Oracle® Argus Insight

Minimum Security Configuration Guide

Release 7.0.1

E28490-01

March 2012

This document describes how to configure security settings for the Argus Insight application. You configure these settings after you install Argus Insight. For details about installing the application, see the *Oracle Argus Insight Installation Guide*.

Contents

- Section 1, "Configuring PwReports.exe Permissions"
- Section 2, "Configuring Permissions in the Windows Registry"
- Section 3, "Granting Permission to IIS Metabase"
- Section 4, "Configuring Folder Access to the Web User Account"
- Section 5, "Configuring Application Pools"
- Section 6, "Configuring Permissions for Log/Application Files and Folders"
- Section 7, "Configuring HTTPS"

ORACLE®

1 Configuring PwReports.exe Permissions

You need to grant permissions to the PwReports.exe file, which is the executable for the Argus Insight application.

In addition, you need to create a domain user who will have access to the web servers and all network services that will be configured in Argus Insight. The instructions in this document use an example user, named *safety_user.* You need to substitute *safety_user* with the name of the domain user that you create.

> **Note:** You need to complete the instructions in this section for each web server and report server in your installation.

To configure the permissions for the Argus Insight application:

1. Go to the web server or the report server.

2. Click **Start** and select **Control Panel.**

3. Double-click **Administrative Tools.**

4. Double-click **Component Services.**

5. Navigate to **Console Root, Component Services, Computers, My Computer,** and select **DCOM Config.**
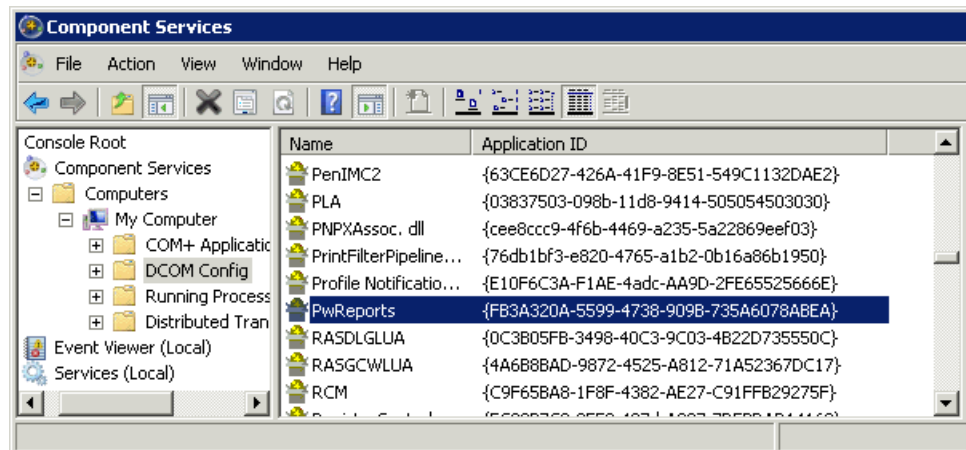

6. Right-click **PwReports** (that is, Argus Insight application) and select **Properties** from the menu.
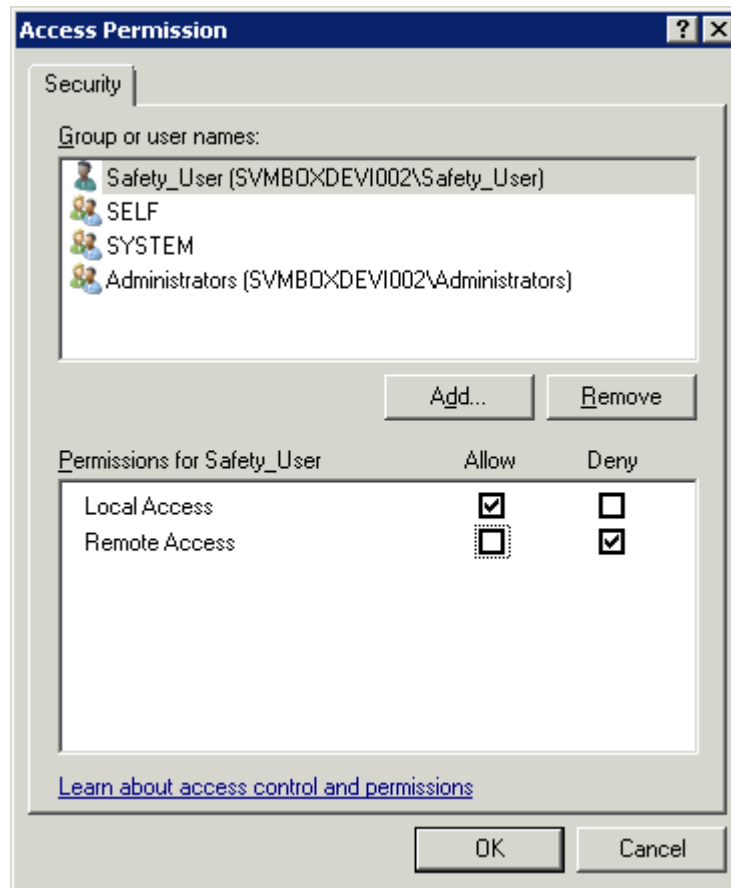
7. Click the **Security** tab.

