Oracle Argus Safety

Minimum Security Configuration Guide

Release 7.0.3

E40568-01

July 2013

This guide describes essential security management options for the following application:

- Oracle Argus Safety 7.0.3

1 Introduction

This document outlines the steps that help strengthen application security. Note that this document is not a replacement for the Argus Safety Installation Guide. The Installation Guide should be referred for Argus Safety installation instructions.

This document has been created to act as a step-by-step Guide for Minimum Security Configurations on Argus Safety Web and Report Servers.

This guide presents the following security guidelines and recommendations:

ORACLE

2 Post Installation Security Configurations

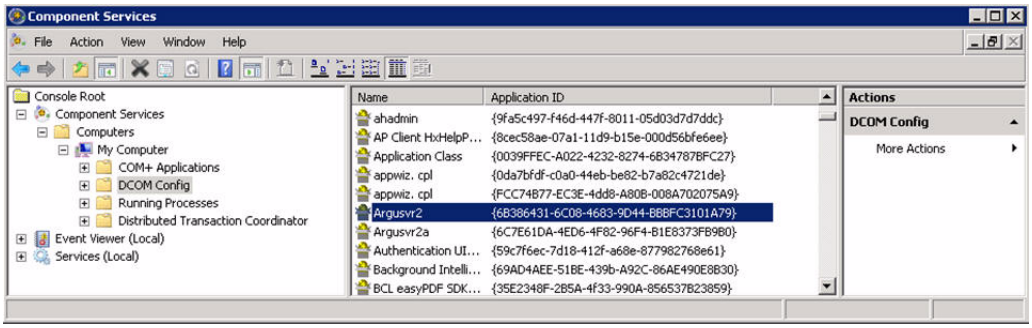
This document lists the various security configurations required after installing Argus Safety:

2.1 Configuring Argusvr2/Argusvr2a Permissions

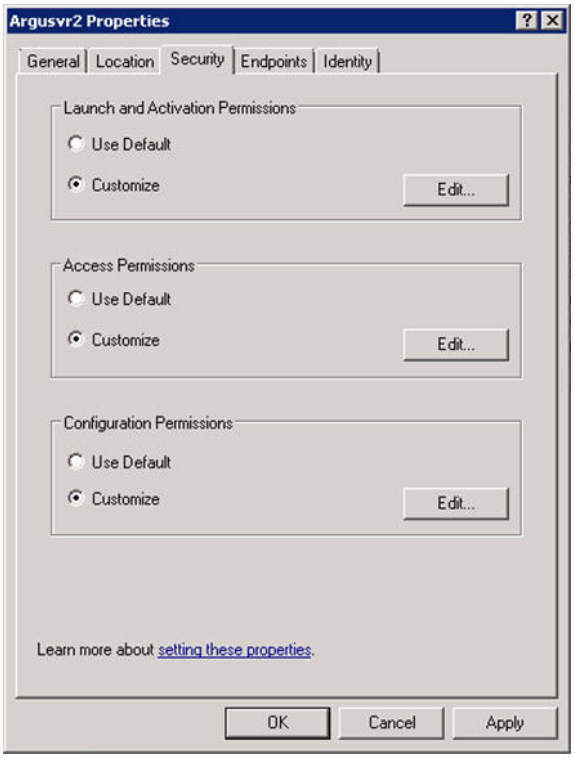
> **Note:** This section needs to be applied to each Web and Report Server.

Execute the following steps to configure Argusvr2/Argusvr2a permissions:

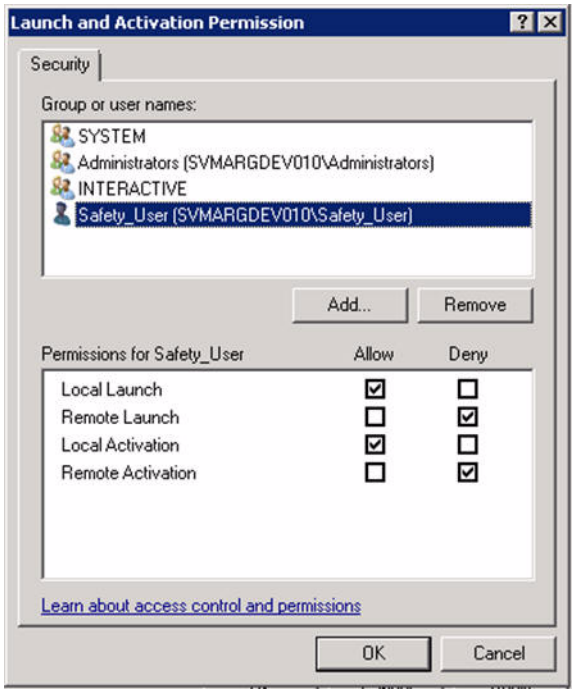
1. Create a domain user which has access to web-servers and all network services that will be configured in Argus such as shared network paths for Intake.
   - In the steps mentioned below, we have used a sample user called 'Safety_User', throughout this section of the Guide.
2. Go to every web server 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:
      – Right-click on Argusvr2 and select Properties.
      – Select the Security tab.
      – Select Customize for these options: **Launch and Active Permissions**, and **Access Permissions**.

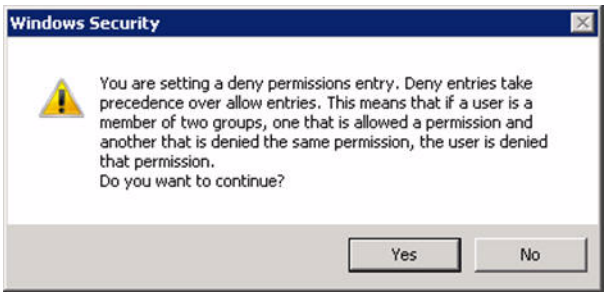


- Click **Edit** under **Launch and Activation Permissions**.
- Add **Domain User** for **Launch and Activation Permissions** with **Local Launch** and **Local Activation** permission selected. Select **Deny** for **Remote Launch** and **Remote Activation**.



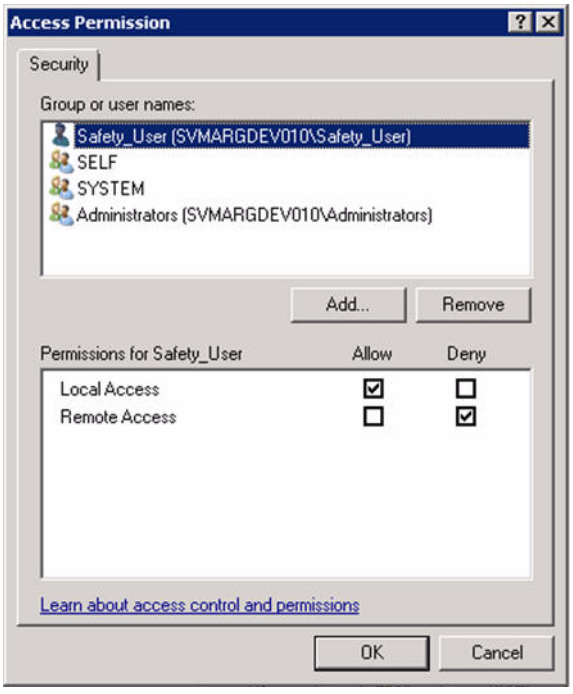
- Click **OK**.

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



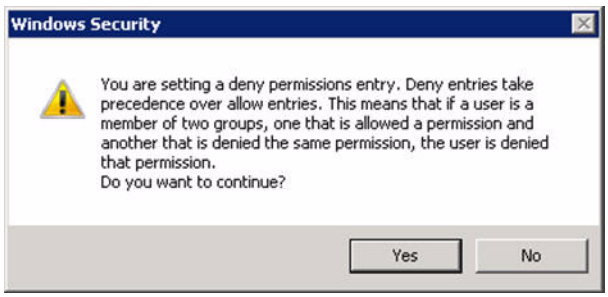
– Click **Edit** for **Access Permissions**.

