Oracle® Argus Safety

Minimum Security Configuration Guide

Release 8.2.1
F28454-02
June 2020

Oracle Argus Safety Minimum Security Configuration Guide, Release 8.2.1

F28454-02

Contents

Preface

This preface contains the following sections:

Audience

This guide describes essential security management options.

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.

Related resources

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 guide describes essential security management options for Oracle Argus Safety 8.2.1 and outlines the steps that help strengthen application security.

> **Note:**
>
> This document is not a replacement of the *Oracle Argus Safety Installation Guide*. The Installation Guide should be referred for Oracle Argus Safety installation instructions.

Use this guide to configure the following security guidelines and recommendations on the Oracle Argus Safety Web and Report Servers:

- Post Installation Security Configurations
- Configuring Log Folders, SQLTimes Path, and Access Permissions
- Configuring HTTPS
- Configuring Password Complexity
- Configuring Case Intake Folders and Security
- Configuring Security for Interface Web Service
- Configuring Security for ESM
- Configuring Security for AG Service
- Configuring X-Content-Type-Options in IIS
- Configuring Oracle Argus Safety with Minimum Security

Post Installation Security Configurations

This document lists the various security configurations required after installing Oracle Argus Safety:

- Configuring Argusvr2/Argusvr2a Permissions
- Configuring Folder Access to Web User Account

Configuring Argusvr2/Argusvr2a Permissions

> **Note:**
>
> This section needs to be applied to each Web and Report Server.

Execute the following steps to configure Argusvr2/Argusvr2a permissions:

1. Create a domain user which has access to web-servers and all network services that will be configured in Oracle Argus Safety such as shared network paths for Oracle Argus Safety Intake.

   In the steps mentioned below, we have used a sample user called 'Safety_User', throughout this section of the Guide.

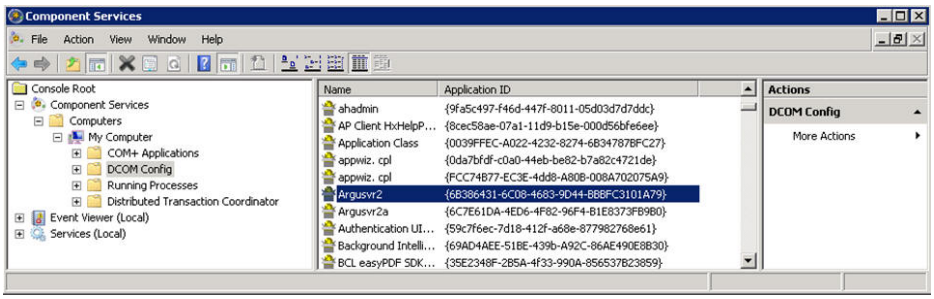
2. Go to every web server and configure the following:

   a. Go to **Control Panel > Administrative Tools**.

   b. Open **Component Services**.

   c. Go to **Console Root > Component Services > Computers > My Computer**.

   d. Select **DCOM Config**:

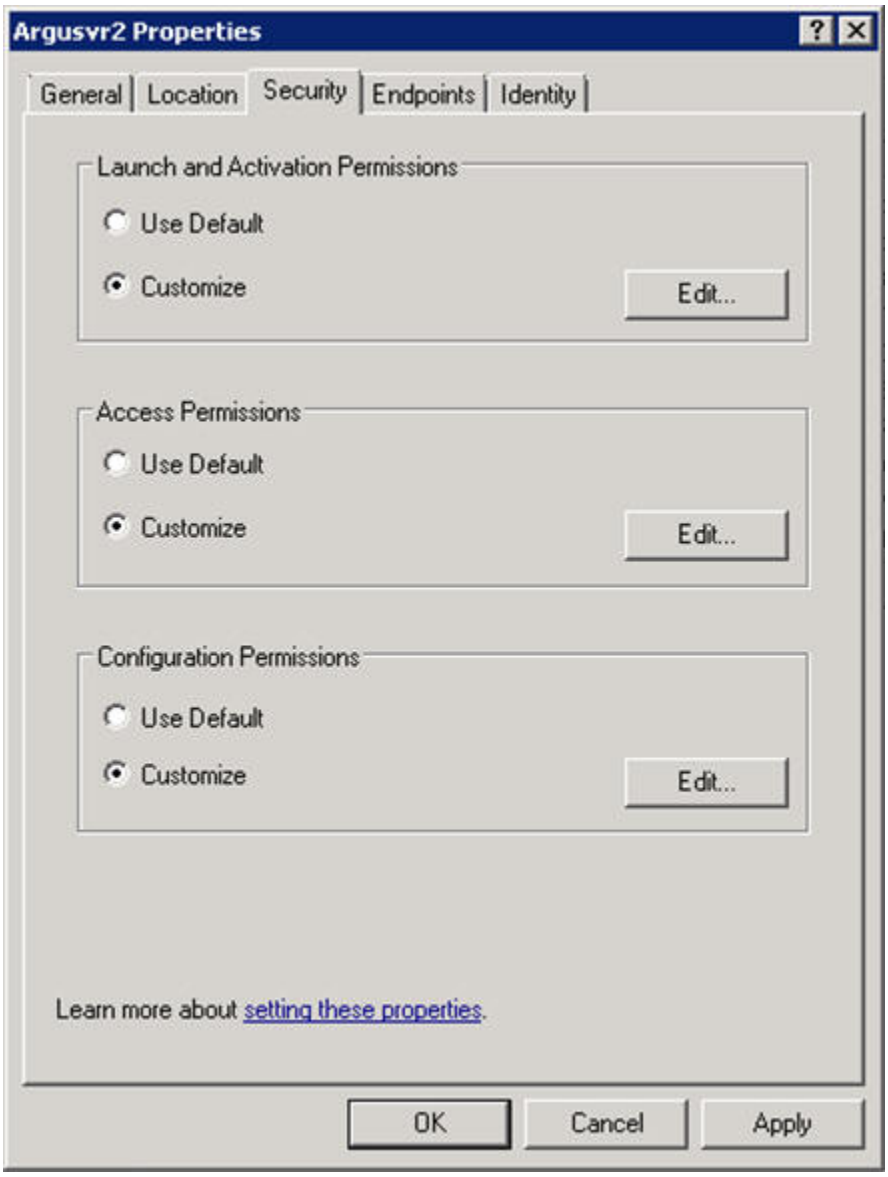


   e. Change Permissions for Argusvr2 by doing the following:

      i. Right-click on Argusvr2 and select **Properties**.