8. Modify the **Launch and Activation Permissions** as follows:

a. Select the **Customize** option.

b. Click **Edit.** The Launch and Activation Permission dialog box opens.
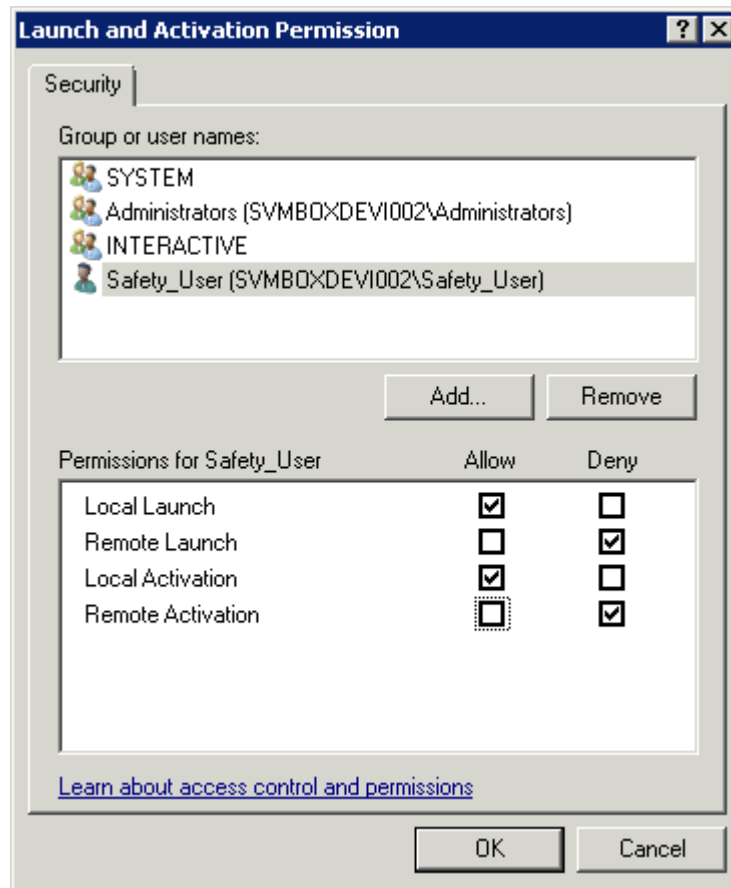
c. Click **Add** to add the domain user who will have launch and activation permissions.

d. Select the **Allow** check box for the **Local Launch** option and the **Local Activation** option.

e. Select the **Deny** check box for the **Remote Launch** option and the **Remote Activation** option.

