Oracle Argus Insight

Minimum Security Configuration Guide

Release 8.4
F51796-01
September 2022

Oracle Argus Insight Minimum Security Configuration Guide, Release 8.4

F51796-01

Contents

Preface

This preface contains the following sections:

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related resources

For information about Oracle Argus patches, see My Oracle Support.

All documentation and other supporting materials are available on the Oracle Help Center.

Access to Oracle Support

To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

Cloud customers receive support assistance through Support Cloud

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (https://hsgbu.custhelp.com/)
- Japanese interface of Oracle Health Sciences Customer Support Portal (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

On-premises customers receive support assistance through My 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.

1

Minimum Security Configuration Guide

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

Keep up to date on software and latest Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts.

Oracle highly recommends that customers:

- Keep all software versions and patches up to date.
- Apply Critical Patch Updates as soon as they are released.

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.**

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\v4.0.30319\aspnet_regiis.exe -ga "safety_user"`, where `safety_user` is an example user that represents the name of the domain user. A domain user has access to the web servers and all network services that will be configured in Argus Insight.

> **Note:**
>
> Make sure you include the domain name when running the command. For example: `C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -ga asd\svcargus`, where
>
> - `asd` is the domain name.
> - `svcargus` is the domain user.

Configure Folder Access to the Web User Account

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

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

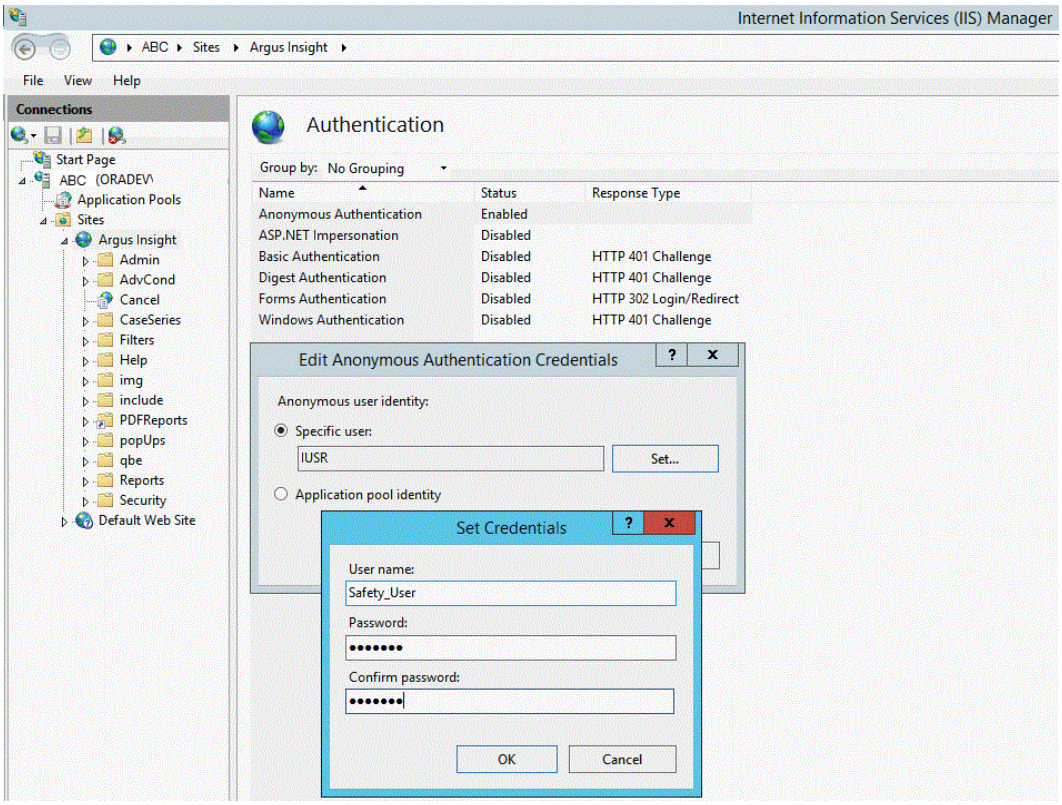
- Configure Anonymous Access
- Configure Virtual Directories

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 Oracle Argus Safety domain user (*safety_user*), click **Set**.
6. Click **OK** to save the changes.

Configure Virtual Directories

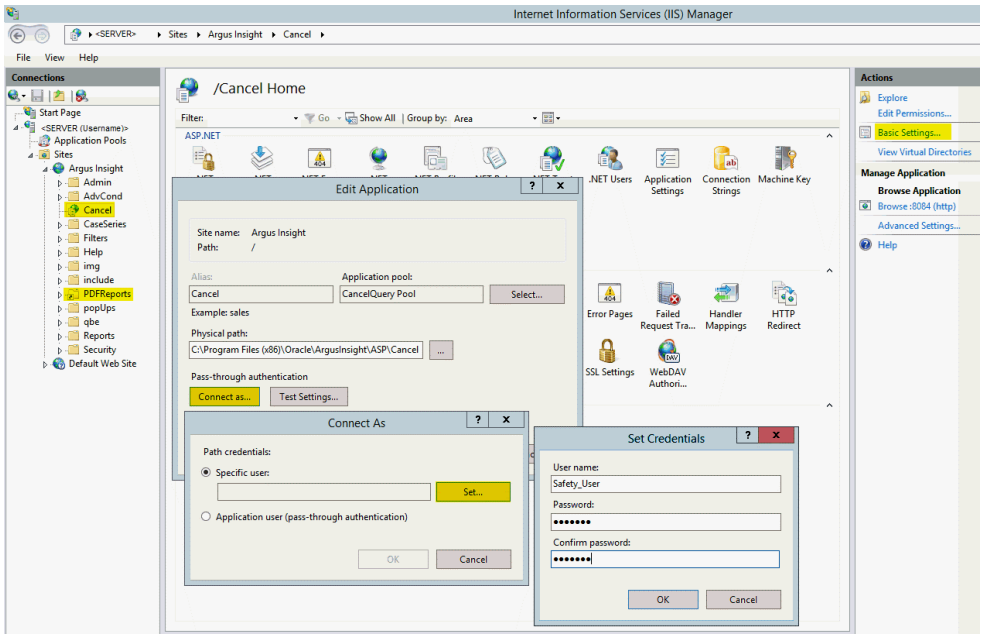
On every web server, you must configure the following virtual directories to connect as the Oracle Argus Safety domain user (*safety_user*):