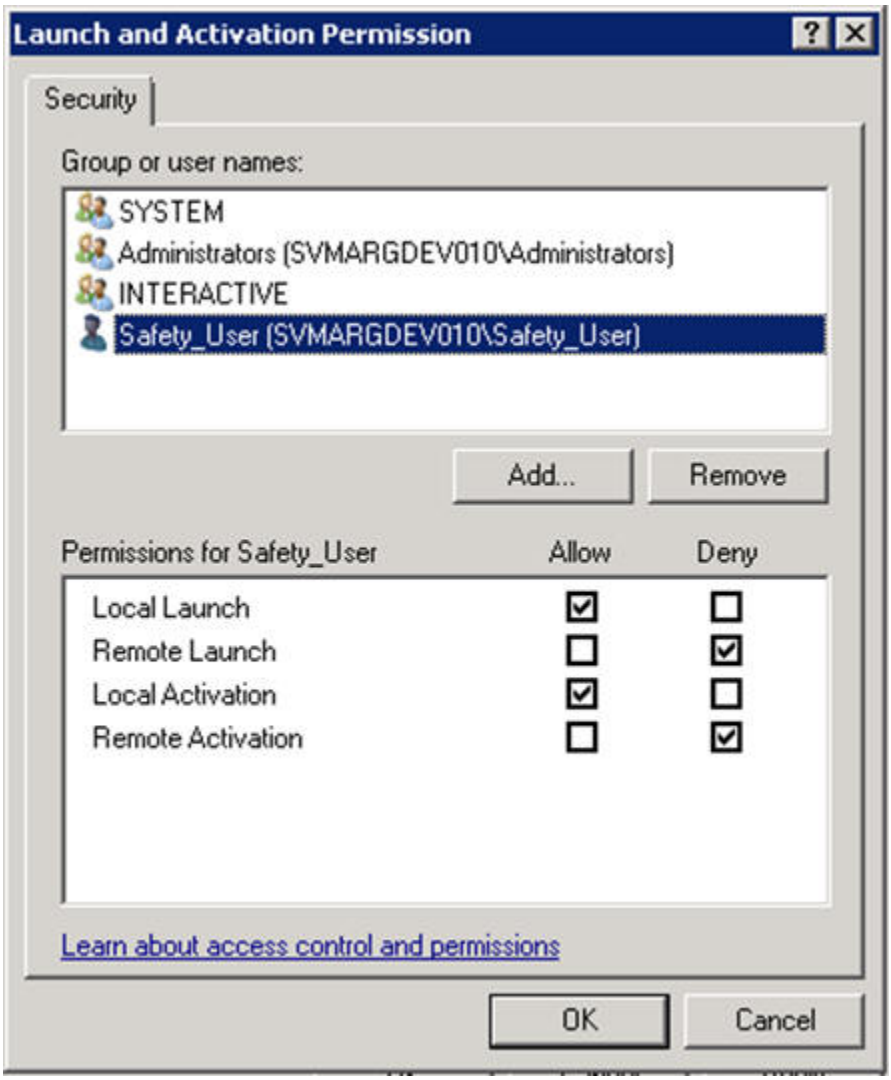
      ii. Select the **Security** tab.

      iii. Select **Customize** for these options: **Launch and Active Permissions**, and **Access Permissions**.



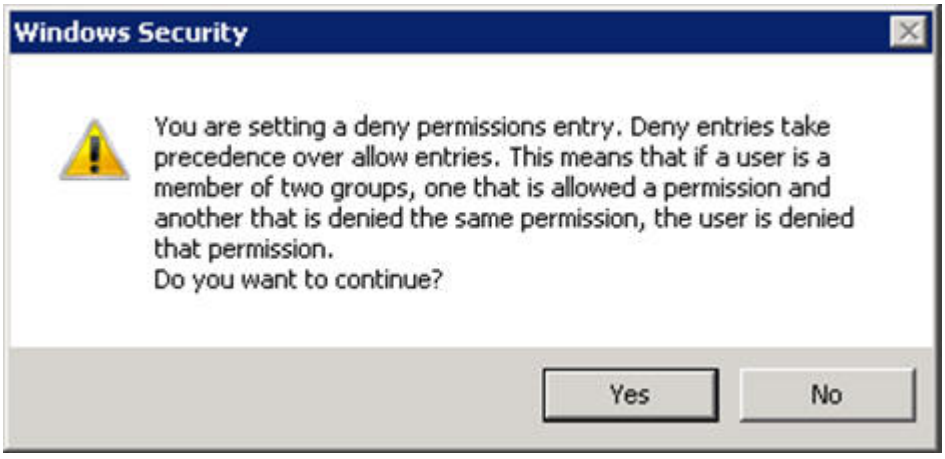
iv. Click **Edit** under **Launch and Activation Permissions**.

v. Add **Domain User** for **Launch and Activation Permissions** with **Local Launch** and **Local Activation** permission selected. Select **Deny** for **Remote Launch** and **Remote Activation**.



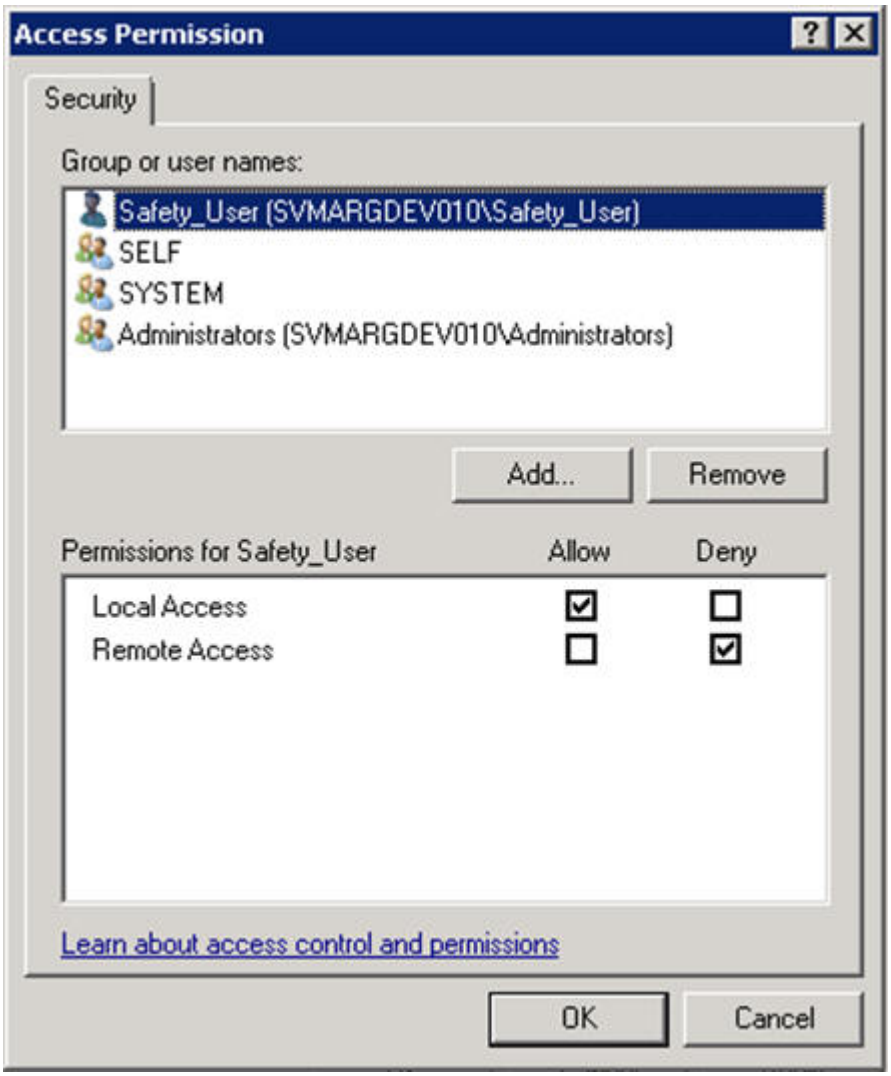
vi. Click **OK**.