f. Click **OK.**

g. Click **Yes** in response to the message about Deny permissions.
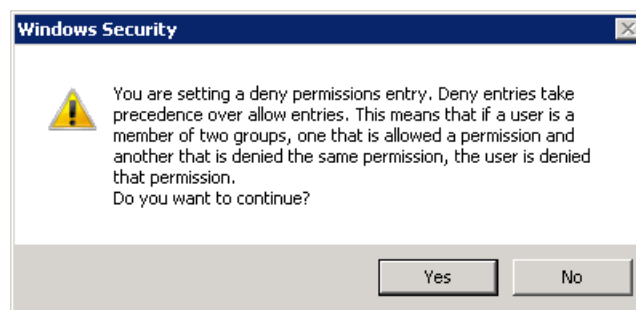
9. Modify the **Access Permissions** as follows:

    a. Select the **Customize** option.

    b. Click **Edit.** The Access Permission dialog box opens.

    c. Click **Add** to add the domain user who will have access permissions.

    d. Select the **Allow** check box for the **Local Access** option.

    e. Select the **Deny** check box for the **Remote Access** option.

    f. Click **OK.**

    g. Click **Yes** in response to the message about Deny permissions.

10. Modify the **Configuration Permissions** as follows:

    a. Select the **Customize** option.

    b. Click **Edit.** The Change Configuration Permission dialog box opens.
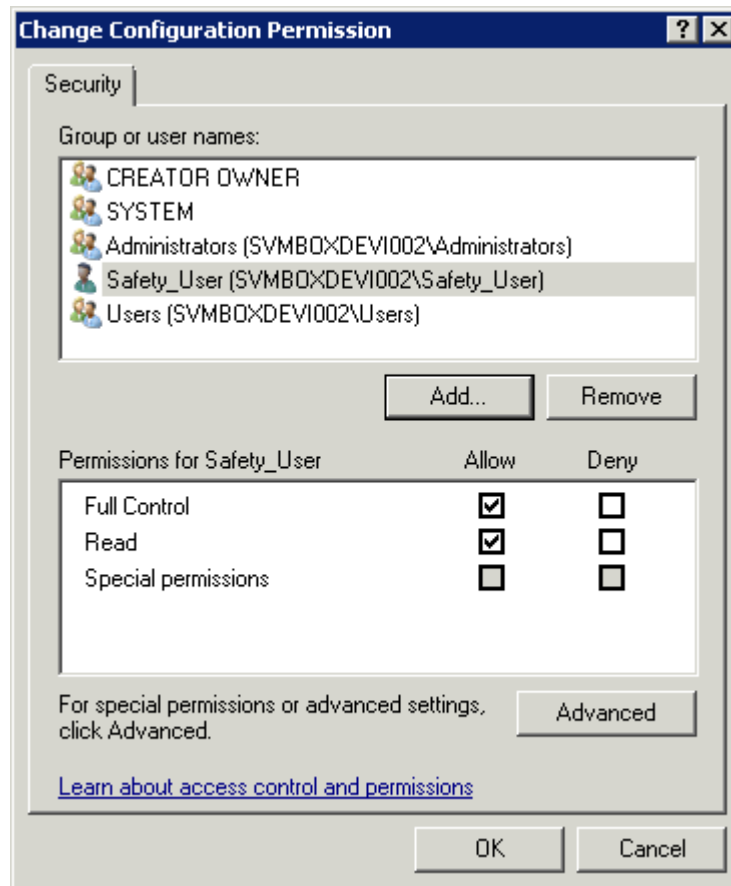
    c. Click **Add** to add the domain user who will have configuration permissions.

    d. Select the **Allow** check box for the **Full Control** option and the **Read** option.

    e. Click **OK.**

11. Click **OK** to save your changes and close the PwReports Properties dialog box.

2 Configuring Permissions in the Windows Registry

To configure permissions in the Windows system registry:

1. Open the Windows Registry Editor:

    a. Click **Start** and select **Run.**

    b. Enter **regedit.**

    c. Click **OK.**

2. Navigate to the following folder:

    HKEY_USERS\S-1-5-20

3. Right-click the **S-1-5-20** folder and select **Permissions.** The Permissions for
S-1-5-20 dialog box opens.
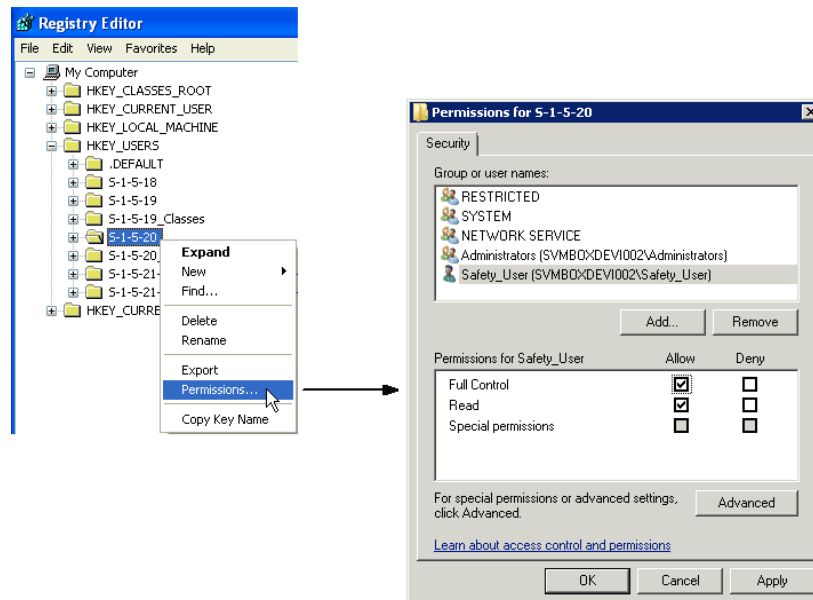
4. Click **Add** to add the domain user.

5. Select the **Allow** check box for the **Full Control** option.

6. Click **OK.**

3 Granting Permission to IIS Metabase

To grant permission to IIS metabase:

1. Use the **Run as administrator** option to open and run Command Line.
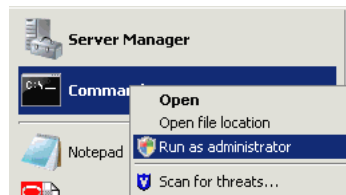
> **Note:** Make sure you run the following command as administrator.

2. Grant the *safety_user* permission to access IIS metabase:

   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis.exe -ga
   "safety_user"

4 Configuring Folder Access to the Web User Account

This section, which describes how to configure folder access to the web user account, includes the following topics:

The instructions in this section assume your installation has a domain server and all servers are configured in that domain.

4.1 Configuring Anonymous Access

On every web server, configure Anonymous access as follows:

1. Navigate to Internet Information Services (IIS) Manager.

2. Double-click **Authentication.**
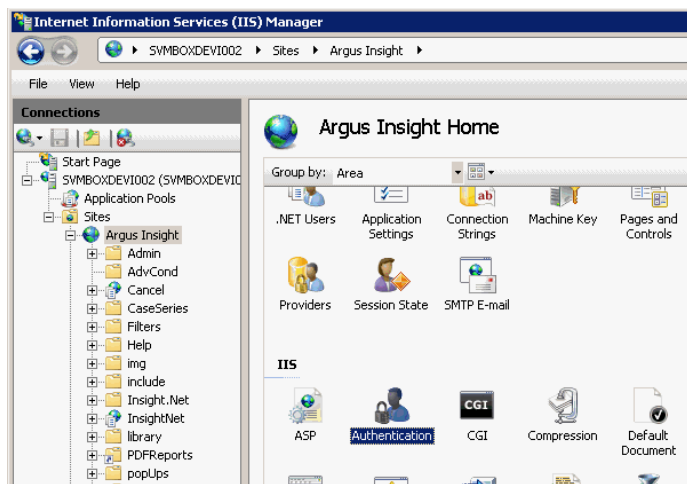
3. Select **Anonymous Authentication** and click **Edit.** The Edit Anonymous Authentication Credentials dialog box opens.
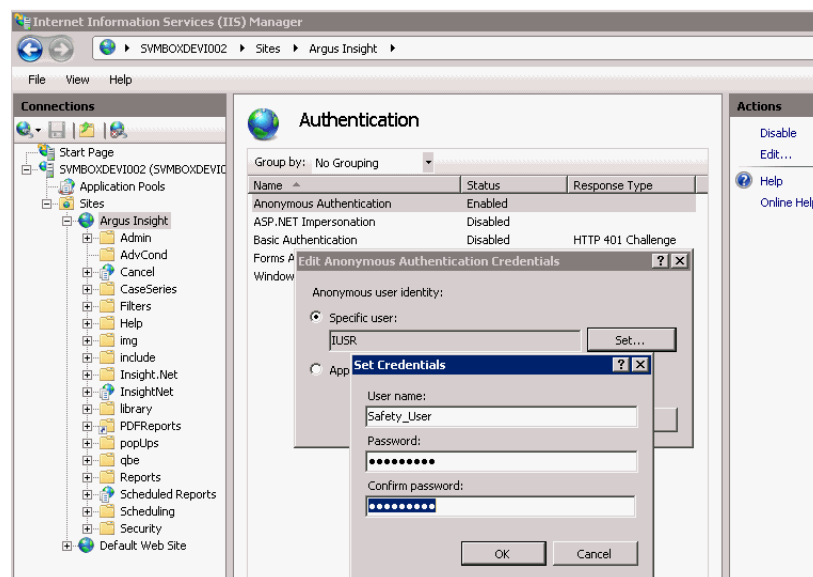
4. Click **Set** to define the user credentials for the Safety domain user (*safety_user*).

