Oracle® Communications Design Studio

Security Guide

Release 7.4.2
F30777-01
November 2020

Oracle Communications Design Studio Security Guide, Release 7.4.2

F30777-01

Contents

A Secure Deployment Checklist

Preface

This guide provides guidelines and recommendations for setting up Oracle Communications Design Studio in a secure configuration.

Audience

This guide is intended for system administrators, database administrators, developers, and integrators, who work with Design Studio.

Related Documents

For more information, see the following documents in the Design Studio documentation set:

- *Design Studio Installation Guide*: Describes the requirements and procedures for installing Design Studio.
- *Design Studio System Administrator's Guide*: Describes information about administering Design Studio. This guide includes information about configuring deployment settings for test environments, backing up and restoring Design Studio data, and automating builds.
- *Design Studio Concepts*: Explains how to use Design Studio to manage and configure data for use across Oracle Communications service fulfillment products. This guide provides a conceptual understanding of Design Studio.
- *Design Studio Developer's Guide*: Provides an overview of Design Studio platform tools, and information about working with design patterns, externally created schemas, and source control. Finally, it provides information about deploying to production environments.
- Design Studio Help: Provides step-by-step instructions for tasks you perform in Design Studio.

See the following books for more information about security:

- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*: Describes how to secure a WebLogic Server production environment.
- *Oracle Application Server Security Guide*: Describes basic web security concepts and describes the Oracle Application Server security framework and how to use it.
- *Oracle Application Server Administrator's Guide*: Describes how to manage Oracle Application Server, including how to start and stop the Oracle Application Server, how to reconfigure components, and how to back up and recover the Oracle Application Server.

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 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

Design Studio Security Overview

This chapter provides an overview of Oracle Communications Design Studio security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up-to-date.** Upgrade to the latest Design Studio product release and apply all appropriate patches.
- **Limit privileges.** Give users only as much access as necessary to perform their work. Review user privileges periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish access and frequency rules for system components and monitor those components.
- **Install software securely.** Use firewalls, secure protocols such as SSL, and secure passwords.
- **Learn and use the Design Studio security features.** Enforce user authorization, establish desktop lock policies, and employ source control.
- **Use secure development practices.** Leverage Design Studio security functionality.
- **Stay informed.** Read all security alerts and promptly install all security patches. See "Critical Patch Updates and Security Alerts" here:

  http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Design Studio Security

Security for Design Studio focuses on a few key areas:

- Limiting use of Design Studio to authorized users
- Controlling access to cartridge management functions
- Protecting cartridge designs
- Preventing run-time cartridge archive tampering

The remaining sections in this document address each of these security considerations.

2
Performing a Secure Installation

This chapter presents planning information for your Oracle Communications Design Studio installation, and describes recommended deployment topologies that enhance security.

For information about installing Design Studio, see *Design Studio Installation Guide*.

Understanding the Design Studio Environment

When planning your Design Studio implementation, consider the following:

- **Which resources need to be protected?**

  You need to protect customer data, such as credit card numbers, internal data, such as proprietary source code, and system components from external attacks and intentional overloads. Run-time archives and projects they are derived from need to be protected to prevent tampering and exposure of internal mechanics. Application components should have restricted access to help prevent creation of viral cartridges.

- **Who are you protecting data from?**

  You need to protect subscriber data from other subscribers and you need to analyze your workflows to determine who in your organization needs access to subscriber data. Design information needs to be protected from potential hackers since it could provide critical details enabling an attack. Access to data should be limited for run-time and design-time information. For example, can a system administrator manage your system components without needing to access the system data?

- **What happens if protections on strategic resources fail?**

  In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Design Studio.