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

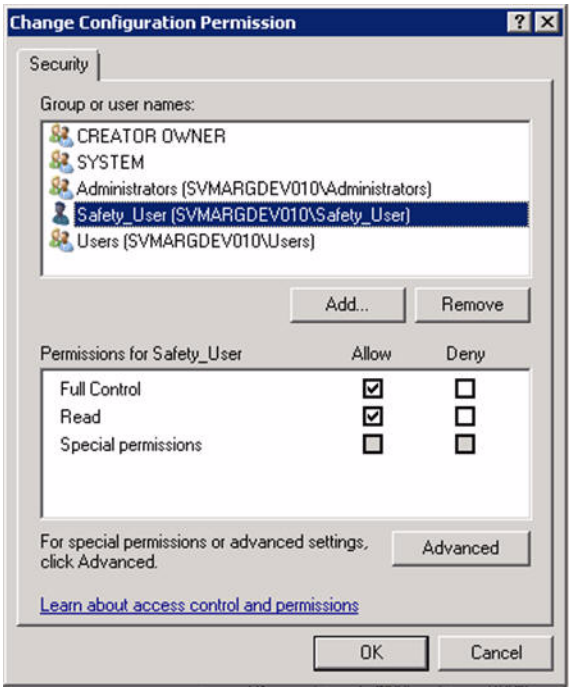


– Click **OK**.

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



- Click **Edit** for Configuration Permissions.
- Add a domain user for **Change Configuration Permission**, with **Full Control** and **Read** permissions selected.

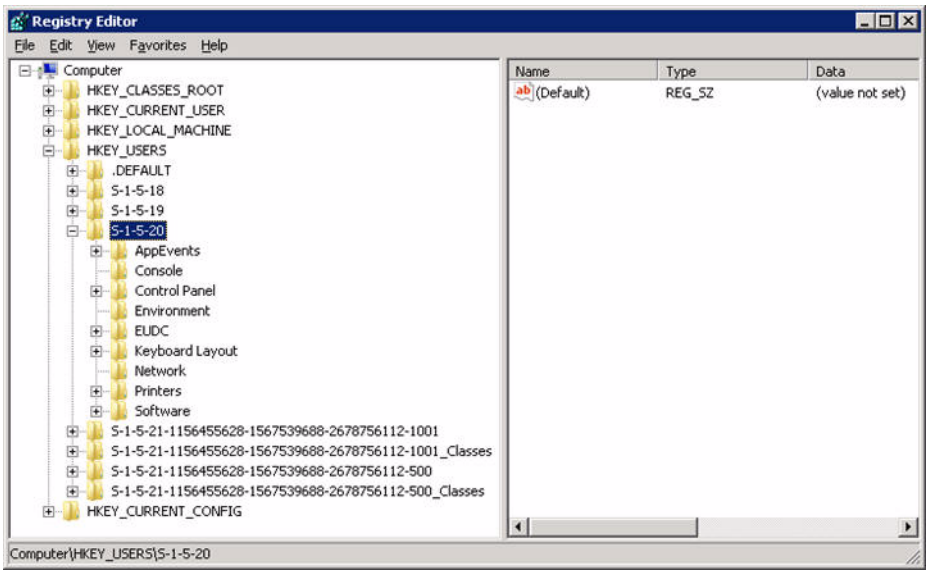


- Click **OK**.
- Click **OK** on the **Argusvr2 Properties** dialog to save the changes.

f. Perform the same changes from Step 2C for Argusvr2a and BCL EasyPDF (BCL easyPDF SDK Loader, bclprnmso).