vii. Click **Yes** when you receive the following **Windows Security** message, regarding Deny permissions:



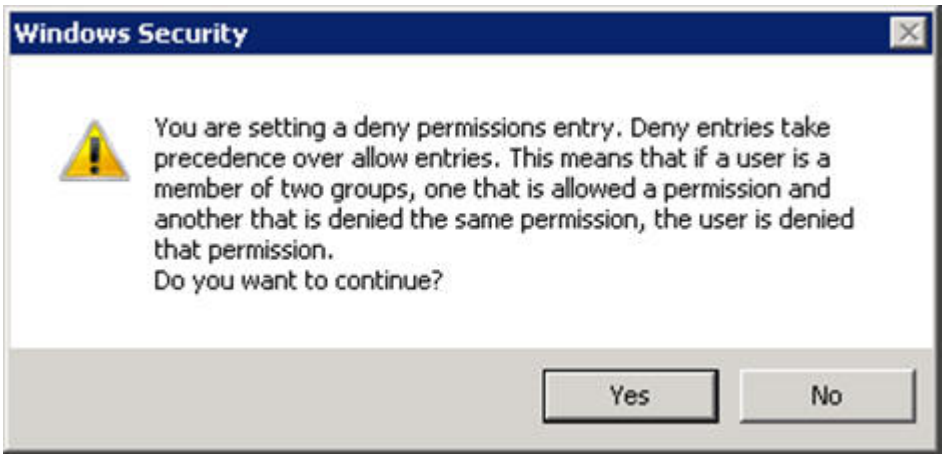
viii. Click **Edit** for **Access Permissions**.

ix. Add **Domain User** for **Access Permissions** with **Local Access** permission selected. Select **Deny** for **Remote Access**.



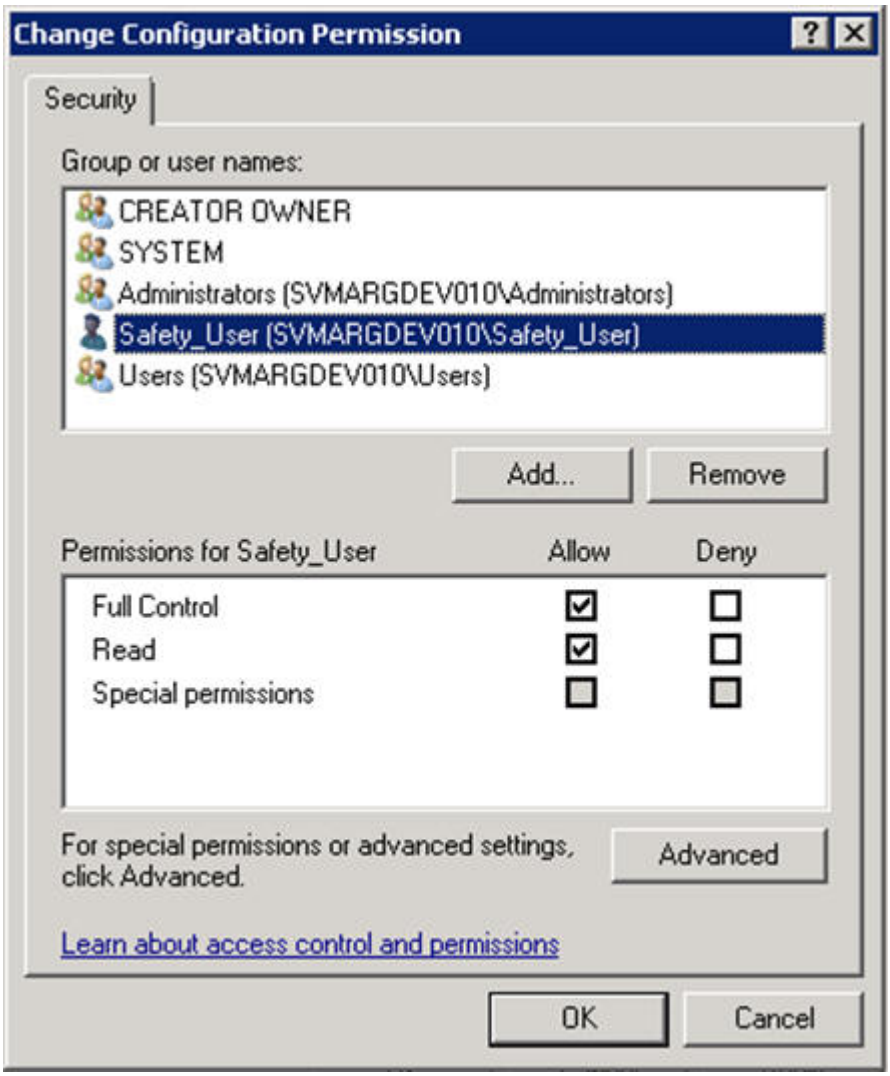
x. Click **OK**.

xi. Click **Yes** when you receive the following **Windows Security** message, regarding Deny permissions:



xii. Click **Edit** for Configuration Permissions.