Figure 2-1 Recommended Deployment Configuration

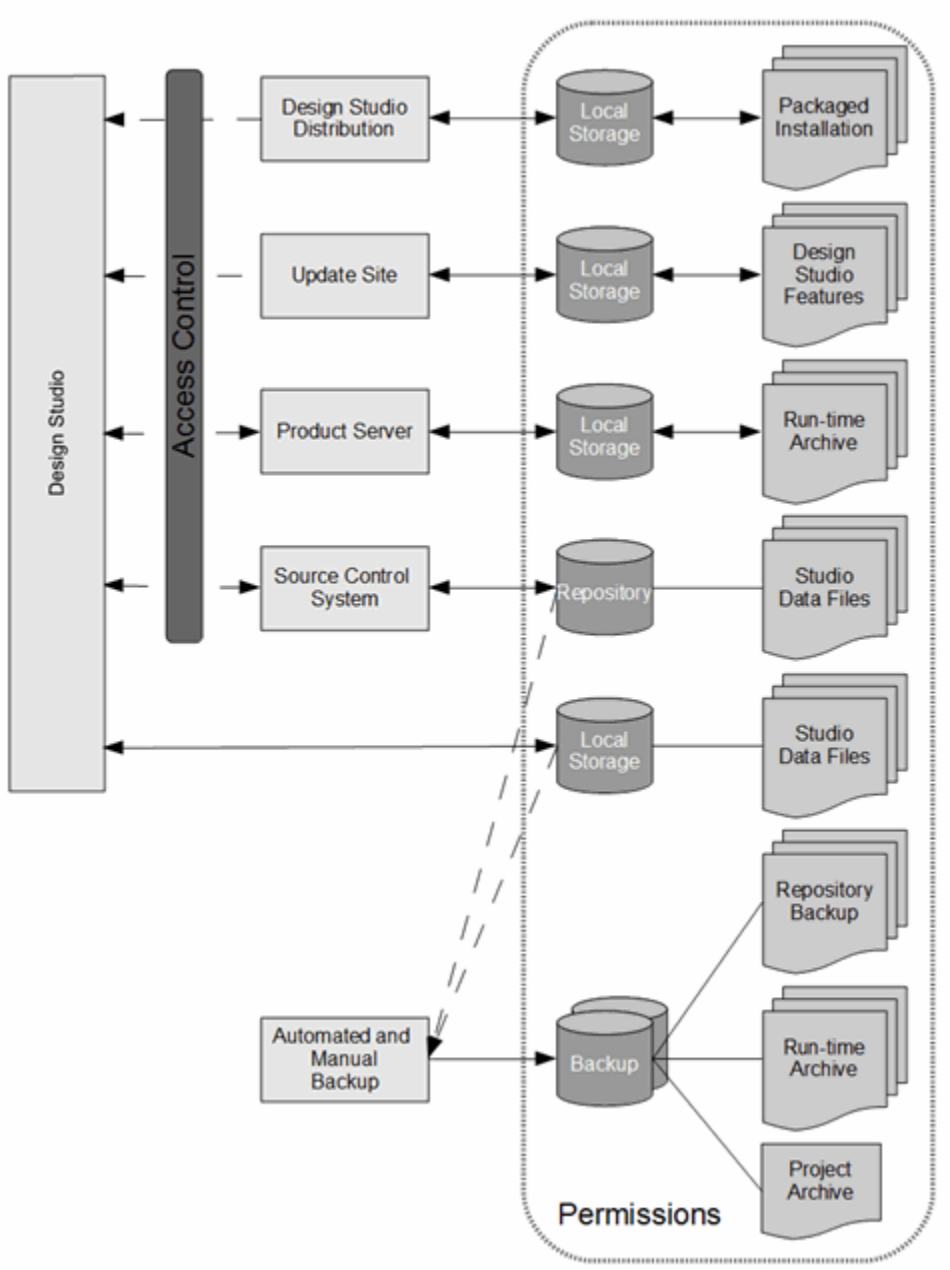

Table 2-1 Design Studio Deployment Recommendations

Component	Recommendation
Design Studio	Limit application and project file permissions to the user. Enable user authentication and desktop locking.
Design Studio Distribution	When distributing Design Studio to users as a pre-packaged archive, use web/FTP server with access control. Limit distribution files access to the web/FTP server for download only.