- 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 Oracle Argus 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.

Configure Application Pools

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

- Argus Insight App Pool
- CancelQuery Pool

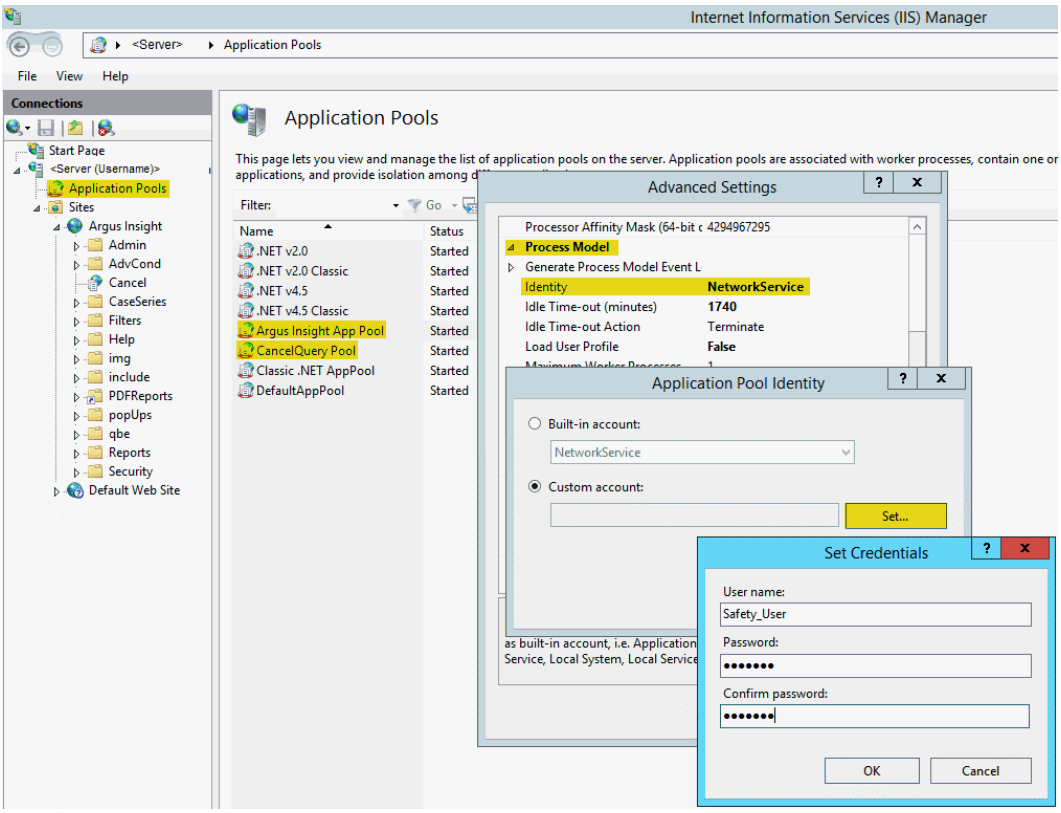
To configure these pools:

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 Oracle Argus 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.

Configure Permissions for Log or Application Files and Folders

You must assign the Oracle Argus 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.

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 Oracle 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**.

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 following parameters and click **OK**.
    a. Name — **X-Content-Type-Options**
    b. Value — **nosniff**

(Optional) Configure Content Security Policy

Oracle Argus Insight supports the use of modern browser as their user interface. Modern browsers have defense-in-depth controls to mitigate cross-site scripting (XSS), click jacking, and cross-site leak vulnerabilities by leveraging the Content Security Policy standards. These controls add a secondary level of protection, in addition, to the usual Oracle Argus Insight security application controls. Though these securities are optional as per the Customer Security Policy, you may apply the following, in case, you want the Content Security Policy.

Implement the following Content Security Policy configurations in IIS:

```
frame-ancestors 'self' *.”ArgusSafetyDomain”:* *.”ArgusInsightDomain”:*;
default-src *.”ArgusSaftyDomain”:* *.”ArgusInsightDomain”:* 'self'; 'unsafe-
inline' 'unsafe-eval'
```

Here, the domains *ArgusSafetyDomain* and *ArgusInsightDomain*, are sample domains, and must be changed to your organizational domains.

For more information, go to My Oracle Support, and search for the *Content Security Policy for Argus Safety and Argus Insight (Doc ID 2891772.1)*.