Oracle® Argus Safety

Minimum Security Configuration Guide

Release 8.1

E76730-01

September 2016

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

• Oracle Argus Safety 8.1

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:

- Post Installation Security Configurations
- Configuring Folder Access to Web User Account
- 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
- Documentation Accessibility

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.

ORACLE

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:
 - Go to **Control Panel** > **Administrative Tools**.
 - Open **Component Services**.
 - Go to Console Root > Component Services > Computers > My Computer.
 - Select DCOM Config:

Component Services					
Action View Window Help ♦ ♦ 2 □ K □ 0 0 0 0 0 10 10 10 10 10 10 10 10 10 10					
🔁 Console Root	Name	Application ID		Actions	
Component Services	🚔 ahadmin	{9fa5c497-f46d-447f-8011-05d03d7d7ddc}	_	DCOM Config	
Computers My Computer COM+ Applications COM+ Config Decomo Decompose	AP Client HxHelpP Application Class appwiz. cpl appwiz. cpl	{8cec58ae-07a1-11d9-b15e-000d56bfe6ee} {0039FFEC-A022-4232-8274-6834787BFC27} {0da7bfdr-C0a0-44eb-be82-b7a82c4721de} {FCC74877-EC3E-4dd8-A808-008A702075A9}		More Actions	,
Distributed Transaction Coordinator	Argusvr2	{6B386431-6C08-4683-9D44-BBBFC3101A79}			
 Event Viewer (Local) G Services (Local) Cocal) 	Argusvr2a Authentication UI Background Intelli BCL easyPDF SDK	{6C7E61DA-4ED6-4F82-96F4-B1E8373F8980} {59c7f6ec-7d18-412f-a68e-877982768e61} {69AD4AEE-51BE-439b-A92C-86AE490E8B30} {35E234BF-285A-4F33-990A-856537B23859}	•		

- 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.

eneral Location Security Endpoints Id	lentity
Launch and Activation Permissions	
C Use Default	
Customize	Edit
C Access Permissions	
C Use Default	
Customize	Edit
Configuration Permissions	
C Use Default	
Customize	Edit
Learn more about <u>setting these properties</u> .	

- 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.

urity	on	
oup or user names:		
& SYSTEM Administrators (SVMARGDE INTERACTIVE Safety_User (SVMARGDEV	V010\Administrator 010\Safety_User)	s)
	Add	Remove
rmissions for Safety_User	Allow	Deny
Local Launch Remote Launch Local Activation Remote Activation		
and about access control and	permissions	

• 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.

o or user names: Safety_User (SVMARGDEV) SELF SYSTEM Administrators (SVMARGDE)	010\Safety_User) V010\Administrator Add	rs) Remove
Safety_User (SVMARGDEV) SELF SYSTEM Administrators (SVMARGDE)	010\Safety_User) V010\Administrator Add	rs) Remove
SELF SYSTEM Administrators (SVMARGDE [\]	V010\Administrator	rs) Remove
5YSTEM Administrators (SVMARGDE)	V010\Administrato	rs) Remove
Administrators (SVMARGDE1	Add	Remove
	Add	Remove
	Add	Remove
ssions for Safety_User	Allow	Deny
cal Access		
mote Access		\square
about access control and p	permissions	
about access control and p	permissions	1

- 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.

nge Configuration Permissio	on	
curity		
roup or user names:		
& CREATOR OWNER		
SYSTEM		
Administrators (SVMARGDE	V010\Administrator	(8)
Safety_User (SVMARGDEV	010\Safety_User)	
M Users (SVMARGDEV010\U	sers]	
	Add	Remove
ermissions for Safety_User	Allow	Deny
Full Control		
Read		
Special permissions		
or special permissions or advance	ced settings	A.d
or special permissions or advanc lick Advanced.	ced settings,	Advanced
or special permissions or advanc lick Advanced.	ced settings,	Advanced
or special permissions or advanc lick Advanced. earn about access control and p	ced settings,	Advanced

- Click **OK**.
- Click **OK** on the **Argusvr2 Properties** dialog to save the changes.
- Perform the same changes from Step 2C for Argusvr2a and BCL EasyPDF (BCL easyPDF SDK 7 (or 6) Loader, bclprnmso).
- **3.** Run the Registry tool in Windows, as shown below:
- 4. Browse to the HKEY_USERS\S-1-5-20 folder:

💻 Computer	Name	Туре	Data
Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_LOCAL_MACHINE HKEY_LOCAL_MACHINE HKEY_LOCAL_MACHINE S-1-5-18 S-1-5-18 S-1-5-19 S-1-5-20 S-1-5-20 EControl Panel Environment EControl Panel Environment EControl Panel Environment ESoftware S-1-5-21-1156455628-1567539688-2678756112-1001 S-1-5-21-1156455628-1567539688-2678756112-1001 Classes S-1-5-21-1156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-1-5-21-156455628-1567539688-2678756112-500 S-15-21-156455628-1567539688-2678756112-500 S-15-21-156455628-1567539688-2678756112-500 S-15-21-156455628-1567539688-2678756112-500 S-15-21-156455628-1567539688-2678756112-500 S-15-21-156455628-1567539688-2678756112-500	(Default)	REG_SZ	(value not set
HEY_CURRENT_CONFIG	21		

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

iroup or user names: & RESTRICTED & SYSTEM METWORK SERVICE					
WETMODV CEDVICE	SYSTEM				
A L CLARK SERVICE	010141				
Administrators (SVMARGDEV	10\Safetu User)	sj			
Darch Osci (Shinki (DEAO	novalety_oset)				
	Add	Bemove			
		1011010			
ermissions for Safety_User	Allow	Deny			
Full Control					
Read					
Special permissions					
Special permissions					
Special permissions					
Special permissions	ed settings,	Ad <u>v</u> anced			
Special permissions or special permissions or advance ck Advanced.	ed settings,	Ad <u>v</u> anced			
Special permissions r special permissions or advance ck Advanced. arn about access control and pe	ed settings,	Ad <u>v</u> anced			
pecial permissions special permissions or advance (Advanced. In about access control and pr	ed settings,	Advanced			

7. 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"

2.2 Configuring BCL easyPDF Permissions

Execute the following steps to configure BCL easyPDF permissions:

- **1.** Go to every web server and configure the following:
 - Go to **Control Panel** > **Administrative Tools**.
 - Open Services.
 - Select and right-click BCL easyPDF SDK 7 (or 6) Loader.
 - Click Properties.

ervices						
Action View	Help					
Services (Local)						
	Q Services (Local)					
	BCL easyPDE SDK 6 Loader	Name -	Description	Status	Startup Type	Log On As
		Background Intelligent Transfer Service	Transfers files in the background using idle network bandwi	Started	Manual	Local System
	Stop the service	Base Filtering Engine	The Base Filtering Engine (BFE) is a service that manages fir	Started	Automatic	Local Service
	Restart the service	BCL easyPDF SDK 6 Loader	Enables easyPDF SDK 6 on server-side environment.	Started	Manual	Local System
	L	Certificate Propagation	Copies user certificates and root certificates from smart		Manual	Local System
	Description:	CNG Key Isolation	The CNG key isolation service is hosted in the LSA proce Sb	op	Manual	Local System
	Enables easyPDF SDK 6 on server-side	COM+ Event System	Supports System Event Notification Service (SENS), whi	Resume	Automatic	Local Service
	environmenc.	COM+ System Application	Manages the configuration and tracking of Component (Manual	Local System
	1	Computer Browser	Maintains an updated list of computers on the network a Re	start	Disabled	Local System
	1	🖗 Credential Manager	Provides secure storage and retrieval of credentials to (Tasks +	Manual	Local System
	1	Cryptographic Services	Provides four management services: Catalog Database		Automatic	Network Service
	1	DCOM Server Process Launcher	The DCOMLAUNCH service launches COM and DCOM se Re	fresh	Automatic	Local System
	1	🖗 Desktop Window Manager Session Man	Provides Desktop Window Manager startup and mainter	operties	Automatic	Local System
	1	C DHCP Client	Registers and updates IP addresses and DNS records fc		Manual	Local Service
	1	Diagnostic Policy Service	The Diagnostic Policy Service enables problem detection He	lp .	Automatic (D	Local Service
	1	Diagnostic Service Host	The Diagnostic Service Host is used by the Diagnostic Policy		Manual	Local Service
	1	🖗 Diagnostic System Host	The Diagnostic System Host is used by the Diagnostic Policy		Manual	Local System
	1	😳 Disk Defragmenter	Provides Disk Defragmentation Capabilities.		Manual	Local System
	1	Oistributed Link Tracking Client	Maintains links between NTFS files within a computer or acro	Started	Automatic	Local System
	1	Distributed Transaction Coordinator	Coordinates transactions that span multiple resource manag	Started	Automatic (D	Network Service
	1	Q DNS Client	The DNS Client service (dnscache) caches Domain Name Sys	Started	Automatic	Network Service
		Committee Elle Curteen /EEC)	Received the case file answertian technology used to store a		Manual	Lard Curtan