Table 2-1 (Cont.) Design Studio Deployment Recommendations

Component	Recommendation
Update Site	Use web/FTP server with access control. Limit update site file access to the web/FTP server for download only.
Product Server	Use Cartridge Management web service access control with limited functions.
Source Control System	Enable user authentication. Limit repository file access to the source control system.
Automated/Manual Backup	Control backup utility access. Limit backup file permissions to backup administrators only.

Employ access control to components to limit use to privileged users. Configure Design Studio files and folders to provide limited permissions to the user or associated component only.

Additionally, carefully consider security requirements for the resources that you deploy to production servers. These run-time archives contain code and logic which execute on production servers. Use source control and access control on any run-time archives (and the cartridge projects which produce them) to protect against cartridge tampering.

Finally, protect against the misuse of cartridge management actions. Unauthorized development of viral cartridges and cartridge deployment, for example, can enable various forms of attack such as denial of service or theft of secure data. Protect against this type of incident by limiting access to the Design Studio application and to the cartridge management functions.

Operating System Security

See the following documents:

- Windows Security Checklist at microsoft.com
- Oracle Solaris Security for System Administrators
- Guide to the Secure Configuration of Red Hat Enterprise Linux 5
- Hardening Tips for the Red Hat Enterprise Linux 5

Cartridge Management Security

Design Studio interacts with product server components for cartridge management functions. Secure these interactions using secure connections. Oracle recommends that you install the product server components with secure connectivity enabled.

Enabling Secure Connectivity

Content contained in cartridge management messaging may include sensitive information. You can use Secure Sockets Layer (SSL) connections to protect against snooping during transport. Employ secure connection configuration for all interactions from Design Studio to the product server components.

See *Design Studio System Administrator's Guide* for more information about enabling SSL connections.

Ensure that you make the SSL keys available to Design Studio. The key store must include keys for any environment connection using SSL.

See "Studio Environment Editor Tab" in Design Studio Help.

See *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

Protecting Deployment Functions

The cartridge management functions should be configured to require user specific authentication credentials. The credentials should allow the minimum privileges necessary to enable the cartridge management functions.

Deployment scripts used for automated deployment should be protected from unauthorized use or tampering. The scripts and ability to execute them need to be restricted to authorized users and have permissions restricted based on the user role.

See Oracle Communications product installation documentation on the Cartridge Management web service for more information.

Secure Design Studio Installation

Design Studio installation includes a number of options for making Design Studio application components secure.

Consider each of the following sections for applicability to your Design Studio installations.

Secure Design Studio Update Site

If providing users access to the Design Studio update site (rather than distributing a pre-packaged installation), use web or FTP access with user access controls. Requiring individual user authorization limits Design Studio feature access to a limited set of users. See authentication configuration instructions for the web server or FTP server in use.

Secure Packaged Installation

Use a secure web server or FTP server when publishing a pre-packaged Design Studio installation. To help prevent development of viral cartridges or tampering of cartridges, restrict the Design Studio application to a limited set of users.

Following extraction, users should ensure that the Design Studio files and folders have full privileges for the user and no privileges for groups or other users.

See operating system-specific documentation for configuring file and directory access privileges.

SSL Key Store

SSL connections are required to secure connectivity to the product servers when executing cartridge management functions. The SSL keys must be made available to each Design Studio installation using a key store. To ensure a secure installation, configure the keys and ensure that the key store is configured with strict file access privileges, readable to Design Studio users only.

3
Implementing Design Studio Security

This chapter presents security mechanisms related to use of Oracle Communications Design Studio.

User Authentication

Design Studio interacts with product server components for cartridge management functions. These functions require user authorization. Design Studio prompts users for credentials, as required. However, this information is not persisted and users are occasionally prompted again. For usability purposes, users are not prompted on every interaction and may not be prompted until after the application is restarted. Use a desktop lock policy to protect against unauthorized usage of cartridge management functions when users are away from their desks.

