

# **Interactive Session Recorder**

Security Guide

Release 5.2

December 2016

## Notices

Copyright© 2016, 2014, 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, then 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.

# Contents

- 1 ISR Security Overview..... 7**
- Secure Installation..... 7
- Critical Security Services and Settings..... 7
- Firewalld Configuration Overview..... 8
- ISR Firewalld Configuration..... 9
- Modifying ISR Firewalld Configuration..... 10
- ISR Port Usage..... 10
- ISR Certificate Files..... 11
- Signing Keys..... 11
- Configuring Reduced Security..... 12
- Configuring FACE Reduced Security..... 12

---

---

# About This Guide

The Interactive Session Recorder (ISR) Security Guide provides information about security considerations and best practices from a network and application security perspective for the ISR product.

## Related Documentation

The following table describes the documentation set for this release.

Document Name	Document Description
ISR Release Notes	Contains information about new ISR features, fixes, and known issues.
ISR Installation Guide	Provides an overview of the ISR, hardware/software requirements and recommendations, storage considerations, pre-installation information, installation procedures, post-install verification procedures, making the first call, and additional advanced topics about the ISR.
ISR User Guide	Contains information about using the ISR Dashboard for all levels of users. Provides information about viewing, playing, deleting recordings, running reports, and managing user profiles.
ISR Administrator Guide	Contains information about using the ISR Dashboard for the Administrator level user (Super User, Account Administrator, Tenant Administrator). Provides information about creating and managing accounts, routes, and users. Also provides information about configuring the ISR, running reports, viewing active calls, and securing the ISR deployment.
ISR API Reference Guide	Contains information about ISR FACE, VoiceXML Commands, legacy application programming interfaces (APIs), Recording File Types/Formats Supported, Return Codes, sendIPCRCommand.jsp Subdialog, Advanced Options, and Troubleshooting.
ISR Monitoring Guide	Contains information about installing and configuring the ISR Monitor, the Monitor database schema, and the Monitor MIB.
ISR Remote Archival Web Services Reference Guide	Contains information about the Remote Archival Web Service, its methods, WSDL definitions, DataType definitions, sample responses, and importing its certificates into the client keystore.
ISR Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the ISR product.

## Revision History

Date	Description
September 2016	<ul style="list-style-type: none"><li>Initial release of ISR 5.2 software.</li></ul>
December 2016	<ul style="list-style-type: none"><li>Removes The DMZ firewall zone from the "Firewalld Configuration Overview" section.</li><li>Updates "Modifying the ISR Firewalld Configuration" for accuracy.</li></ul>



---

## ISR Security Overview

This chapter describes how to configure security on the ISR.

---

### Secure Installation

Security begins during ISR installation and choosing appropriate settings during installation helps protect your systems and data. Ensure that the critical security services and settings (described below) are installed and enabled. Oracle strongly recommends using a non-root account for logins to setup, configure, and administer your ISR systems. Choose secure passwords during installation and do not remove secure file permissions settings unless absolutely necessary.

### Critical Security Services and Settings

By default, Oracle Linux 7 comes with several security features enabled. To help ensure the security of your systems, Oracle recommends that you do not disable these features.

- **Firewalld**—On Oracle Enterprise Linux 7, the firewalld service replaces the configuration elements of iptables from previous versions of Enterprise Linux. Keeping the firewalld service enabled and active provides an excellent defensive measure to secure your systems. For more information on the firewalld service, see [http://docs.oracle.com/cd/E52668\\_01/E54669/E54669.pdf](http://docs.oracle.com/cd/E52668_01/E54669/E54669.pdf), section 26.3. By default, the ISR platform utilizes the zones detailed below, and our applications install firewalld service configurations to enable standard communications amongst the various zones. To change the zones on which an application is allowed to operate, see the section “Firewalld Optional Configuration” in this guide.
- **SELinux/seten force**—Provides an enhanced level of control over the files, processes, and users of the Operating System. For more information on the SELinux/seten force, see [http://docs.oracle.com/cd/E52668\\_01/E54669/E54669.pdf](http://docs.oracle.com/cd/E52668_01/E54669/E54669.pdf), section 26.2.

### Creating and Using a Non-Root User Account

Oracle strongly recommends using a non-root account for logins to setup, configure, and administer your ISR systems. Instead, create a normal user account in the 'isr' group.

