# Oracle Argus Safety Minimum Security Configuration Guide



Release 8.4 F51719-02 September 2022

ORACLE

Oracle Argus Safety Minimum Security Configuration Guide, Release 8.4

F51719-02

Copyright © 2019, 2022, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

## Contents

#### Preface

Audience	iv
Documentation accessibility	iv
Related resources	iv
Access to Oracle Support	iv

## 1 Minimum Security Configuration Guide

Keep up to date on software and latest Critical Patch Updates	1-1
Post Installation Security Configurations	1-2
Configuring Argusvr2/Argusvr2a Permissions	1-2
Configuring Folder Access to Web User Account	1-8
Configuring Log Folders, SQLTimes Path, and Access Permissions	1-12
Configuring Log Folders	1-12
Configuring SQLTimes Path	1-13
Configuring HTTPS	1-13
Configuring Password Complexity	1-14
Configuring Case Intake Folders and Security	1-15
Configuring Security for Interface Web Service	1-15
Configuring Security for ESM	1-16
Configuring Security for AG Service	1-16
Configuring X-Content-Type-Options in IIS	1-16
(Optional) Configuring Content Security Policy	1-17
Configuring Oracle Argus Safety with Minimum Security	1-17
Configure the IIS Manager for Windows Server	1-17
Secure Sensitive Configuration and Operational Data	1-18
Configure Identity in the IIS Application Pools	1-18
Configure Oracle Argus Safety Windows Service to run as a Domain User	1-18



### Preface

This preface contains the following sections:

- Audience
- Documentation accessibility
- Related resources
- Access to Oracle Support

## 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**

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 onpremises 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:

- Keep up to date on software and latest Critical Patch Updates
- 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
- (Optional) Configuring Content Security Policy
- Configuring Oracle Argus Safety with Minimum Security

### 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.



## 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:

File Action View Window Help           Image: Second					
Console Root	Name	Application ID		Actions	
Component Services	🚔 ahadmin	{9fa5c497-f46d-447f-8011-05d03d7d7ddc}		DCOM Config	24
Computers     My Computer		{8cec58ae-07a1-11d9-b15e-000d56bfe6ee}		More Actions	
COM+ Applications	Application Class	{0039FFEC-A022-4232-8274-6B34787BFC27} {0da7bfdf-c0a0-44eb-be82-b7a82c4721de}		0.0000000000000000000000000000000000000	
E DCOM Config	appwiz. cpl	{FCC74B77-EC3E-4dd8-A80B-008A702075A9}			
Running Processes Distributed Transaction Coordinator	Argusvr2	{6B386431-6C08-4683-9D44-BBBFC3101A79}			
E levent Viewer (Local)	🚔 Argusvr2a	{6C7E61DA-4ED6-4F82-96F4-B1E8373FB9B0}			
E Services (Local)		{59c7f6ec-7d18-412f-a68e-877982768e61}			
		{69AD4AEE-51BE-439b-A92C-86AE490E8B30}			
	BCL easyPDF SDK	{35E2348F-2B5A-4f33-990A-856537B23859}	•		

- 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.

Launch and Activation Permissions	
C Use Default	
Customize	Edit
Access Permissions	
C Use Default	
Customize	Edit
Configuration Permissions	
C Use Default	
• Customize	Edit
earn more about setting these properties.	

- 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.



oup or user names:		
Administrators (SVMARGDE)	V010\Administrator	(s)
Safety_User (SVMARGDEV	010\Safety_User)	
	Add	Remove
ermissions for Safety_User	Allow	Deny
Local Launch	V	
Remote Launch Local Activation		
Remote Activation		

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

precedence over allow entries. T member of two groups, one that	
another that is denied the same	
that permission. Do you want to continue?	

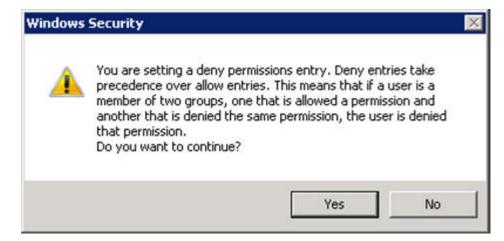


viii. Click Edit for Access Permissions.

