath Wizard, which installs it and configures the SSID to utilize it.

FIGURE 1. Cloudpath Integration Module for Microsoft CA



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.
- Cloudpath 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 Cloudpath.

- "Configuring Cloudpath" on page 3
- "Downloading the Integration Module" on page 6
- "Configuring the Web Server" on page 7
- "Testing the System" on 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 Cloudpath

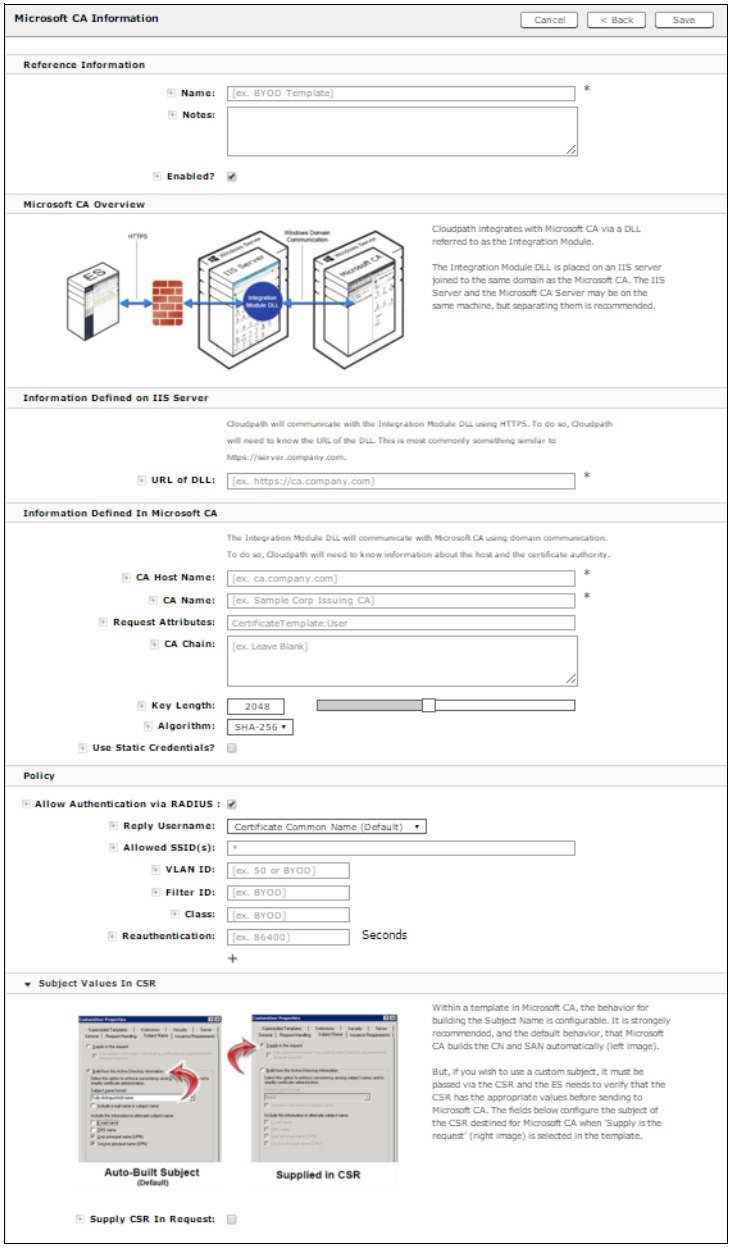
Use these steps to set up a certificate template for the Microsoft CA. The certificate template allows the certificates to be pulled from the Microsoft CA.

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



4. Enter the *URL of the DLL*. Cloudpath communicates with the Integration Module DLL using HTTPS. To do so, Cloudpath needs to know the URL of the DLL.

Note >>
If you configure or change settings in the Microsoft CA certificate template, you must download and install a new copy of the DLL and files.

5. On the *Microsoft CA Information* page, enter the *Name* and *Notes* for the certificate template, and *Enable* it for use.
6. 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*.
7. 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.
8. 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.