5. Click **OK** to save your changes.

4.2 Configuring Virtual Directories

On every web server, you must configure the following virtual directories to connect as the Safety domain user (*safety_user*):

- Cancel
- InsightNet
- PDFReports
- Scheduled Reports

To configure these virtual directories:

1. Select one of the virtual directories and click **Basic Settings.** The Edit Application dialog box opens.
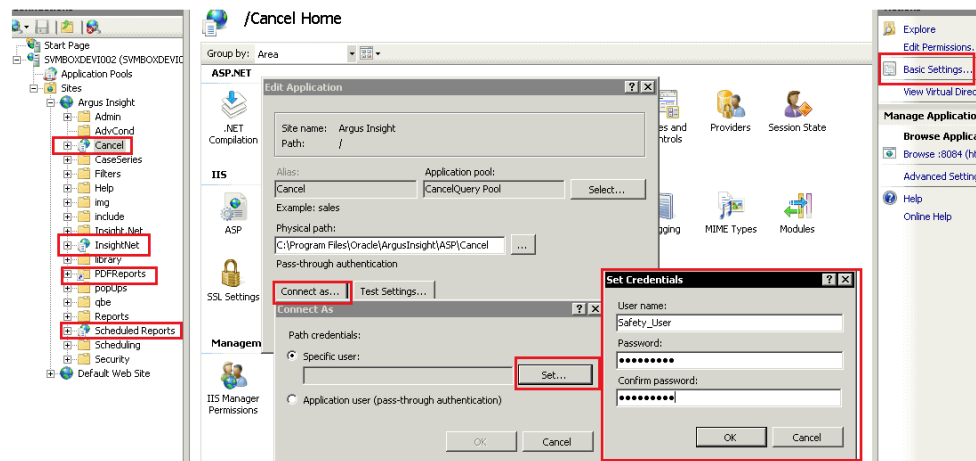
2. Click **Connect as.** The Connect As dialog box opens.

3. Select the **Specific user** option and click **Set.** The Set Credentials dialog box opens.

4. Enter the user name and password for the Safety domain user (*safety_user*).

5. Click **OK** until you close all the open dialog boxes.
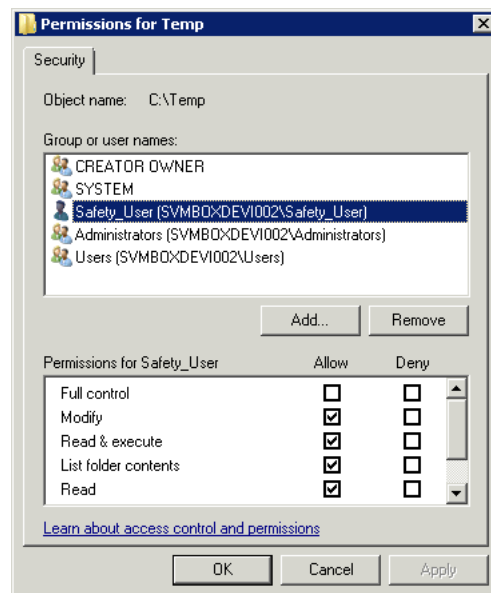
6. Repeat the process for the other virtual directories.