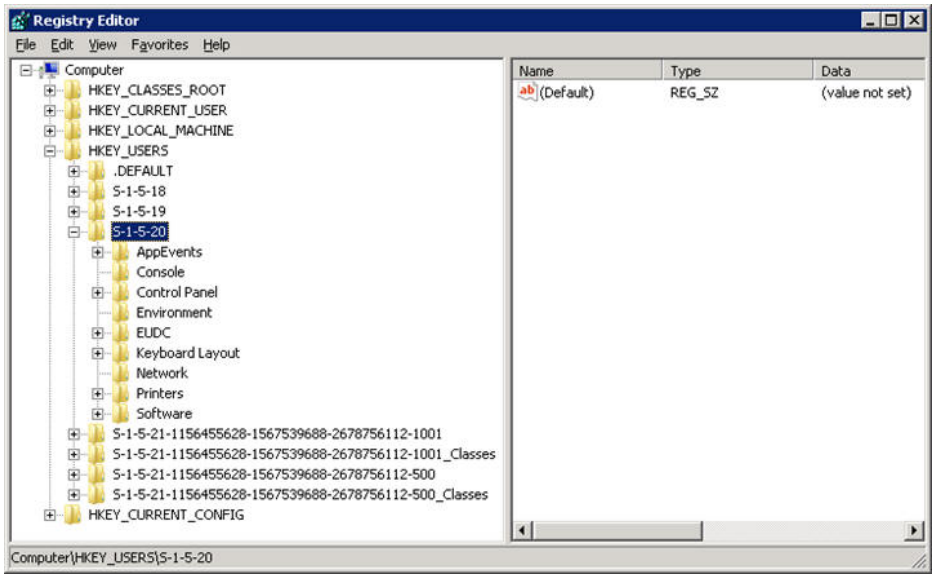
xiii. Add a domain user for **Change Configuration Permission**, with **Full Control** and **Read** permissions selected.



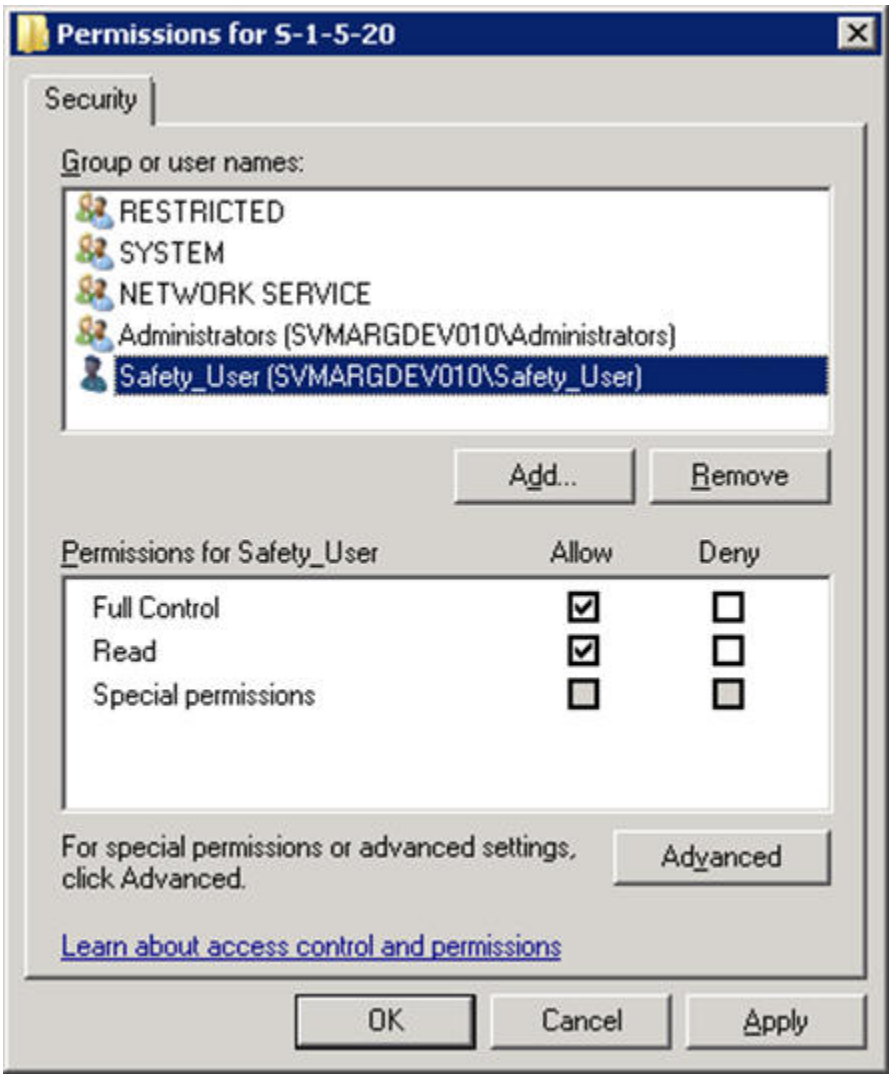
xiv. Click **OK**.

xv. Click **OK** on the **Argusvr2 Properties** dialog to save the changes.

3. Repeat step 2 for Argusvr2a.
4. Run the Registry tool in Windows, as shown below:
   a. Browse to the `HKEY_USERS\S-1-5-20` folder:



   b. Right-click the folder and select **Permissions**.
   c. Add a Safety Domain User with **Full Control** permission.



5. Give permission to Access IIS Metabase to **Safety_User** by running following command from the command prompt as administrator:

```
C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis
.exe -ga "Safety_User"
```

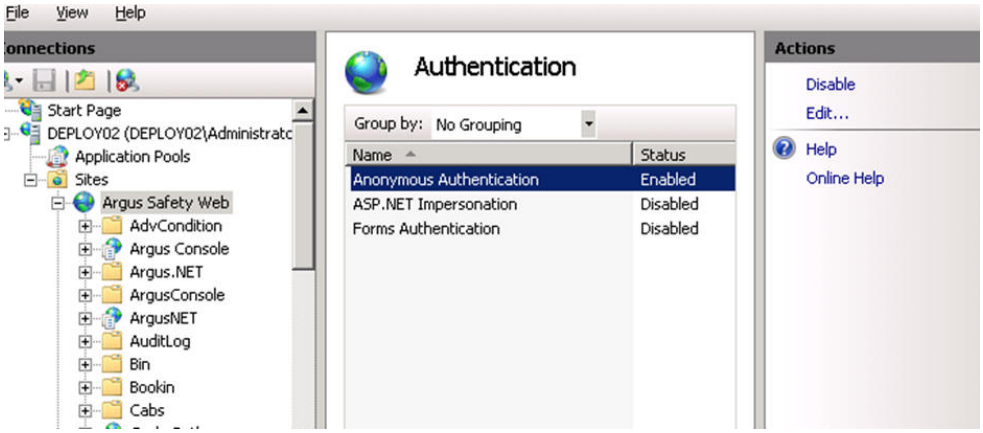
Configuring Folder Access to Web User Account

We should have a Domain server and all the servers should be configured in that domain.