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

curity		
iroup or user names:		
Safety_User (SVMARGDEV SELF SYSTEM Administrators (SVMARGDE		[5]
	Add	Remove
ermissions for Safety_User	Allow	Deny
Local Access Remote Access		
earn about access control and p	<u>permissions</u>	
	ОК	Cance

- 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.

ange Configuration Permissi	on	?
ecurity		
Group or user names:		
& CREATOR OWNER		
SYSTEM		
Administrators (SVMARGDE Safety_User (SVMARGDE)		rsj
Users (SVMARGDEV010\L		
	Add	Remove
Permissions for Safety_User	Allow	Deny
Full Control	$\mathbf{\nabla}$	
Read	$\mathbf{\nabla}$	
Special permissions		
For special permissions or advan	ced settings,	Advanced
click Advanced.		
Learn about access control and	permissions	
		Cancel
	OK	Cance



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:

- 🙀 Computer	Name	Туре	Data
HKEY_CLASSES_ROOT     HKEY_CURRENT_USER     HKEY_LOCAL_MACHINE     HKEY_USERS     HKEY_USERS     HKEY_USERS     HKEY_USERS     HKEY_USERS     HKEY_USERS     S-1-5-18     S-1-5-19     S-1-5-19     S-1-5-20     S-1-5-20     Control Panel     Control Panel     DEFAULT     EUDC     HKeyboard Layout     Network     P-10     S-1-5-21-1156455628-1567539688-2678756112-1001     S-1-5-21-1156455628-1567539688-2678756112-1001     S-1-5-21-1156455628-1567539688-2678756112-500     S-15-521-115645568     S-15-521     S-15-521     S-15-521-115645568	(Default)	REG_SZ	(value not set
	•		

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



curity		
roup or user names:		
& RESTRICTED		
SYSTEM		
NETWORK SERVICE		
Administrators (SVMARGD		(15)
🖁 Safety_User (SVMARGDE	V010\Safety_User)	
	Add	Remove
		<u>11</u> 011040
ermissions for Safety_User	Allow	Deny
Full Control		
Read		
Special permissions		
or special permissions or adva	nced settings.	Advanced
ick Advanced.		Advanced
CK MUYANCOU.		
earn about access control and	d permissions	

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

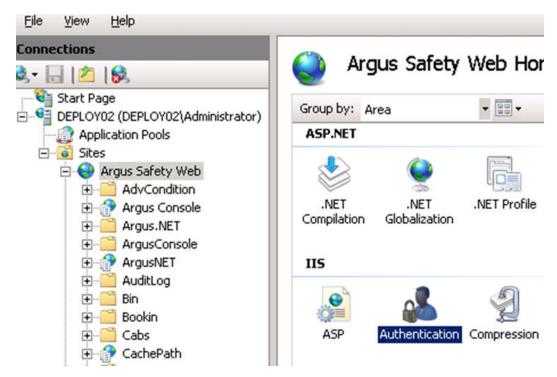
C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\aspnet\_regii s.exe -ga "Safety User"

#### 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:

nnections	A		Actions
• 🗟 🖄 😹	Authentication		Disable
Start Page DEPLOY02 (DEPLOY02)Administrate	Group by: No Grouping		Edit
Application Pools	Name 🔺	Status	🕢 Help
E Sites	Anonymous Authentication	Enabled	Online Help
🖻 😔 Argus Safety Web	ASP.NET Impersonation	Disabled	
🗄 🧮 AdvCondition	Forms Authentication	Disabled	
🗄 💮 Argus Console			
庄 🛁 Argus.NET 🗕 🗕	4		
🕀 🚞 ArgusConsole			
🕀 🔐 ArgusNET			
庄 🦳 AuditLog			
庄 🛅 Bin			
🕀 🛁 Bookin			
🕀 🛗 Cabs			
1 - ^ - · - ·			

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

📲 Start Page	Group by: No Grouping	
DEPLOY02 (DEPLOY02\Admin	Edit Anonymous Authentication Credentials	? ×
- 👩 Application Pools	Eule Anonymous Authentication creaentials	الشلف
🖃 👩 Sites	Anonymous user identity:	
🖻 😌 Argus Safety Web		
	Specific user:	
庄 🔐 Argus Console	IUSR Set	
🕀 🦳 Argus.NET		
🕀 🖳 🗎 ArgusConsole	O Application pool identity	
庄 🔐 ArgusNET	Set Credentials ? 🗙	
🕀 🖳 🔁 🔁 🗄		
庄 🧮 Bin	User name:	el
🕀 🛁 Bookin	safety_user	
庄 🛁 Cabs	Password:	
😟 🔐 CachePath		
😟 🦳 CaseForm		
😟 🧮 CaseSearch	Confirm password:	
主 🛁 Common	•••••	
庄 🛁 Config		
nfiguration: 'localhost' applicationH	lost.conf	

Edit	Anonymous Authenticati	ion Credentials	? ×
An	onymous user identity:		
•	Specific user:		
	safety_user		<u>S</u> et
C	Application pool identity		
		ОК	Cancel

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:



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

5	0		Actions
1 😥	/ArgusNET Home		🔉 Explore
Argus Safety Web	Filter: - T Go - G	Show All Group by: Area	Edit Permissions
- AdvCondition	ASP.NET	and Di anabah Mara	Basic Settings
Argus Console			View Virtual Directorie
ArgusConsole	🛛 🐴 🛸 🔝	👻 🗟 💦 🗐 🖾 🦹 🖏 🥵	
ArgusNET	.NET .NET .NET Error	.NET .NET Profile .NET Trust Application Connection Machine Key Pages and Session State SMTP E-mail	Manage Application
AuditLog	Authorizat Compilation Pages	Edit Application ? ×	Browse Application
Bin	IIS		Browse :8083 (http)
Bookin	🔎 🤷 🖷	Site name: Arous Safety Web	Advanced Settings
Cabs CaseForm			
CaseSearch	ASP Authentic Authorizat Rules	Path: / HTTP Logging MIMEType Respon	s Modules
Common			
Config		Alias: Application pool:	
Controls	Output Request SSL Settings	ArgusNET Argus NET Pool Select	
33	Caching Filtering	Example: sales	
sshboards ctionary	Management	Physical path:	
ctionary Nav		C:\Program Files\Oracle\Argus\Argus\Web\ASP\Argus.N	
28	E &	Comptly 2 X	
rror	Configurat IIS Manager	Pass-through authentication Connect As ? ×	
GHP	Editor Permissions	Connect as Test Settings Path credentials:	
Help			
img Include		Enable Preload     Specific user:	
ntegrations		Set	
Interface		Set Credentials 7 × n authentication)	
js			
Lam		User name:	
etters		safety_user OK Cancel	
Login		Password:	
Lookup NAV			
Portal.NET			
Reports		Confirm password:	
Temporal		••••••	
TopFrame			
ilities			

c. Give full access on the following folders or files to Safety\_User:

 $\texttt{C:\Temp}\$  or Configured Root Folder for temp files

<ArgusInstallPath>

<Documentum Installation Path> and

C:\Documentum

<Windows>\AGService.ini

d. Configure Application Pools.

Connections	0					Actions
Start Page Start Page StyMARGDEV010 (SVMARGDEV01 Application Pools	Application Pools This page lets you view and manage the list of application different applications. Fitter:	Advanced Settings	are associated with worker processes	contain one		Add Application Pool Set Application Pool Default Application Pool Tasks Start
E M Jaces	Lines:	🗄 (General)		-		B 300
	Name *	.NET Framework Version	v2.0		Applications	
	Argus Console Pool	Enable 32-Bit Applications	True		p.	C Recycle
	Argus NET Pool	Managed Pipeline Mode	Classic		2	Edit Application Pool
	Classic .NET AppPool	Name	Argus Console Pool		Þ	Basic Settings
	2 DefaultAppPool	Queue Length	1000		p.	Recycling
		Start Automatically	True			
		E CPU		Construction of	tion Pool Identity	Advanced Settings
		Limit	0	Applicac	don Pool Identicy	Rename
		Limit Action	NoAction	CBuil	it-in account:	Remove
		Limit Interval (minutes)	5			
		Processor Affinity Enabled	False	Ap	oplicationPoolIdentity	View Applications
		Processor Affinity Mask	4294967295	@ 0#	stom account:	Help
		Process Model				
		Identity	ApplicationPoolIdentity		Se	t Online Help
		Idle Time-out (minutes)	20			
		Load User Profile	False			
		Maximum Worker Processes	1			
		Ping Enabled	True		.0K Ca	ancel
		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 Si specific user identity.	n as ervice, Cancel		

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  ${\tt Webgate}$  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
- Configuring SQLTimes Path

#### **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.confi
g
```

<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:

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 and then open the Server Certificates under the IIS section.
- 4. Create/import your SSL certificate.
- 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.



Туре:		IP address:		Port:
https	•	All Unassigned		▼ 443
Host name:				
SL cortificate				
	ə:			1
55L certificate ArgusWeb	•:			View
	•:		<b>•</b>	View
	•:		■ OK	View Cancel

- 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:

 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>
</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.



4. Modify the Service Behavior configuration as follows:

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.
- 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.

## (Optional) Configuring Content Security Policy

Oracle Argus Safety 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 Safety 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).* 

#### Configuring Oracle Argus Safety with Minimum Security

#### In this chapter:

- Configure the IIS Manager for Windows Server
- Secure Sensitive Configuration and Operational Data
- Configure Identity in the IIS Application Pools
- Configure Oracle Argus Safety Windows Service to run as a Domain User

#### 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.