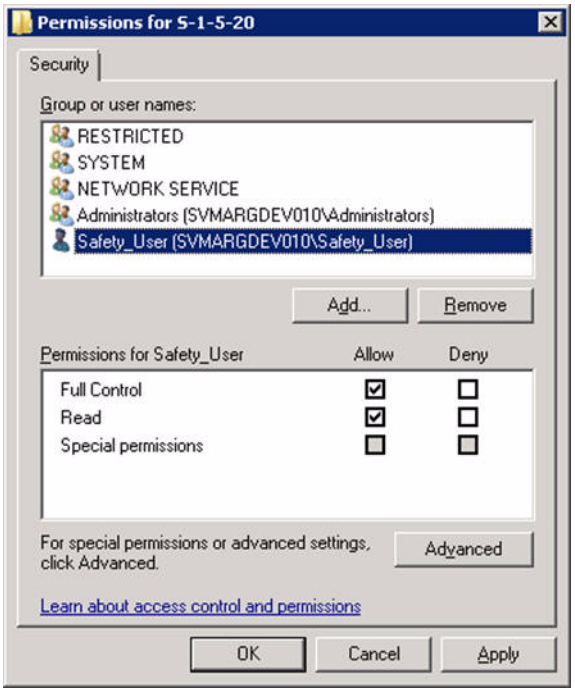
3. Run the Registry tool in Windows, as shown below:

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.



d. Give permission to Access IIS Metabase to **Safety_User** with the following command:

```
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -ga "Safety_
User"
```

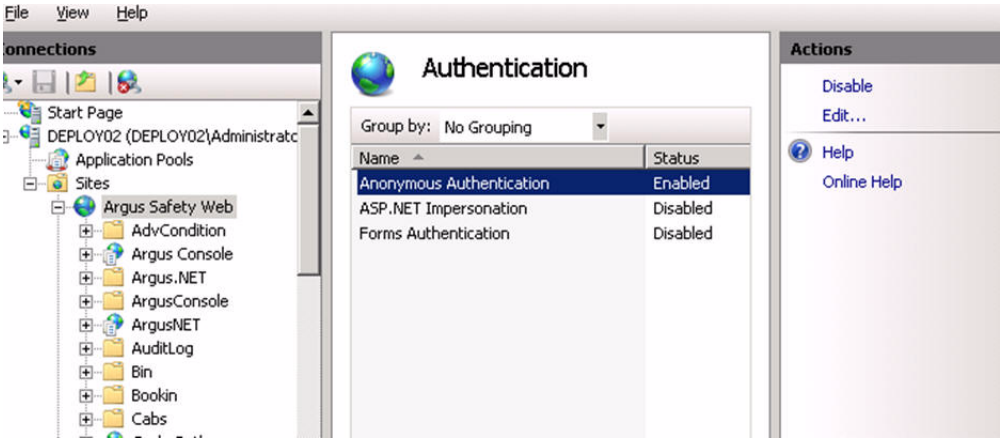
3 Configuring Folder Access to Web User Account

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

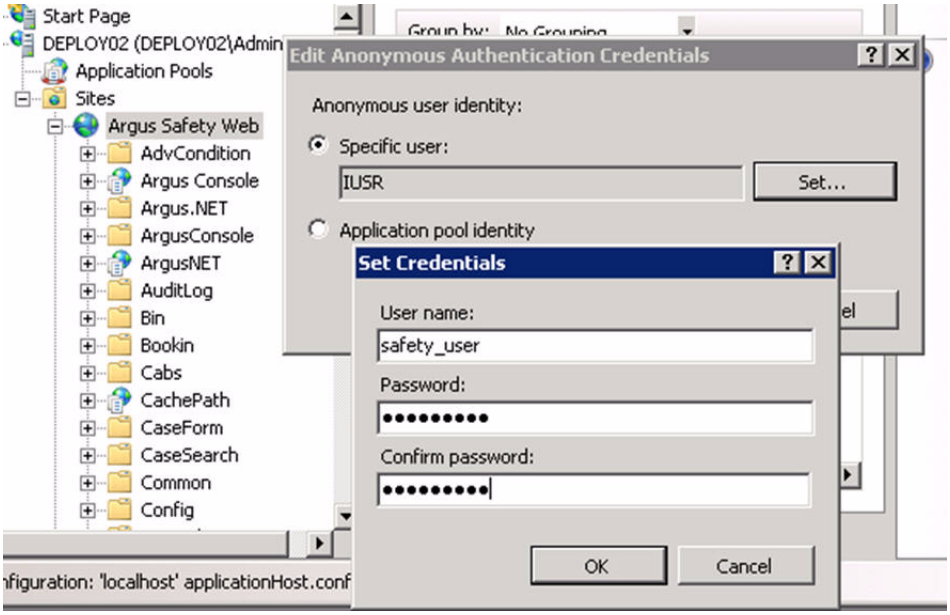
1. On every Web Server/Report Server, Anonymous access should be configured as follows:

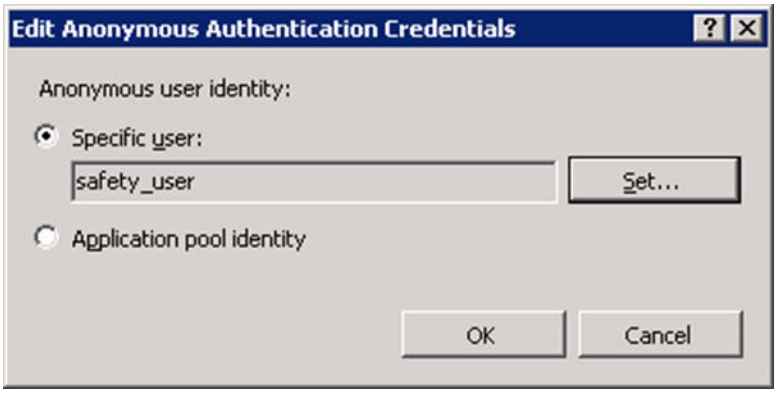
   a. Go to **IIS Configuration Manager** > **Authentication**:

b. Edit **Anonymous Authentication**:



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



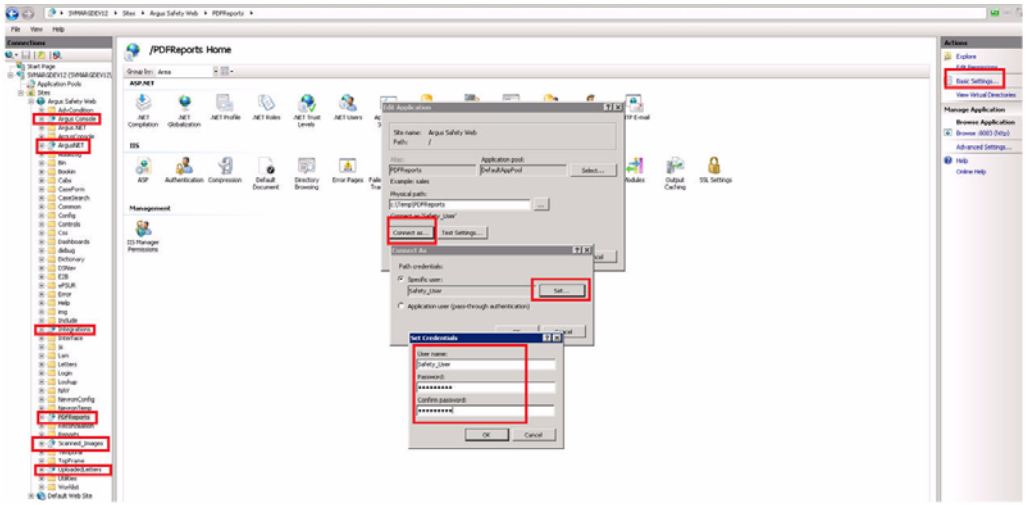


2. On every Web Server:

   PDFReports, UploadedLetters, Integrations, GHP, ArgusNet, Argus Console, and Scanned_Images virtual directory should be configured to connect as Safety Domain User [Safety_User] as follows:

   a. Select virtual directory and click on Basic Settings.

