Oracle® Argus Insight

Minimum Security Configuration Guide

Release 8.2

E96560-01

August 2018

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

1 Configure LDAP Authenticator Class.exe Permissions

You need to grant permissions to the LDAP Authenticator Class.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 in your installation.

To configure the permissions for the Argus Insight application:

1. Go to the web server.
2. Click **Start**, and select **Run.**

   The Run command dialog box appears.
3. In the **Open** field, enter **MMC comexp.msc /32**, and click **OK**.

The Component Services screen appears.

4. In the left pane, navigate to **Console Root > Component Services > Computers > My Computer** > **DCOM Config.**
5. In the right pane, right-click **LDAP Authenticator Class** (that is, Argus Insight application), and select **Properties** from the menu.
6. Click the **Security** tab.
7. Modify the **Launch and Activation Permissions** as follows:
   a. Select the **Customize** option.
   b. Click **Edit.**

      The Launch and Activation Permission dialog box appears.
   c. To add the domain user who will have launch and activation permissions, click **Add**.
   d. For the **Local Launch** option and the **Local Activation** option, select the **Allow** check box.
   e. For the **Remote Launch** option and the **Remote Activation** option, select the **Deny** check box.
   f. Click **OK.**
   g. Click **Yes** in response to the message about Deny permissions.
8. Modify the **Access Permissions** as follows:
   a. Select the **Customize** option.
   b. Click **Edit.**

      The Access Permission dialog box appears.
   c. To add the domain user who will have access permissions, click **Add**.
   d. For the **Local Access** option, select the **Allow** check box.
   e. For the **Remote Access** option, select the **Deny** check box.
   f. Click **OK.**
   g. Click **Yes** in response to the message about Deny permissions.
9. Modify the **Configuration Permissions** as follows:

   Note: If the Minimum Security user is the Service Accounts user, skip this step.

   a. Select the **Customize** option.
   b. Click **Edit.**

      The Change Configuration Permission dialog box appears.
   c. To add the domain user who will have configuration permissions, click **Add**.
   d. For the **Full Control** option and the **Read** option, select the **Allow** check box.
   e. Click **OK.**

10. Click **OK** to save the changes and close the LDAP Authenticator Class Properties dialog box.

2 Configure 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.**

      The Run command dialog box appears.

   b. In the **Open** field, 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 appears.
4. To add the domain user, click **Add**.
5. For the **Full Control** option, select the **Allow** check box.
6. Click **OK.**

3 Grant Permission to IIS Metabase

To grant permission to IIS metabase:

1. Use the **Run as administrator** option to open and run Command Prompt screen.

   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 Configure 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:

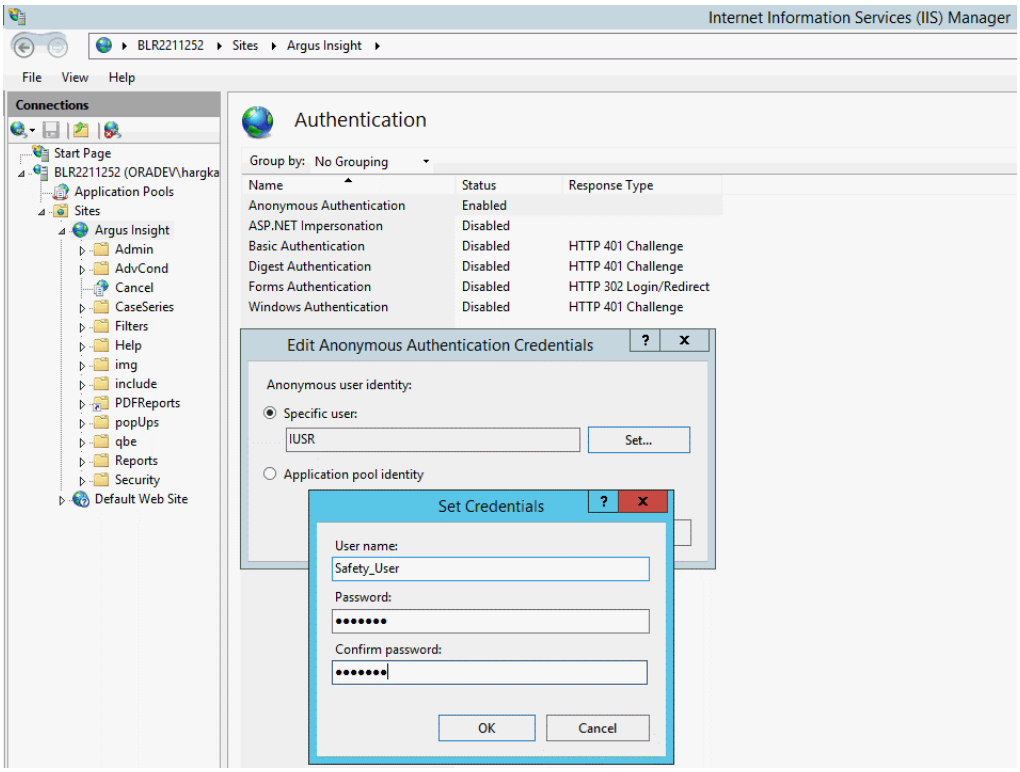
The instructions in this section assume your installation has a domain server and all servers are configured in that domain.