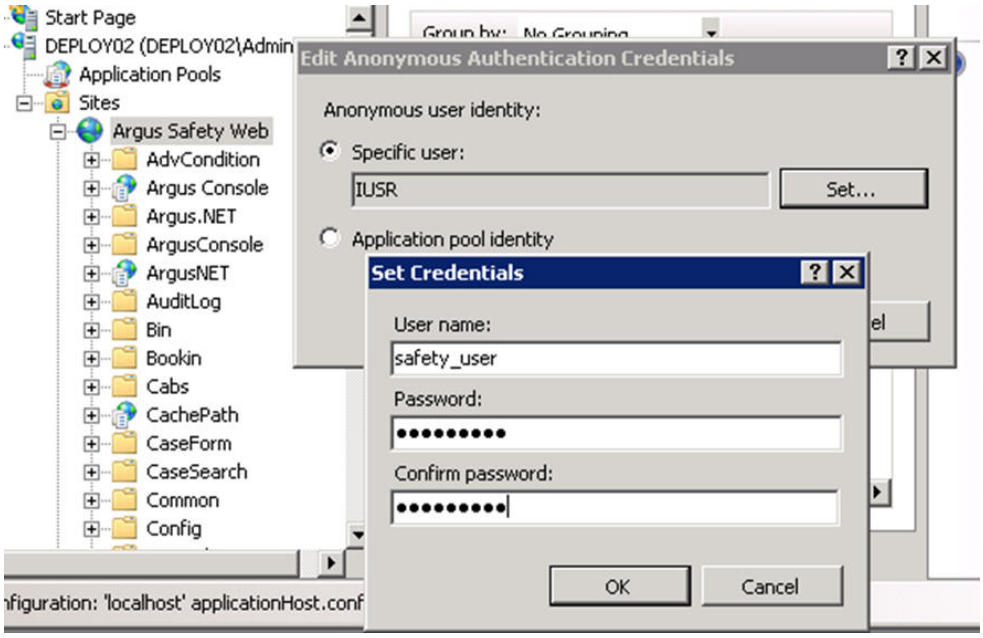
On every Web Server/Report Server, Anonymous access should be configured as follows:

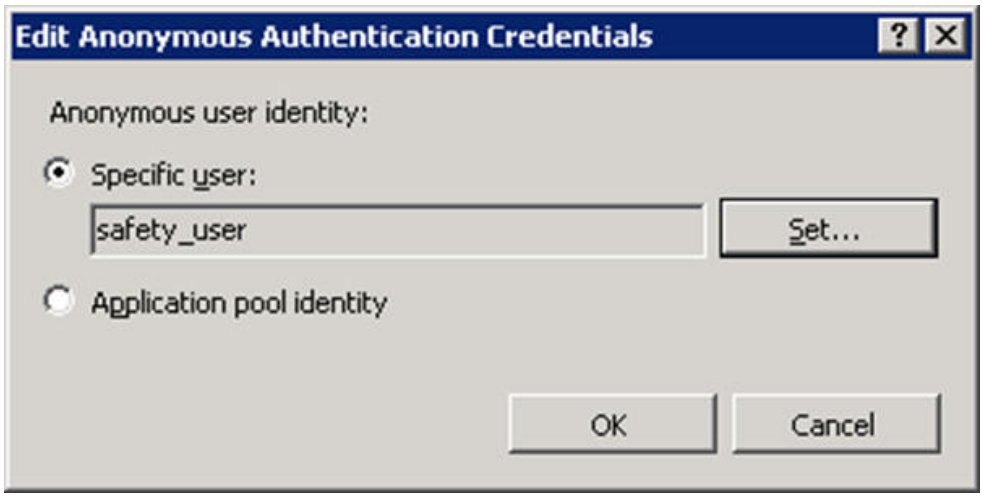
1. Go to **IIS Configuration Manager > Authentication**:

2. Edit **Anonymous Authentication**:



3. Set user credentials to the Safety domain user (Safety_User):





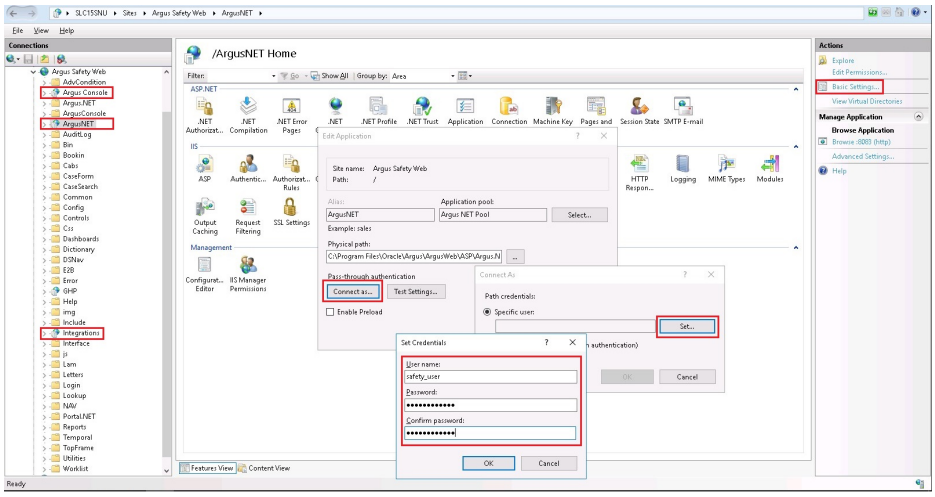
4. On every Web Server:

   `Integrations`, `GHP`, `ArgusNet`, and `Argus Console` virtual directories should be configured to connect as Safety Domain User [Safety_User] as follows:

> **Note:**
>
> If `Webgate` is configured, then the `webgate`, `oamsso`, and `oamsso-bin` virtual directories require the same configuration.

   a. Select virtual directory and click on **Basic Settings**.

   b. Select **Connect as > Set Path Credentials > Enter Safety Domain User [Safety_User] and Password**.



c. Give full access on the following folders or files to Safety_User:

   `C:\Temp\` or Configured Root Folder for temp files

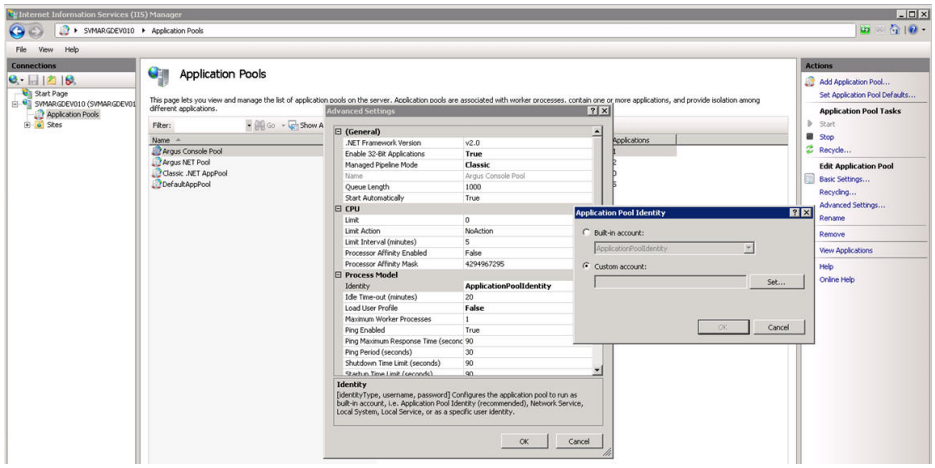
   <ArgusInstallPath>

   <Documentum Installation Path> and

   `C:\Documentum`

   `<Windows>\AGService.ini`

d. Configure `Application Pools`.