To create a new user in the 'isr' group:

1. Add the new user by executing the following command:

```
[root@localhost ~]# useradd -g 9001 <username>
```

2. Set the user's password by executing the following command:

```
[root@localhost ~]# passwd <password>
```

- Grant the user sudo permissions by adding them to the wheel group:

```
[root@localhost ~]# usermod -aG wheel <username>
```

- Verify you can use the new user account and the sudo permissions are configured correctly.

```
# logout
Localhost login: isradm
Password: *****
[isradm@localhost ~]$ touch /var/log/messages
touch: cannot touch '/var/log/messages': Permission denied
[isradm@localhost ~]$ sudo touch /var/log/messages
[isradm@localhost ~]$
```

### File Permissions

Do not unnecessarily remove file permission restrictions on files and directories. By default, ISR files are set to the most restrictive possible settings required for the system to operate.

### Secure Passwords

Oracle recommends you use unique and complex passwords for ISR database accounts, as well as OS user accounts. The following Oracle MySQL password rules offer a good starting point:

- At least 8 characters long
- Contain at least 1 uppercase and 1 lowercase letter
- Contain at least 1 number
- Contain at least 1 special character

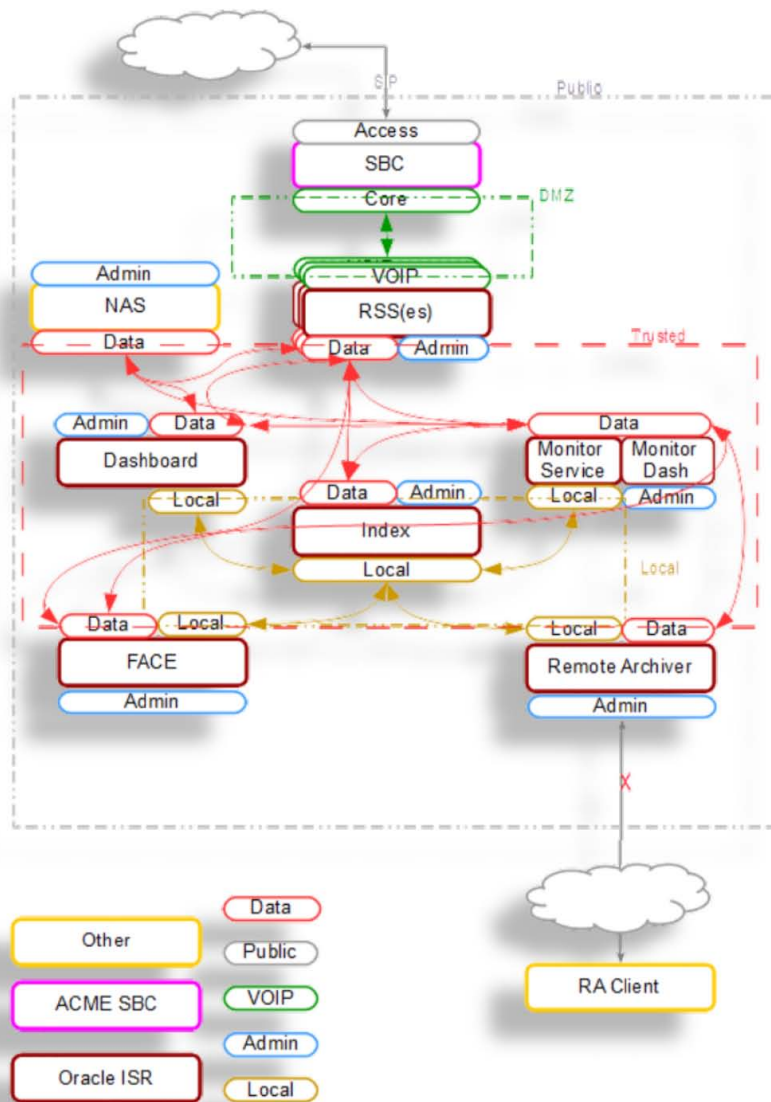
## Firewalld Configuration Overview

---

The firewalld service provides a strong line of defense in securing ISR Servers and Services. The firewall is, by default, enabled and configured to provide a secure operating environment for ISR. There are three default zones utilized by ISR services:

- **Public**—The default firewall zone interfacing to the most networks; This zone is utilized by the 'Admin' Ethernet interface. Services utilizing this zone include:
  - SSH
  - ISR Dashboard (HTTPS)
  - Remote Archival Web Service (HTTPS)
- **Trusted**—An internal firewall zone used by Data services such as:
  - MySQL (for non-VM RSS hosts)
  - ISR Web Services (HTTPS)
  - ISR Web Services (HTTP)
  - VoIP traffic (SIPREC/RTP)
- **Internal**—An internal firewall zone used by ISR VMs for communication. Services include:
  - MySQL





## ISR Firewall Configuration

By default, ISR provides a secure default firewall configuration which should not require end user changes. However, it may be necessary to modify these settings to disable unnecessary ISR services, or to allow communication with third party services. To help ensure the security of your systems, it is recommended that you do not disable the firewall.

- Service Configuration Files—ISR provides firewall zone configuration files, found in the `/opt/isr/security/firewalld/services/` directory. These files outline the services and ports utilized by the particular ISR service and configure the firewalld service to allow these communications.
- Interface/Zone Settings—ISR configures the firewall based on the “ISR Network Interface Mapping” performed during initial configuration.
- Service/Zone Settings—ISR comes preconfigured to allow the ISR Services to be run only on specified zones.

### Modifying ISR Firewall Configuration

By default, the firewall is configured upon installation to allow all services to communicate on specified interfaces within the firewall zones. However, you may need to move a service to an additional zone, or remove an extraneous firewall service from a particular zone.

Common changes include:

- Adding the ISR Dashboard service to the public zone if it must be reachable from external addresses. This can be done by entering the following commands on the ISR Dashboard host:

```
$ sudo firewall-cmd --zone=public --add-service dashboard
$ sudo firewall-cmd --zone=public --add-service dashboard --permanent
```

Similarly, it can be removed from the internal zone:

```
$ sudo firewall-cmd --zone=internal --remove-service dashboard
$ sudo firewall-cmd --zone=internal --remove-service dashboard --permanent
```

- Disabling unused components such as the ISR converter service.

```
$ sudo firewall-cmd --zone=data --remove-service converter
$ sudo firewall-cmd --zone=data --remove-service converter --permanent
```

- Adding the Remote Archival service to the public zone if it must be reachable from external addresses. This can be done by entering the following commands on the ISR Remote Archival host:

```
$ sudo firewall-cmd --zone=public --add-service raws
$ sudo firewall-cmd --zone=public --add-service raws --permanent
```

Similarly, it can be removed from the internal zone:


```
$ sudo firewall-cmd --zone=internal --remove-service raws
$ sudo firewall-cmd --zone=internal --remove-service raws --permanent
```

### ISR Port Usage

The ISR Platform utilizes the following ports, which are available on the networks displayed in the last column for each component host shown in the following table:

Component	Port	Description	Notes	Networks
All ISR Component Hosts	123	NTP		Admin
RSS	22*	SSH	SSL	Admin
	5060	SIP Listen Port (Recorder)		VoIP
	8080	HTTP Webserver		Data
	8443	Secure HTTP Webserver		Data
	8886	Archiver XMLRPC Listen		Data
	8887	API XMLRPC Listen		Data
	8888	Recorder XMLRPC Listen		Data
	8889	Converter XMLRPC Listen		Data
	9998	REST API Listen Port (Recorder)	SSL	Data
	9999	REST API Listen Port (Converter)	SSL	Data
22000-46000	RTP		VoIP	

Component	Port	Description	Notes	Networks
Index	22*	SSH	SSL	Admin
	3306	MySQL		Local, Data
Dashboard	22*	SSH	SSL	Admin
	80	HTTP Webserver	Disabled/optional	Admin/External
	443	Secure HTTP Webserver	SSL	Admin/External
FACE	22*	SSH	SSL	Admin
	8080	Web Service Port	Disabled/optional	Data
	8443	Web Service Port	SSL	Data
RAWS	22*	SSH	SSL	Admin
	8080	Web Service Port	Disabled/optional	Data
	8443	Web Service Port	SSL	Data

 **Note:** The ISR does not use port 22 within its system, however, it is typically open in the firewall for administrative connectivity.