4.1 Configure Anonymous Access

On every web server, configure Anonymous access as follows:

1. Navigate to Internet Information Services (IIS) Manager.
2. In the left pane, select **Argus Insight**.
3. In the right pane, double-click **Authentication.**
4. Right-click **Anonymous Authentication**, and from the drop-down menu, click **Edit.**

   The Edit Anonymous Authentication Credentials dialog box appears.



5. To define the user credentials for the Safety domain user (*safety_user*), click **Set**.
6. Click **OK** to save the changes.

4.2 Configure Virtual Directories

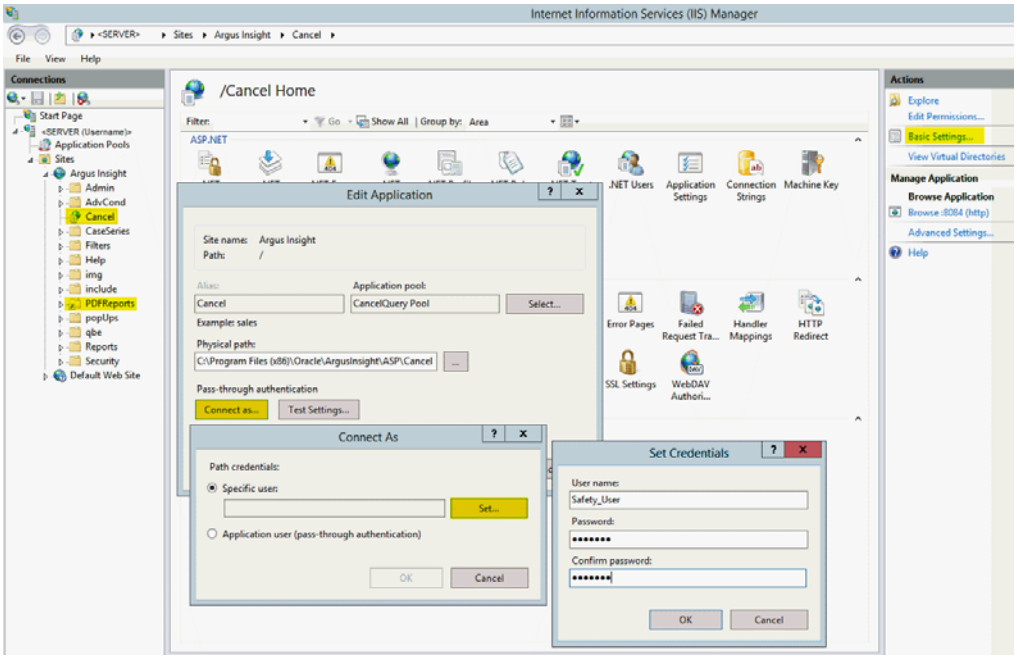
On every web server, you must configure the following virtual directories to connect as the Safety domain user (*safety_user*):

- Cancel
- PDFReports

To configure these virtual directories:

1. Select one of the virtual directories, and click **Basic Settings.**

   The Edit Application dialog box appears.



2. Click **Connect as.**

   The Connect As dialog box appears.

3. Select the **Specific user** option, and click **Set.**

   The Set Credentials dialog box appears.