Configure `Argus.net` and `Argus Web` pool to run under the Safety_User identity.

> **Note:**
>
> If Oracle Access Manager is installed, give full control permission to everyone on `Webgate` folder.
>
> `Argus Web` Pool has the same settings as defined for `Argus Console` Pool and `Argus NET` Pool.

e. Restart the Web Server.

Configuring Log Folders, SQLTimes Path, and Access Permissions

In this chapter:

Configuring Log Folders

The various modules of Oracle Argus SafetyWeb log information to Log files in the configured folders. The configuration for logging can be found in the `<logConfig>` section in the following files:

`<ArgusInstallPath>\ArgusConsole\logger.config`

`<ArgusInstallPath>\Argus.Net\logger.config`

`<ArgusInstallPath>\Argus.Net\Bin\RelsysWindowsService.exe.config`

`<ArgusInstallPath>\web.config`

`<ArgusInstallPath>\..\Bin\Argusvr2.config`

`<ArgusInstallPath>\..\Bin\Argusvr2a.configx`

`Argus Safety\Agproc.config` (on the AG Service Box)

By default, the log level is set as 'Error':

```
<add userid="--All--" Enterprise="--All--" logLevel="Error" />
```

This means that the application logs only errors encountered by it on the web server. The log level can be configured to any of the following values:

Off

Error

Warning

Information

Verbose

If a higher level log needs to be configured for a specific user or a specific Enterprise, an additional line can be added in the `<LoggerConfigs>` section as shown below:

```
<add userid="thomas" Enterprise="ESN1" logLevel="Verbose" />
```

The above example enables verbose logging for the user "thomas" who belongs to the Enterprise with the EnterpriseShortName "ESN1".

The folder where the log files are generated can be found in the following configuration in the same .config file:

```
<appender name="RollingLogFileAppender"
type="log4net.Appender.RollingFileAppender"> <param name="File"
value="C:\Temp\ArgusLogs\ArgusNet\RelsysWindowsService.log" />
```

Different modules of the application should have different log file names (or paths). By default, the logs are configured to be generated under `C:\Temp\ArgusLogs` or a subfolder under it.

This folder needs to have Read/Write/Modify permissions to the Domain user with which the Oracle Argus Safety Website has been configured to run as.

Configuring SQLTimes Path

The folder where SQLTimes logs are generated is configurable. The configuration needs to be made in `argus.ini` (present in the Windows folder).

The following example illustrates this configuration:

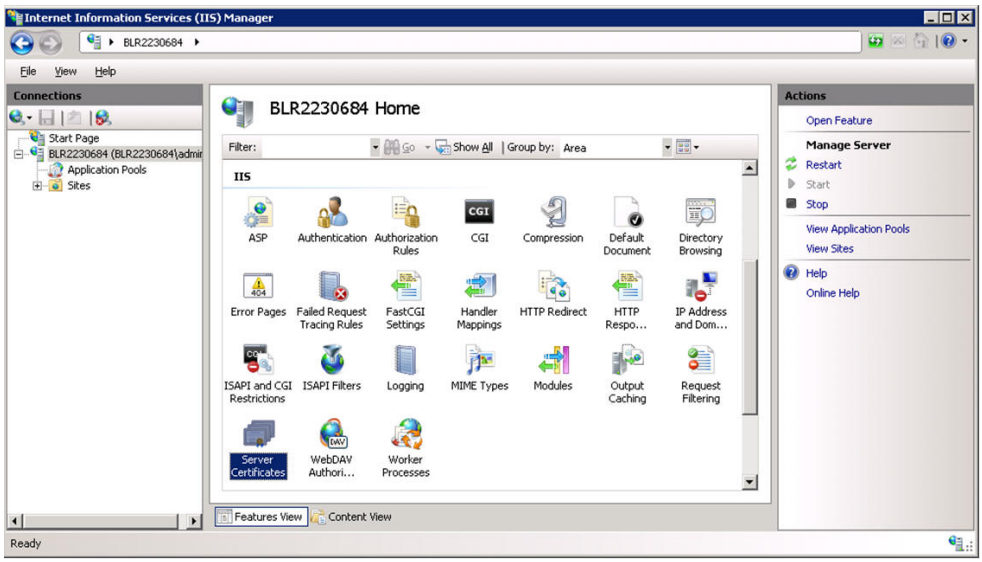
```
[Workstation]SqlTimesPath=C:\Temp\ArgusLogs\SqlTimes
```

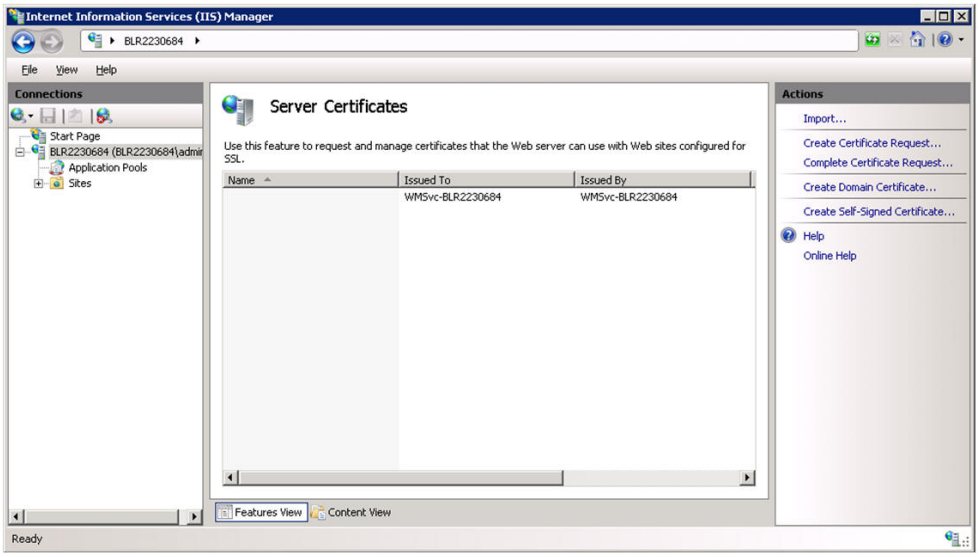
This folder needs to have Read/Write/Modify permissions to the Domain user with which the Oracle Argus Safety Website has been configured to run.