## ISR Certificate Files

Many ISR services are configured for more secure requests via HTTPS, including:

- ISR Dashboard
- Remote Archival Webservice
- ISR FACE
- RSS REST Webservice

To access these services, the clients you use will need either public keys or certificates, which are generated at installation time, or negotiated through a public key exchange. Public keys and certificates can be found in the following locations:

Component	Public Key Location	Description
RSS	/opt/isr/security/keys/rss_cert.pem	Certificate + Public Key for ISR components to connect to RSS REST service
Dashboard	/opt/isr/security/keys/puma.crt	Certificate file
FACE	/opt/isr/security/keys/face-public.key	Public key for FACE HTTPS clients
Remote Archiver	/opt/isr/security/keys/raws-public.key	Public key for RAWs HTTPS clients

## Signing Keys

Many ISR services utilize self-signed keys which are generated during installation. For better security, Oracle recommends that keys are signed by a Certificate Authority. You must generate a certificate signing request (CSR) and use it to request a signed certificate from a CA. For java applications' keys (such as FACE and RAWs), you can generate a CSR via the `keytool -certreq -alias <your_alias> -keyalg RSA -file <your_domain>.csr -keystore <your_keystore>` command. For example:

## ISR Security Overview

---

```
keytool -certreq -alias ocisr -keyalg RSA -file ocisr.oracle.com.csr -
keystore /opt/isr/security/keys/tomcat.keystore
```

For the ISR Dashboard certificate, use the following open SSL command `openssl req -new -sha256 -key <your_key_file_name> -out <your_domain>.csr`. For example:

```
/usr/bin/openssl req -sha256 -key$key_loc/rss_cert.pem -out
ocisr.oracle.com.csr
```

The RSS certificate is for internal use only within the ISR lab and does not require a signed certificate.

## Configuring Reduced Security

---

The ISR's FACE functionality, Dashboard, and Remote Archival Webservice may all be run with reduced security. This section describes how to use the `configCis.sh` script to loosen security on these components.

### Configuring FACE Reduced Security

The ISR's FACE functionality may be run with reduced security. You can use the `configCis.sh` script to loosen security settings on the FACE host.

1. To disable HTTPS in FACE, run the `configCis.sh` script and select HTTP for FACE.

```
[root@face ~]# configCis.sh
-----
Please select from the following menu:
-----

s) Show the current configuration
m) Modify the current configuration
i) Add/modify a second network interface
f) Set face default configuration in DB
q) Quit

Choice: f

WARNING, this action will reset the FACE to its default configuration.
** All customization of FACE or EEN configured will be lost.

Continue? (yes|no) [yes] yes
You have been warned.

Enter Face Host IP: [] 1.2.3.4
Protocol to use for FACE connections? (http|https) [https] http

FACE connection protocol set to http
Enter ObserveIT Server IP: [] 2.3.4.5
Protocol to use for ObserveIT Server connections? (http|https) [https] https
ObserveIT connection protocol set to https
Attempting to restore backup SQL
Backing up FACE Config (to /opt/isr/faceSetupTemplate.sql.bak) .
Updating FACE IP in SQL Script.
Updating FACE HTTP/S in SQL Script.
Updating ObserveIT IP in SQL Script.
```

2. Change the ObserveIT web service configuration in ISR to HTTP from HTTPS if you want to use reduced security configuration of the ObserveIT web service. Run the `configCis.sh` script and choose **http** as the protocol for ObserveIT Server connections in the **f) Set face default configuration in the DB** section.

```
[root@face ~]# configCis.sh
-----
Please select from the following menu:
-----
```

```
s) Show the current configuration
m) Modify the current configuration
i) Add/modify a second network interface
f) Set face default configuration in DB
q) Quit
```

Choice: f

```
WARNING, this action will reset the FACE to its default configuration.
** All customization of FACE or EEN configured will be lost.
```

```
Continue? (yes|no) [yes] yes
You have been warned.
```

```
Enter Face Host IP: [] 1.2.3.4
Protocol to use for FACE connections? (http|https) [https]
```

```
Updating JBoss config for https
/opt/jboss/standalone/configuration/standalone.xml
```

```
Enter keystore password:
FACE connection protocol set to https
Enter ObserveIT Server IP: [] 2.3.4.5
Protocol to use for ObserveIT Server connections? (http|https) [https] http
ObserveIT connection protocol set to http
Attempting to restore backup SQL
Backing up FACE Config (to /opt/isr/faceSetupTemplate.sql.bak).
Updating FACE IP in SQL Script.
Updating FACE HTTP/S in SQL Script.
Updating ObserveIT IP in SQL Script.
```

This restarts the JBoss process, which is required after you change the ObserveIT HTTP connection configuration.