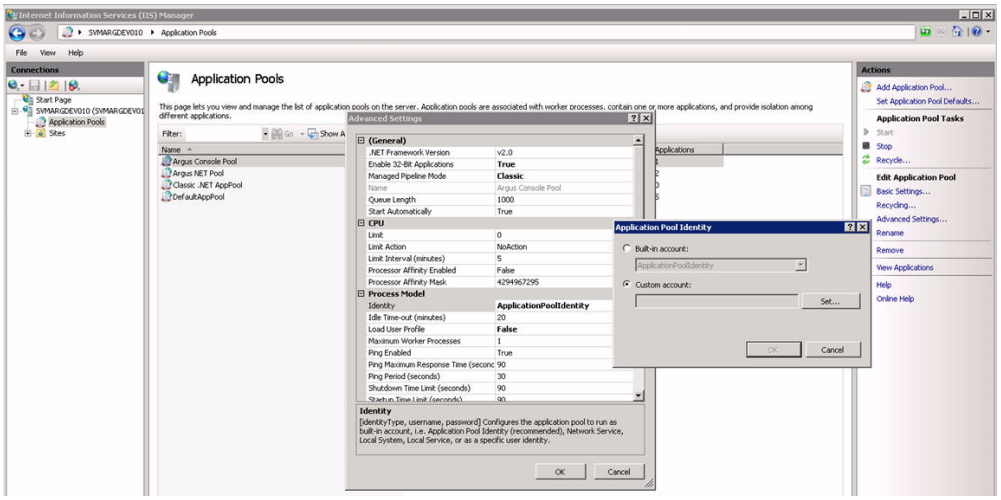
   b. Select Connect as > Set Path Credentials > Enter Safety Domain User [Safety_User] and Password



3. 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

4. Configure Application Pools.



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

5. Restart the Web Server.

4 Configuring Log Folders, SQLTimes Path, and Access Permissions

4.1 Configuring Log Folders

The various modules of Argus Safety Web 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.config
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 Argus Safety Website has been configured to run as.

4.2 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]