Configuring HTTPS

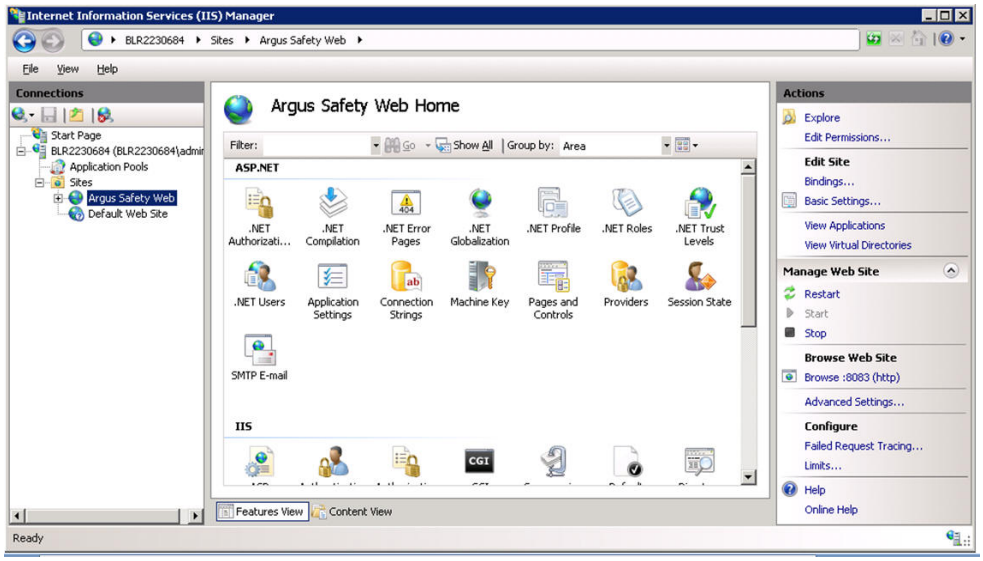
Execute the following steps to configure HTTPS:

1. Login to each Web Server and Report Server and perform the following steps to configure HTTPS.
2. Launch the **Internet Information Services (IIS) Manager**.
3. Select the server node as shown in the diagram below and then open the **Server Certificates** under the **IIS** section.

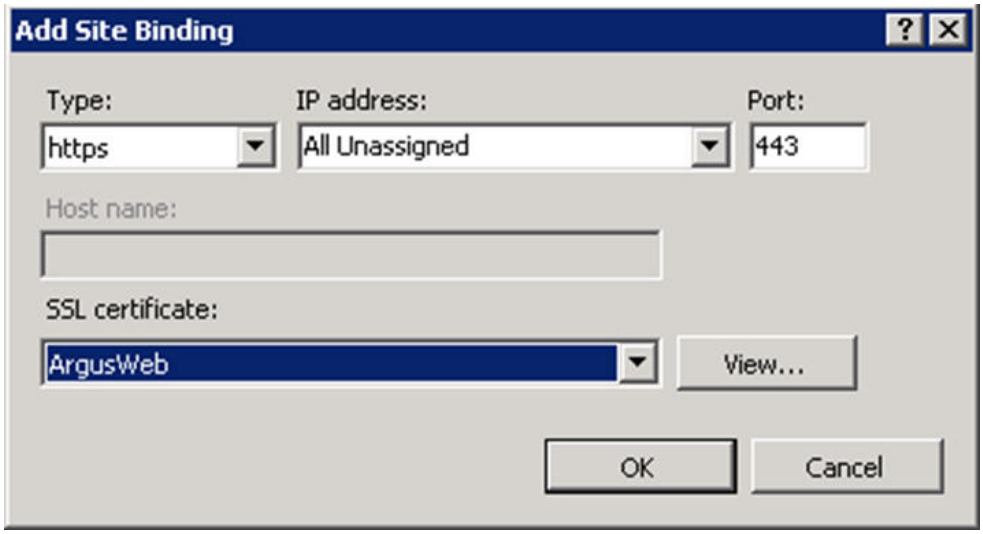




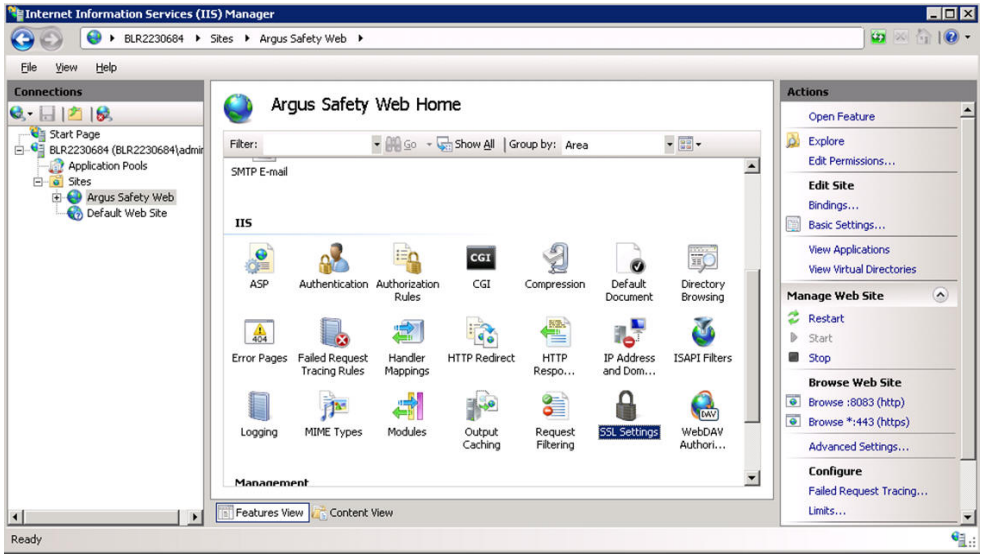
4. Create/import your SSL certificate.
5. After the certificate is created, select **Argus Safety Web** under the **Sites** option and go to **Actions > Bindings**.



6. Add a new **Binding** for the SSL Port. Select **https** as the port to bind and the SSL certificate in the **SSL Certificate** drop-down list that was created previously.



7. Click **OK**.
8. HTTPS is now enabled for Oracle Argus Safety. To ensure that the SSL connection is required, select **SSL Settings** under the **Argus Safety Web** node.



9. Select **Require SSL** and click **Apply**.

   To disable insecure SSL protocols, follow the steps to disable:

   - SSL 1.0
   - SSL 2.0
   - SSL 3.0
   - TLS 1.0
   - TLS 1.1

   as per following article: https://support.microsoft.com/en-us/kb/245030.

Configuring Password Complexity

Execute the following steps to configure password complexity:

1. Log in to Oracle Argus Safety with access to Argus Console.
2. Open Argus Console.
3. Go to **System Configuration > System Management**.
4. Select **Security** from the left-hand pane.
5. Configure the following options to control password complexity:
   - Number of non-alpha characters in password: The number entered here will ensure that the users enter that many non alpha characters during password updates. Setting this value to a 0 will not require a non-alpha character.
   - Minimum number of characters in the password: This defines the minimum length of a password.
   - Number of previous passwords that cannot be repeated: This will prevent users from using the same password again after the number entered in this field.