- Click the **Log On** tab and:
- Click the **This account** radio button.
- Set user credentials to the Safety domain user (Safety_User) and click **OK**.

C Local System acco	unt	
Allow service to	interact with desktop	
This account:	Safety_User	Browse
Password:	•••••	
Confirm password:	•••••	-

- When the **General** tab opens:
 - Select **Automatic** from the **Startup type** drop-down list.
 - Click **OK** to close the **Properties** dialog box.
- When the system returns to the main Services window, start the BCL easyPDF SDK 7 (or 6) Loader.
- Close the Services window.

3 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:
- Go to **IIS Configuration Manager** > **Authentication**:



• Edit Anonymous Authentication:

nnections			Actions
s- 🗔 121 188 🔰 😔 👘		Disable	
Start Page	Group by: No Grouping		Edit
DEPLOY02 (DEPLOY02\Administratc	. No Grouping	1	D Liele
Application Pools		Status	Heip
🖻 👩 Sites 🛛 🔹 Anonymo	us Authentication	Enabled	Online Help
🖻 😜 Argus Safety Web 🛛 🔹 ASP.NET	Impersonation	Disabled	
AdvCondition Forms Au	thentication	Disabled	
🕀 🔐 Argus Console			
🕀 🛁 Argus.NET 🚽			
🕀 🚞 ArgusConsole			
🕀 💮 ArgusNET			
🕀 🚞 AuditLog			
🕀 🛗 Bin			
🕀 🛅 Bookin			
🕀 🛗 Cabs			

• Set user credentials to the Safety domain user (Safety_User):

Start Page	Edit Anonymous Authentication Credentials	?×
Application Pools Sites Argus Safety Web AdvCondition One Argus Console	Anonymous user identity:	
 ⊕- ☐ Argus.NET ⊕- ☐ ArgusConsole ⊕- ⊕ ArgusNET ⊕- ☐ AuditLog ⊕- ☐ Bin 	C Application pool identity Set Credentials User name:	
Bookin Cabs CachePath CaseForm CaseSearch Common	safety_user Password: •••••••• Confirm password: ••••••••	F
rfiguration: 'localhost' applicationH	ost.conf	

Edit	Anonymous Authenticatio	n Credentials	? ×
Ar	nonymous user identity:		
œ	Specific <u>u</u> ser:		
	safety_user		<u>S</u> et
0	Application pool identity		
		ОК	Cancel

• 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:

- Select virtual directory and click on Basic Settings.
- Select Connect as > Set Path Credentials > Enter Safety Domain User [Safety_User] and Password

V12 + Sites + Argus Safety Web + POFRaports +	- W
12 1 2 de	Supervised and

- 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
- Configure Application Pools.

Platemet Information Services (119	5) Manager							
SVMARGDEV010	Application Pools						🔛 🗠 🔂 I 🕑 +	
File View Help								
Connections	-						Actions	
Start Page	Application Pools This page lets you view and manage the list of different applications.	Add Application Pool Set Application Pool Defaults Application Pool Tasks						
+ Sites	Filter:	Show A					▶ Start	
0.000	Name 4	E (General)	🗄 (General)				Stop	
	Annua Concele Deal	.NET Framework Version	v2.0	Appacations			2. Recurle	
	Argus Console Pool	Enable 32-Bit Applications	True		2		- nocyoun	
	Classic NET Applical	Managed Pipeline Mode	Classic				Edit Application Pool	
	Cidool: INC PApprovi	Name	Argus Console Pool		e la		Basic Settings	
	Construction of the second sec	Queue Length	1000		P		Recycling	
		Start Automatically	True				Advanced Settings	
		E CPU	E CPU Application Pool Identity					
		Limit	0	Transa		Kename		
		Limit Action	NoAction	C Bult	-in account:		Remove	
		Limit Interval (minutes)	5	ann	ApplicationPoolIdenbity		Man Analyshing	
		Processor Affinity Enabled	False	1.99			view Appacaciono	
		Processor Affinity Mask	4294967295	 Cust 			Help	
		E Process Model					Online Help	
		Identity	ApplicationPoolIdentity	1				
		Idle Time-out (minutes)	20					
		Load User Profile	False					
		Maximum Worker Processes	1				1	
		Ping Enabled	True			Cancel		
		Ping Maximum Response Time (see	conc 90	-				
		Ping Period (seconds)	30					
		Shutdown Time Limit (seconds)	90					
		Startun Time Limit (seconds)	90	-				
	Identity [identityType, username, password] built-in account, i.e. Application Pool Local System, Local Service, or as a	Configures the application pool to ru Identity (recommended), Network Se specific user identity.	n as ervice,					
			ок	Cancel	<i>h</i>			