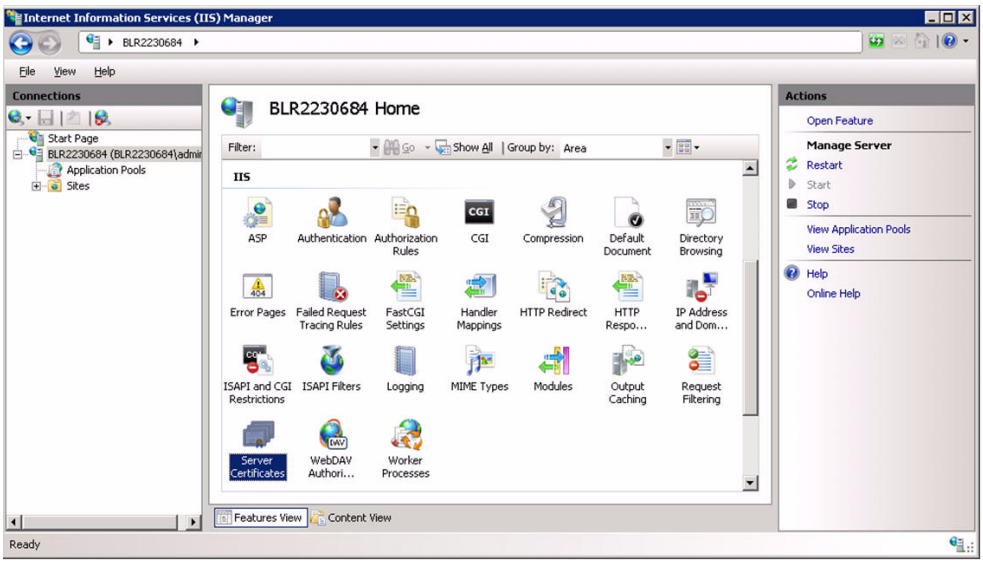
SqlTimesPath=C:\Temp\ArgusLogs\SqlTimes

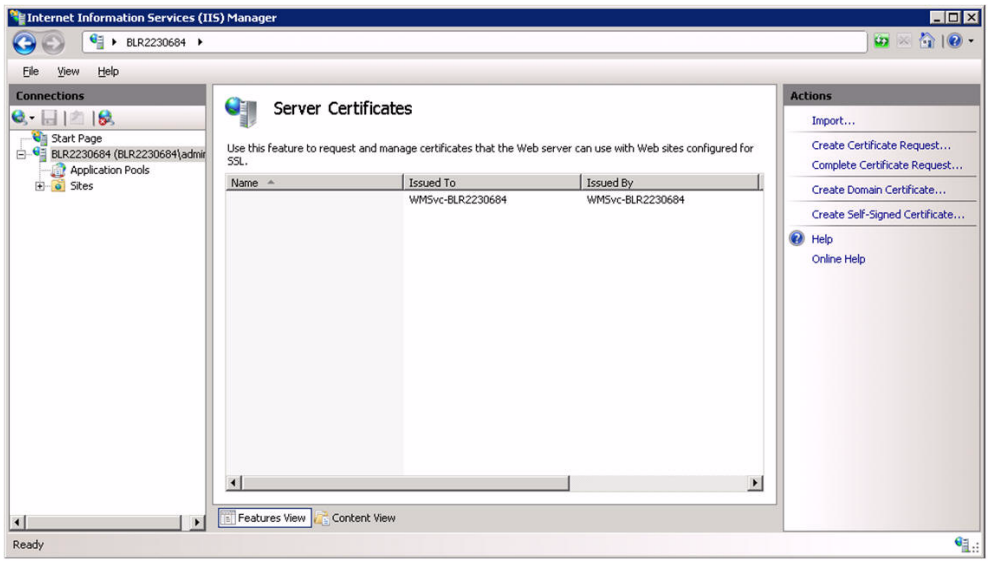
This folder needs to have Read/Write/Modify permissions to the Domain user with which the Argus Safety Website has been configured to run.

5 Configuring HTTPS

Execute the following steps to configure HTTPS:

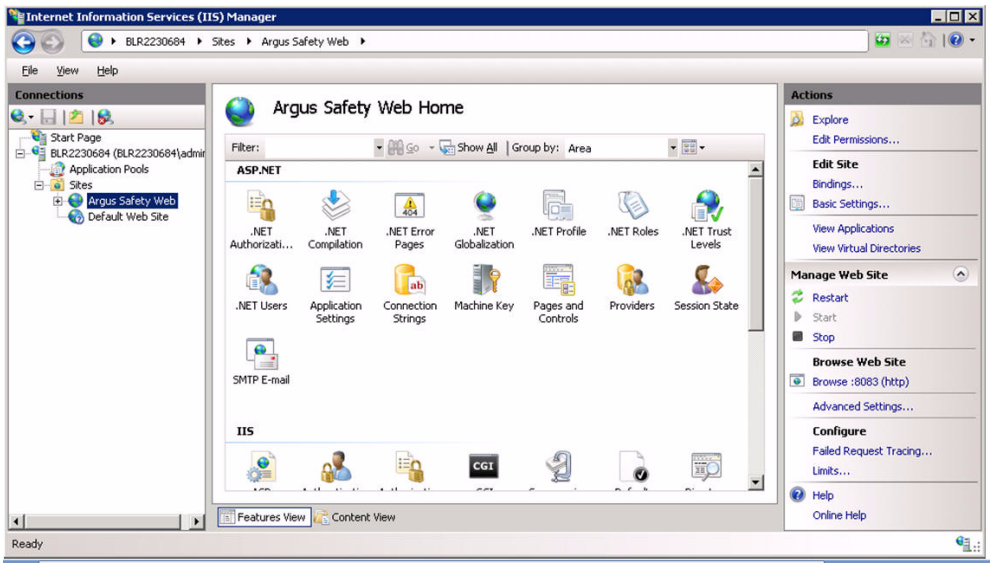
1. Login to each Web Server and Report Server and perform the following steps to configure HTTPS.
2. Launch the **Internet Information Services (IIS) Manager**.
3. Select the server node as shown in the diagram below and then open the **Server Certificates** under the **IIS** section.