Configuring Case Intake Folders and Security

The Oracle Argus Safety Intake service should be configured to run under a Domain user, who has read-write access onto the IN and OUT folder paths. There are no other security guidelines for Oracle Argus Safety Intake.

Configuring Security for Interface Web Service

The PSL Web Service has been built on top of Microsoft Windows Communication Foundation. The following gives a very detailed understanding of the concepts of WCF Security and the various configurations that are possible to configure security on the WCF Web Service.

Execute the following steps to configure the PSL Web Service to use Transport and Message Security:

1. Locate the `<system.serviceModel>` section in the `<ArgusInstallPath>\Integrations\web.config` file.

   By default, the bindingConfiguration used by the Service Endpoint is *wsHttpUnsecure*.

2. Security can be configured in the same binding Configuration or a new configuration can be created. The steps mentioned in this section uses a new binding configuration called wsHttpSecure.

   To achieve this, modify the endpoint configuration to use the new bindingConfiguration:

```
<services>
     <service
behaviorConfiguration="Relsys.InterfaceLibrary.RelsysServiceBehavior
" name="Relsys.InterfaceLibrary.RelsysService">
     <endpoint address="" binding="wsHttpBinding"
contract="Relsys.InterfaceComponents.IRelsysService"
bindingConfiguration="wsHttpSecure"/>
     </service>
</services>
```

3. Create a new binding configuration under the hierarchy `<bindings><wsHttpBinding>`, as shown below:

```
<bindings>
     <wsHttpBinding>
       <binding name="wsHttpSecure">
         <security mode="TransportWithMessageCredential">
           <transport clientCredentialType="Certificate"/>
           <message clientCredentialType="Certificate" />
         </security>
       </binding>
     </wsHttpBinding>
   </bindings>
```

The different values available for the clientCredentialType for transport and message elements can be found in the WCF documentation mentioned at the beginning of this section.

4. Modify the Service Behavior configuration as follows:

```
<behaviors>
     <serviceBehaviors>
       <behavior
name="Relsys.InterfaceLibrary.RelsysServiceBehavior">
         <serviceCredentials>
           <clientCertificate findValue="00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00" x509FindType="FindByThumbprint" >
           </clientCertificate>
           <serviceCertificate findValue="00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00"
x509FindType="FindByThumbprint"/>
         </serviceCredentials>
       </behavior>
      </serviceBehaviors>
   </behaviors>
```

In the above configuration, configure the *findValue* and *x509FindType* according to the Server Certificate and the Client Certificate.

Configuring Security for ESM

The Oracle Argus Interchange service should be configured to run under a Domain user. This domain user should have appropriate privileges to some Interchange related folders, as given below:

- `<Interchange Service Install Path>\DTDFiles` - Full Control
- `Outgoing` Folder- Full Control
- `Attachment Outgoing` Folder- Full Control
- `Incoming` Folder- Full Control
- `Log` Folder- Full Control

For E2B Viewer, the folder referred to as the Template path in `Argus.ini` (`<ArgusInstallPath>\E2BViewer\Templates\`) needs to be given Full Access. This folder is used for CIOMS and MedWatch views.

These changes must be validated at the box placed at the following location:

`<ArgusInstallPath>\E2BViewer\Templates\`

Configuring Security for AG Service

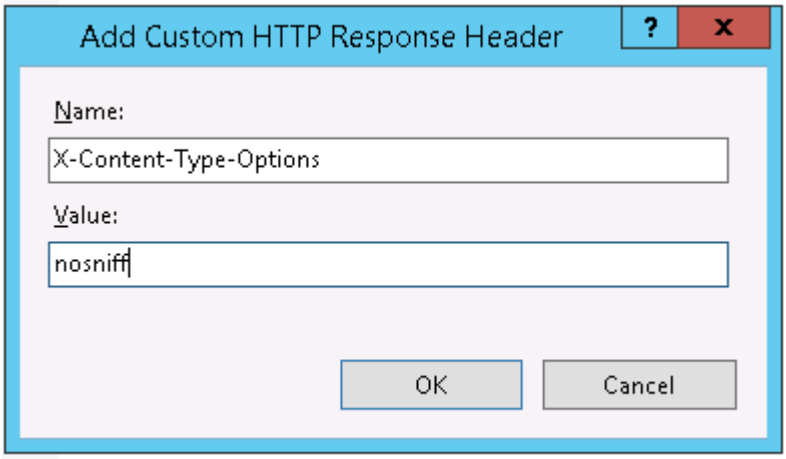
For AG Service to correctly show the status of all the processes on AG Service Configuration screen, the Safety_User needs R/W access to `AGService.INI` file.

Configuring 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, set the **Name** to "X-Content-Type-Options" and the **Value** to "nosniff", then click **OK**.



Configuring Oracle Argus Safety with Minimum Security

In this chapter:

Configure the IIS Manager for Windows Server

> **Note:**
>
> For Windows Server, IIS 6 Management Compatibility and Application Development > ASP.NET/ASP roles must be installed.

1. Select **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand the Connection Panel and open **Sites**.
3. Select **Argus Safety Web**.
4. On the right panel, click **Basic Settings**.
5. Click **Connect as…**
6. Click **Specific User** and click **Set**.
7. Enter Domain user name and password, and click **OK**.
8. Click **OK**.
9. To verify the user credential is valid for the connection, click **Test Settings**.

Secure Sensitive Configuration and Operational Data

To make sure that only the IIS user with Administrator rights can access the following files and folders, set the minimum permission as **Full Control** for the user under which IIS is running.

- `Argus.ini` Windows directory file
- `MessageCache` shared folder

Configure Identity in the IIS Application Pools

1. Select **Start > Administrative Tools > Internet Information Services (IIS) Manager.**
2. Select **Application Pools**.
3. Right-click the **Argus Console Pool** and select **Advanced** settings.
4. In the identity field, enter user ID and password.
5. Reset IIS.

> **Note:**
>
> Make sure to reset IIS after modifying the areas listed in the Reset IIS section of the *Oracle Argus Safety Installation Guide*.

6. Repeat the same configuration for **Argus NET Pool**.

> **Note:**
>
> This configuration will prevent any error when filtering data on the Worklist Portal screen.

Configure Oracle Argus Safety Windows Service to run as a Domain User

1. Select **Control Panel > Administrative Tools > Services**.
2. Double-click **Argus Safety Windows Service**.

   The Argus Safety Windows Service Properties (Local Computer) dialog box appears.
3. Click the **Log On** tab.
4. Click **This Account**.
5. Enter the credentials.
6. Click **OK**.
7. Right-click the **Windows Service** and select **Restart**.