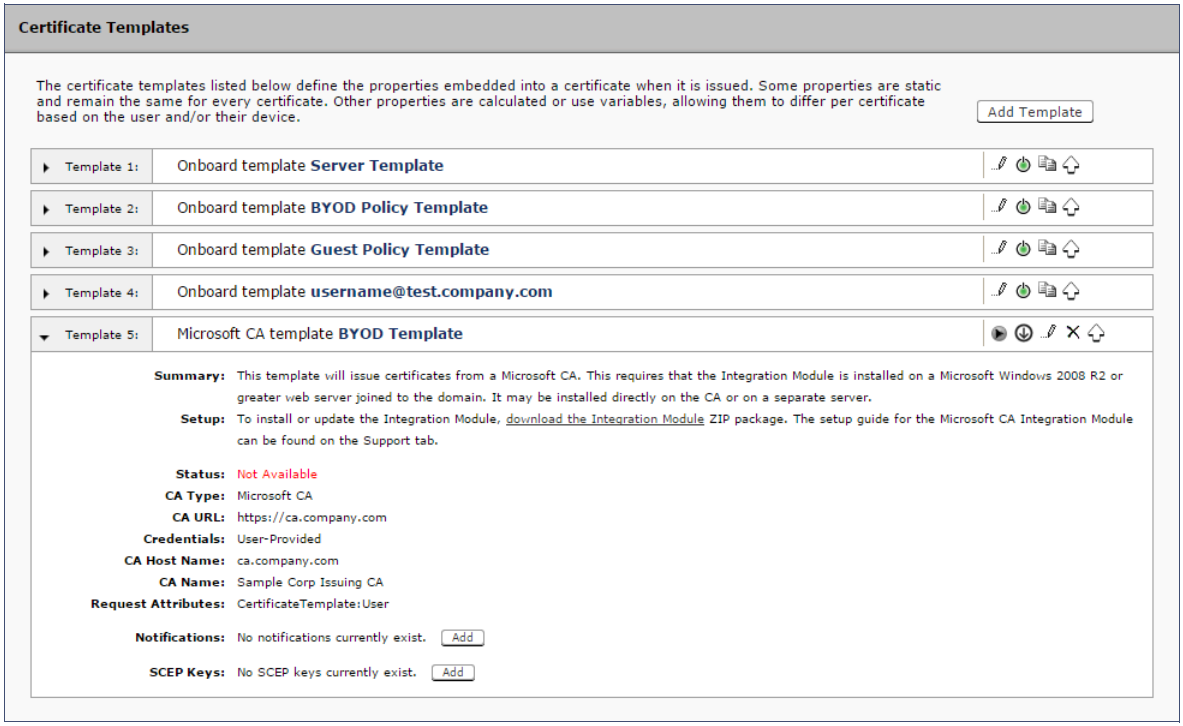
9. Use the *Specify Subject Values In CSR* settings if you want to configure the subject of the CSR destined for Microsoft CA when the template is set to "Supply in request".

Downloading the Integration Module

The Integration Module for Microsoft CA is downloaded from the Cloudpath *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

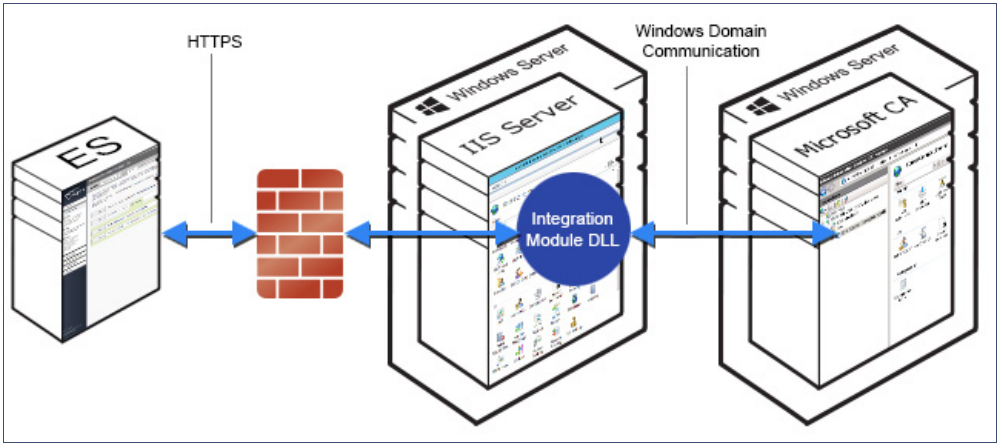


Configuring the Web Server

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 Cloudpath with Microsoft CA in a Network



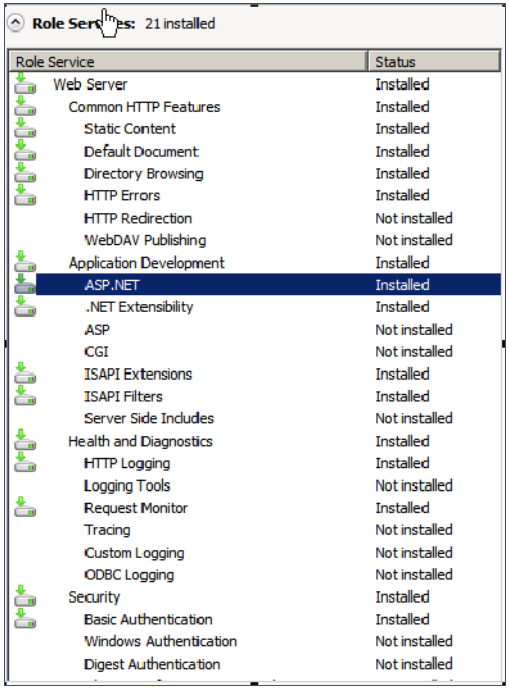
Use the steps outlined in the following sections to set up your IIS server.