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

Note: Argus Web Pool has the same settings as defined for Argus Console Pool and Argus NET Pool.

• 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**.

Internet Information Services (II)	5) Manager								- 🗆 ×
BLR2230684 S	Sites 🕨 Argus Sa	afety Web 🔸						1 🛛 🖉	10-
Eile <u>V</u> iew <u>H</u> elp									
Connections	Actions								
Start Page	Filter:	us salety	Go - Group by: Area				•	Explore Edit Permissions	
BLR2230684 (BLR2230684)admir BLR2230684 (BLR2230684)admir Difference Stes Argus Safety Web	ASP.NET			<u> </u>	R			Edit Site Bindings	
	.NET Authorizati	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	View Applications View Virtual Directories	
	.NET Users	Application Settings	Connection Strings	Machine Key	Pages and Controls	Providers	Session State	Manage Web Site CREstart Start Stop Browse Web Site CREstart Description	٢
	II5		View	CGI	A.			Advanced Settings Configure Failed Request Tracing Limits Welp Online Help	
Ready	Ling. Cardios Hor	201 KOIN							•

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.

ype:	IF	Paddress:		Port:
ittps	- 4	All Unassigned		▼ 443
lost name:				
SI cartificata				
or certificate	·			1
			-	View

- 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.

③ ◎ ● ▶ BLR2230684 ▶ 5	ites 🕨 Argus S	5afety Web 🔸) 🖬 🖂 🖄 I 🕲
File Yew Help Connections	Arous Safety Web Home								Actions
Start Page BLR2230684 (BLR2230684\admir BLR2230684 (BLR2230684) Application Pools Sites Application Safety Web Gofault Web Site	Filter: SMTP E-mail	·····,	• 89 50 • (Show All G	roup by: Area		•		Open Feature Explore Edit Permissions Edit Site Bindings
	ASP	Authentication	Authorization Rules	CGI CGI	Compression	Default Document	Directory Browsing		View Applications View Virtual Directories Vianage Web Site
	Error Pages	Failed Request Tracing Rules	Handler Mappings	HTTP Redirect	HTTP Respo	IP Address and Dom	ISAPI Filters		Start Stop Browse Web Site Browse :8083 (http) Browse *:443 (https)
	Logging Manageme	MIME Types	Modules View	Output Caching	Request Filtering	SSL Settings	WebDAV Authori	<u>.</u>	Advanced Settings Configure Failed Request Tracing Limits

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.

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:
- **6.** 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.
- **7.** Minimum number of characters in the password: This defines the minimum length of a password.
- **8.** 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:

- Locate the <system.serviceModel> section in the <ArgusInstallPath>\Integrations\web.config file.
- By default, the bindingConfiguration used by the Service Endpoint is *wsHttpUnsecure*.
- 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>
```

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

```
<br/><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.

• Modify the Service Behavior configuration as follows:

```
<br/>
```

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 Configuring Security for BCL easyPDF SDK 7 (or 6) Loader

Minimum Security User configuration should be performed on BCL easyPDF SDK 7 (or 6) Loader service for Login.

This ensures that if the user configures the Report Server and attaches the attachment to the Expedited Report, the Expedited Report will generate the PDF without any failure.

12 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=trs if you are hearing impaired.

Oracle Argus Safety Minimum Security Configuration Guide Release 8.1

E76730-01

 $[\]operatorname{Copyright} @$ 2016 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them 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 END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.