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

5. Click **OK** until all the open dialog boxes are closed.

6. Repeat the process for the other virtual directories.

5 Configure Application Pools

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

- Argus Insight App Pool
- CancelQuery Pool

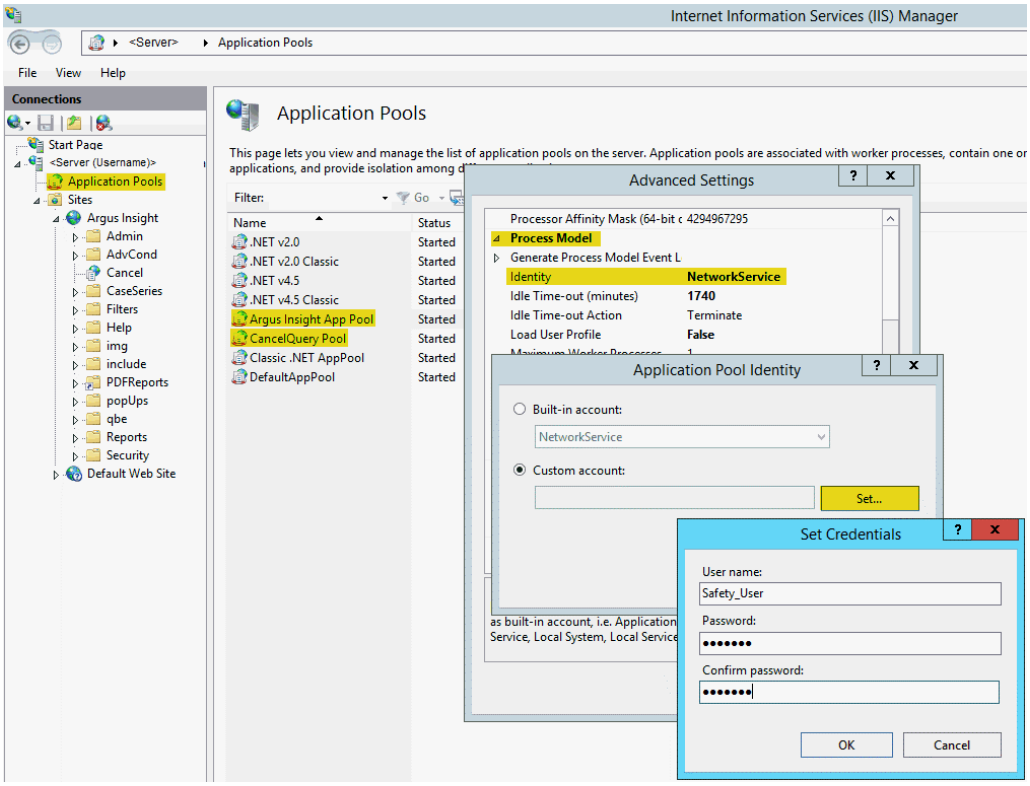
To configure these pools:

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 appears.



4. Expand **Process Model.**
5. Edit the **Identity.**
6. Select the **Custom account** option, and click **Set.**

   The Set Credentials dialog box appears.
7. Enter the user name and password for the Safety domain user (*safety_user*).
8. Click **OK** until all the open dialog boxes are closed.
9. Repeat the process for the other application pools.

6 Configure 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\CacheTemp
- *Insight_Installation_Directory*\ArgusInsight\PDFReports
- *Insight_Installation_Directory*\ArgusInsight\Upload

To configure the permissions:

1. Navigate to the appropriate file or folder, and right-click.

2. In the Permissions dialog box, select a group or user name.
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 the changes.
5. Repeat the process for the other files and folders.

7 Configure HTTPS

1. Log in to the web server.
2. Start Internet Information Services (IIS) Manager.
3. In the left pane, select the server node.
4. In the right pane, select the **Server Certificates** icon in the IIS section, and click **Open Feature.**
5. Create or import your SSL certificate.
6. Wait until the certificate is created.
7. In the left pane, navigate to **Sites,** select **Argus Insight,** and click **Bindings.**
8. Click **Add.**

   The Add Site Binding dialog box appears.
   a. In the **Type** drop-down list, select **https**.
   b. In the **Port** field, enter the SSL port to bind.
   c. In the **SSL certificate** drop-down list, select **Argus Insight**.
   d. Click **OK** to save the changes.

   HTTPS is now enabled for Argus Insight.

To ensure the SSL connection is required:

1. In the left pane, navigate to **Sites**, and select **Argus Insight.**
2. In the right pane, select the **SSL Settings** icon in the IIS section.
3. Click **Require SSL.**
4. Click **Apply.**

8 Configure X-Content-Type-Options in IIS

1. Open Internet Information Services (IIS) Manager.
2. In the **Connections** pane, go to the site, application, or directory for which you want to set a custom HTTP header.

3. In the Home pane, double-click **HTTP Response Headers**.
4. In the HTTP Response Headers pane, in the **Actions** pane, click **Add...**
5. In the **Add Custom HTTP Response Header** dialog box, enter the followig parameters and click **OK**.
   a. Name—**X-Content-Type-Options**
   b. Value—**nosniff**

9 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 that have purchased support 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.

Minimum Security Configuration Guide, Release 8.2
E96560-01