All Design Studio users should have personal access credentials for cartridge management functions. The credentials should be kept private and never be shared.

See *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

Design Studio Source Control

Cartridge designs may include information beneficial to a product server attack. It is important to limit access to Design Studio projects.

Employ a source control system to protect cartridge designs and enable authentication and access controls of the source control system.

Restrict access to cartridge designs to a restricted set of developers. Each developer should use personal authentication credentials when interacting with the source control system. Track all changes committed to the source control repository on a per-user basis to discourage inclusion of viral content in the cartridge implementation. Additionally, Oracle recommends that all submissions are reviewed by a second party.

See documentation for your source control system for details on configuring authentication and access control functionality.

System Security Maintenance

Administrators should perform regular activities and additional measures to further secure the system. To help maintain a secure system, administrators should:

- Employ password policies for complexity, aging, and failed login attempts
- Review access and activity logs for suspicious activity
- Promptly maintain and periodically review user access and permissions
- Regularly check for component updates

- Review cartridge designs for insecure sensitive information
- Validate systems are installed with the highest reasonable security settings

Regular assessment should be done for each component of the system, including archived components, source control interactions, and cartridge management functions. Administrators should be reviewing who is accessing what parts of the system and the validity of such actions.

4
Security Considerations for Developers

This chapter presents planning information for your Oracle Communications Design Studio cartridge development and describes recommended design practices that enhance security.

Secure Variable Values

Define all environment-specific content with model variables. Do not include sensitive model values directly in the design model. Instead, use cartridge model variables as place-holders.

Ensure flag indicating sensitive model and cartridge management variables is used as appropriate (for example, user IDs and passwords). Sensitive variables are obfuscated in the persisted model and redacted in the user interface to protect the actual value.

Use the sensitive flag and SSL connections to secure the configured values.

See "Cartridge Management Security" and Design Studio Help for more information about model variables.

Secure Documentation

The content contained in the cartridge documentation should be considered confidential. This documentation may be exported to a stand-alone document. Access to the exported documentation should employ suitable controls to guard the content. Oracle recommends that highly sensitive information not be placed into the cartridge documentation.

Secure Automation Tasks

The Oracle Communications Order and Service Management (OSM) automated and activation tasks send requests to Oracle Communications ASAP using web services. Web services users are created in a WebLogic credential store by using the OSM credential store administration tool. The OSM automated tasks and activation tasks require the credential map and key.

The credential map and key are specified in the OSM activation task details. To protect the map and key, cartridge variables should be used. The corresponding cartridge variables should be defined with the sensitive data flag enabled.

Custom automation tasks using the automation Java API should use obfuscation for protecting the map and key.

See *Order and Service Management System Administrator's Guide* for credential store information and *ASAP Server Configuration Guide* for web service user configuration details.

Secure Reporting

Ensure that you protect model data and report input parameters by using cartridge variables when working with sensitive data. Design Studio reports display cartridge variables in the place of data values when variables are used in report designs.

During report generation, Design Studio does not decode any obfuscated data. Report designers should use the security features available in BIRT to ensure that sensitive input data is not displayed to users.

A

Secure Deployment Checklist

- Are Oracle Communications Design Studio installation components accessible only to users?
- Have model variables been used in cartridge designs?
- Are sensitive variables marked sensitive?
- Is sensitive information excluded from the Design Studio documentation?
- Has the Cartridge Management web service been configured to use SSL?
- Is a source control system in place?
- Does the source control system restrict access to specific users?
- Is user-specific source control change tracking enabled?
- Do user-accessible update sites require user-specific authentication?
- Do the following file and folder permissions restrict access to authorized users or specific components?
  - Package installation
  - Design Studio features
  - Run-time cartridge archives
  - Source control repository
  - Design Studio project data files