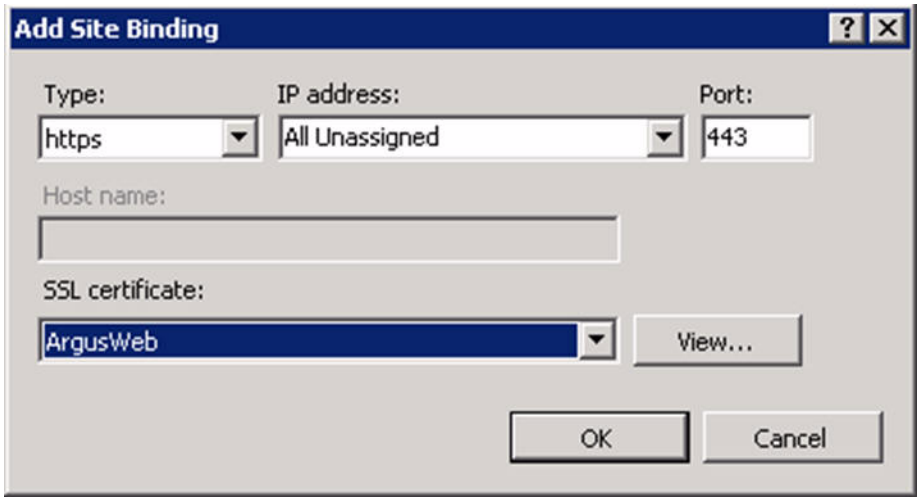


4. Create/import your SSL certificate.

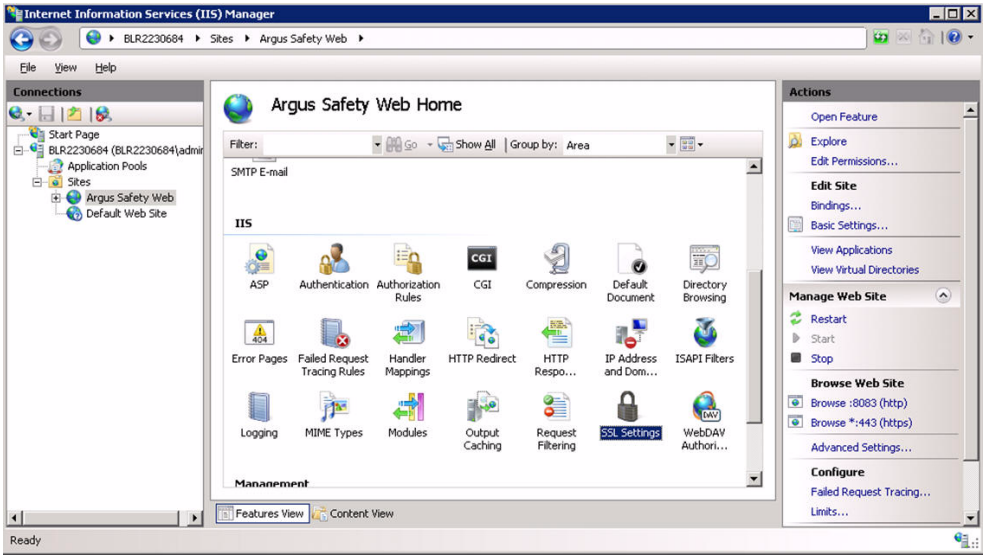
5. After the certificate is created, select **Argus Safety Web** under the **Sites** option and go to **Actions > Bindings**.



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 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**.

6 Configuring Password Complexity

Execute the following steps to configure password complexity:

1. Log in to 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:
   a. 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.
   b. Minimum number of characters in the password: This defines the minimum length of a password.
   c. 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.

7 Configuring Case Intake Folders and Security

The Argus 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 Intake.

8 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.
2. By default, the bindingConfiguration used by the Service Endpoint is *wsHttpUnsecure*.
3. 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.
4. 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>
```

5. 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.

6. 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.

9 Configuring Security for ESM

The 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

10 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.

11 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.

Oracle Argus Safety Minimum Security Configuration Guide Release 7.0.2
E40568-01

to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.