5 Configuring Application Pools

You must configure the following application pools to run under the *safety_user* identity:

- Argus Insight App Pool
- CancelQuery Pool
- InsightNet Pool

To configure these pools:

1. Select **Application Pools** to open the Application Pools page.
2. Select one of the application pools that you must configure.
3. Click **Advanced Settings.** The Advanced Settings dialog box opens.
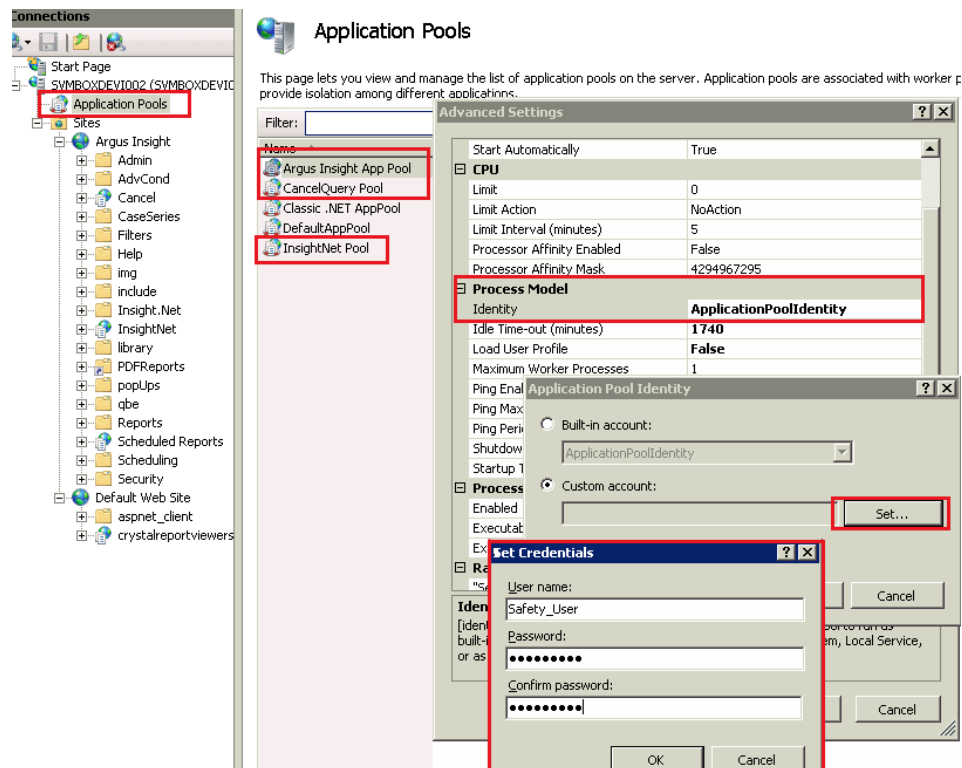
4. Expand **Process Model.**
5. Edit the **Identity.**
6. Select the **Custom account** option and click **Set.** The Set Credentials dialog box opens.
7. Enter the user name and password for the Safety domain user (*safety_user*).
8. Click **OK** until you close all the open dialog boxes.
9. Repeat the process for the other application pools.

6 Configuring Permissions for Log/Application Files and Folders

You must assign the Safety domain user (*safety_user*) the proper read, modify, and execute permissions for the following folders and files:

- C:Windows\AI.ini
- C:Windows\ArgusSecureKey.ini
- C:\Temp
- *Insight_Installation_Directory*\ArgusInsight\Bin\Log
- *Insight_Installation_Directory*\ArgusInsight\Bin\Logs
- *Insight_Installation_Directory*\ArgusInsight\CacheTemp
- *Insight_Installation_Directory*\ArgusInsight\PDFReports
- *Insight_Installation_Directory*\ArgusInsight\Scheduled Reports
- *Insight_Installation_Directory*\ArgusInsight\Upload

To configure the permissions:

1. Navigate to the appropriate file or folder.

2. Open the Permissions dialog box.

3. Select the **Allow** check box for the following permissions:

   - Modify
   - Read & execute
   - Read

   ***
   Note: Do not provide **Full control** for any of these folders or files.
   ***

4. Click **OK** to save your changes.

5. Repeat the process for the other files and folders.

7 Configuring HTTPS

To configure HTTPS:

1. Log in to the web server.

2. Start Internet Information Services (IIS) Manager.

3. Select the server node, select the **Server Certificates** icon in the IIS section, and click **Open Feature.**
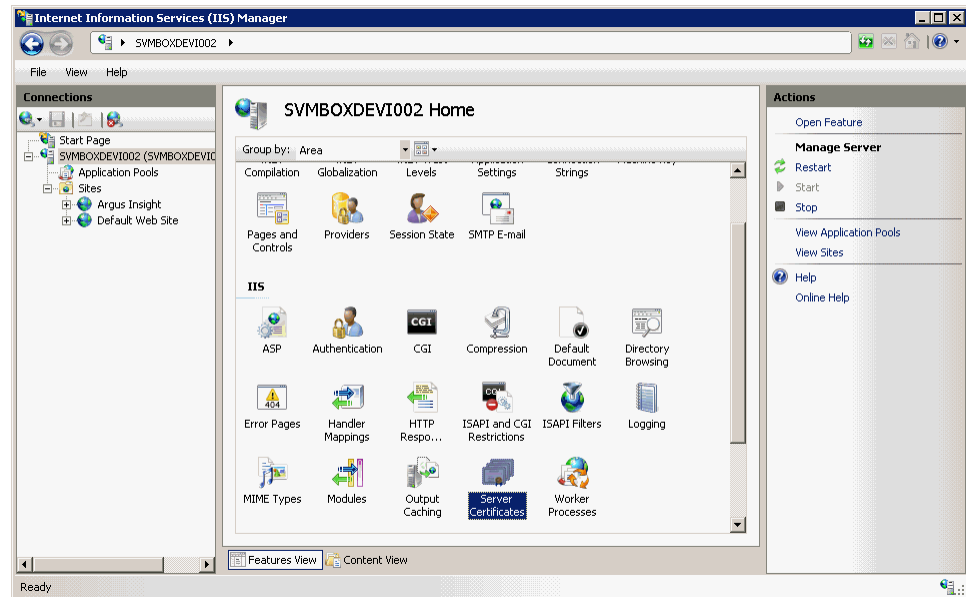
4. Create or import your SSL certificate.
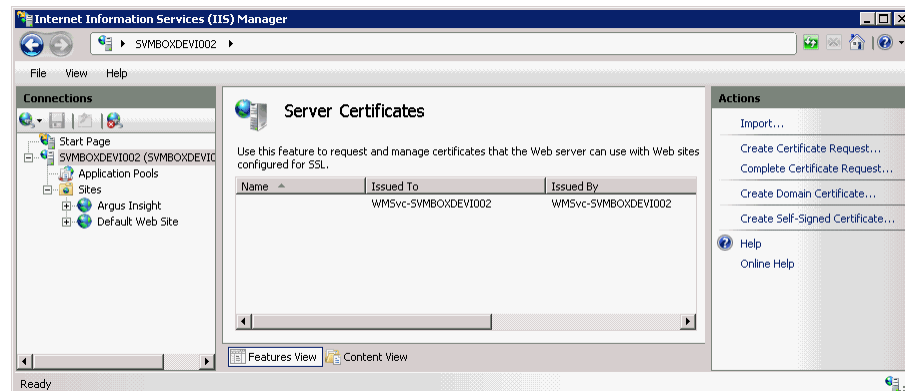
5. Wait until the certificate is created.