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



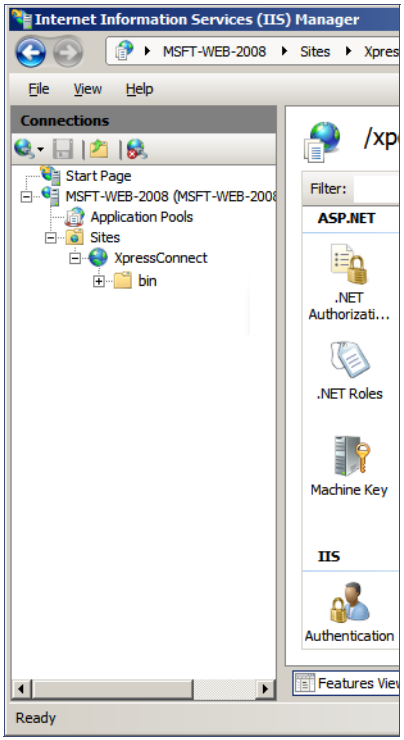
3. In the right window, scroll down to the *Role Services* section. In the list, locate *ASP.NET* and verify that it has the *Installed* Status.

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\cloudpath*
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 *Cloudpath*.

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\cloudpath*), 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 Cloudpath and the Microsoft CA

After the Integration Module is deployed, you can test the communication between Cloudpath 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 Cloudpath 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.

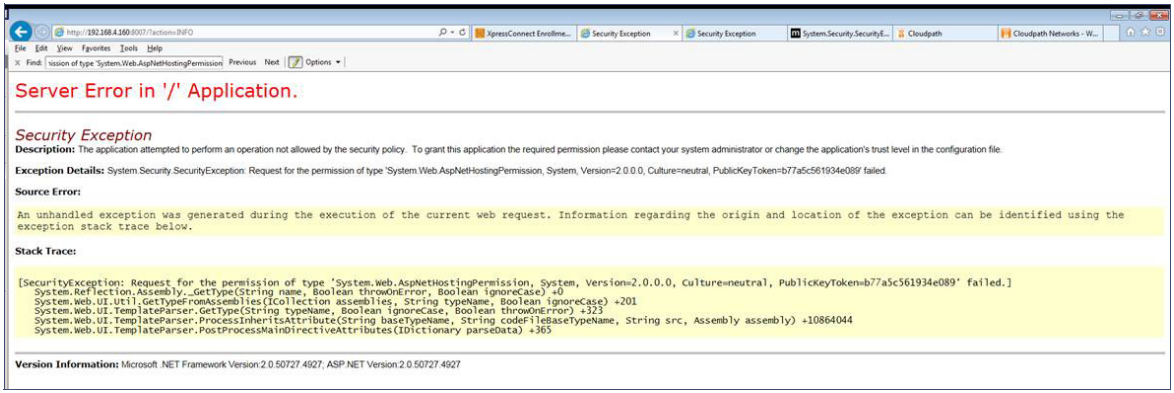
ASP.NET Installed on the IIS Server

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.

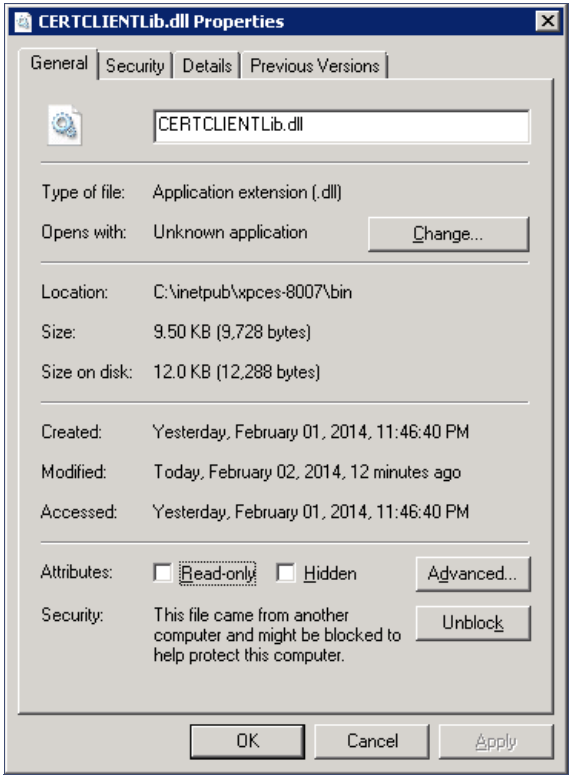
FIGURE 7. Security Exception Error



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



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.