6. Navigate to **Sites,** select **Argus Insight,** and click **Bindings.**
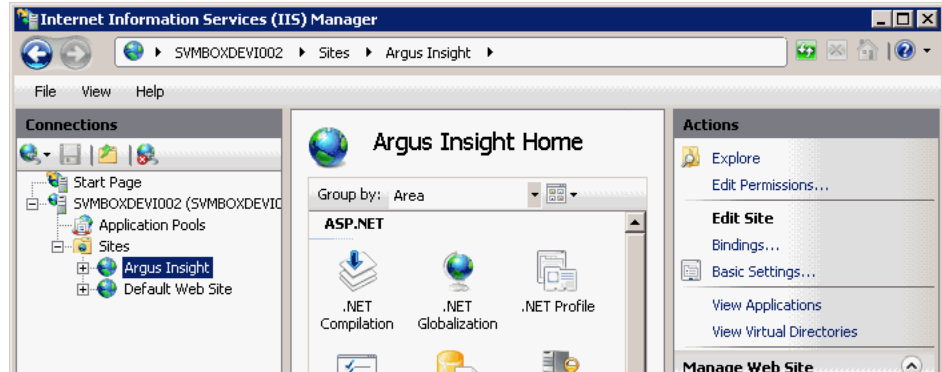
7. Click **Add.** The Add Site Binding dialog box opens.
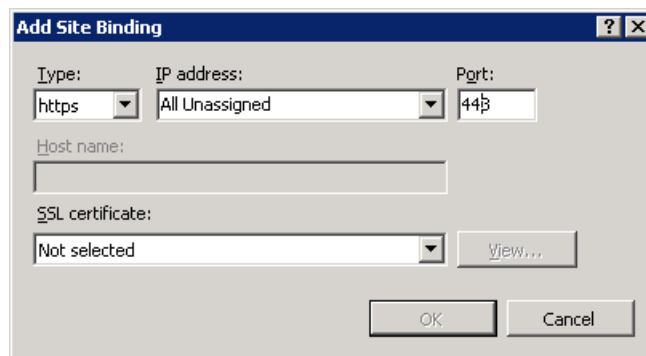
a. In the **Type** field, select **https** from the list.

b. In the **Port** field, enter the SSL port to bind.

c. In the **SSL certificate** field, select **Argus Insight** from the list.

d. Click **OK** to save your changes.

HTTPS is now enabled for Argus Insight.

To ensure the SSL connection is required:

1. Navigate to **Sites** and select **Argus Insight.**

2. Select the **SSL Settings** icon in the IIS section.
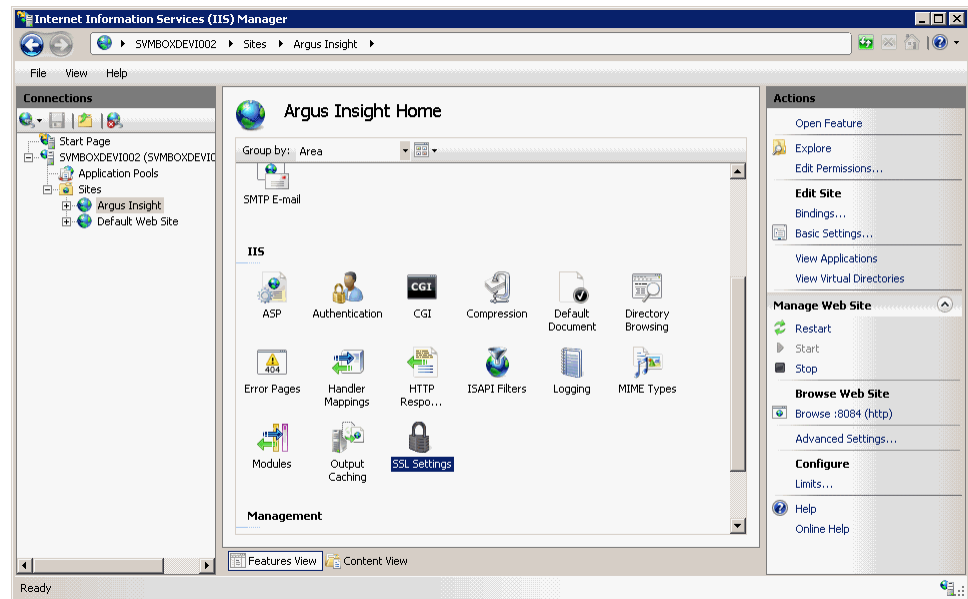
3. Click **Require SSL.**

4. Click **Apply.**

8 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.