Oracle
Primavera
Gateway Administration Guide

Version 20
October 2021

ORACLE®

Contents

About the Gateway Application Administration Guide

Primavera Gateway facilitates the sharing and synchronization of project and resource data between Primavera applications and other enterprise applications.

This guide provides is intended to be used by people who have administrator access to Gateway.

Within our documentation, some content might be specific for cloud deployments while other content is relevant for on-premises deployments. Any content that applies to only one of these deployments is labeled accordingly.

Managing Personal Information

This guide describes how to configure and manage personal information (PI) in Primavera Gateway.

Gateway administrators and Gateway developers must review this guide.

In This Section

About Consent Notices

Consent notices inform users how personal information (PI) is collected, processed, stored, and transmitted, along with details related to applicable regulations and policies. Consent notices also alert users that the action they are taking may risk exposing PI. Primavera Gateway helps you to ensure that you have requested the appropriate consent to collect, process, store, and transmit the PI your organization holds as part of Primavera Gateway data.

> **Note**: Consent notices are switched *off* by default in Primavera Gateway.

Consent notices must:

▶ be written in clear language which is easy to understand.
▶ provide the right level of detail.
▶ identify the purpose and legal basis for your collection, processing, storage, and transmission of PI.
▶ identify whether data will be transferred to named third parties.
▶ identify PI categories and list the data which will be collected, processed, stored, and transmitted.

About Personal Information

Personal information (PI) is any piece of data which can be used on its own or with other information to identify, contact, or locate an individual or identify an individual in context. This information is not limited to a person's name, address, and contact details. For example, a person's IP address, phone IMEI number, gender, and location at a particular time could all be personal information. Depending on local data protection laws, organizations may be responsible for ensuring the privacy of PI wherever it is stored, including in backups, locally stored downloads, and data stored in development environments.

Cookies Policy in Primavera Gateway

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

Your Responsibilities

Information security and privacy laws can carry heavy penalties and fines for organizations which do not adequately protect PI they gather and store. If these laws apply to your organization, it is your responsibility to configure consent notices before they are required. You should work with your data security and legal teams to determine the wording of the consent notices you will configure in Primavera Gateway.

If a consent notice is declined, it is your responsibility to take any necessary action. For example, you may be required to ensure that the data is not stored or shared.

Personal Information (PI) Data in Primavera Gateway

PI may be visible in multiple areas of Primavera Gateway, including but not limited to user administration, resource and role administration, assignments, work products and documents, reports, issues, risks, user defined fields, codes, and timesheets.

PI may be at risk of exposure in multiple areas of Primavera Gateway, including but not limited to integrating data between applications, downloaded logs, web services, and API.

As part of Primavera Gateway Cloud Services, you may be using Oracle Identity Cloud Service ("Oracle IDCS") to manage your user access and entitlements across a number of cloud and on-premises applications and services. If you are using or accessing Oracle IDCS, you are responsible for deleting your details and data from the Oracle IDCS environment. You are responsible for retrieving your content in Oracle IDCS during your applicable services period.

Ensuring Privacy of Data Collection

Primavera Gateway only collects credentials to setup deployment connections to applications for integration. Integration data such as project data and resource data is also stored in Gateway database. Ensure users with appropriate roles have controlled access to data.

Limiting Granular Access to Data

Integration data originates from source applications such as P6 EPPM, Primavera Cloud, and Unifier.

Ensuring Data Purging and Data Deletion

Primavera Gateway provides user configurable option to automatically delete application data at regular intervals. Ensure you set this up in Gateway settings. Ensure data is purged either manually or scheduled for purging.

Ensuring Privacy of Data Portability

Primavera Gateway provides options to export and import data between source and destination applications. Ensure your users have the appropriate role-based rights and access privileges to perform these tasks.

Ensuring Privacy of End User Access

Primavera Gateway collects only credentials for connecting to different applications for integration. Ensure users are set up with appropriate role and access privileges to access data. Gateway does not store any other user information.

Ensuring Right to Erasure

Primavera Gateway provides options to delete connection credentials and integration data. Ensure users are set up with the correct roles to perform these tasks. Also, ensure user credentials are securely and permanently deleted upon request.

Ensuring Availability

Ensure you request a backup of Primavera Gateway data regularly.

Ensuring Secure Encryption

Primavera Gateway supports HTTPS protocol. Ensure you configure Gateway with HTTPS for data encryption in transition and also use Total Data encryption for the database.

Ensuring Secure Logging

Primavera Gateway supports secure logging for cloud and on-premises customers. Access to synchronization job logs is controlled by the role and access privileges assigned to a user. Ensure users are set up with correct roles and access privileges.

Configuring Consent Notices for Primavera Gateway

To configure consent notices for Primavera Gateway:

1) Sign in to Primavera Gateway as an administrator or developer.
2) Select ✕ and then select **Settings**.
3) In the **General** tab, select **Enable Configurable Consent Forms**.

4) In the sidebar, select **Configuration**.

5) Select the **Consent Forms** tab.

6) In the **Name** field, select a consent form, and then select ✏ **Edit...**.

> **Note**: The **Cookies Consent** is automatically enabled when any consent form is enabled.

7) The **Edit <Consent Form Name>** dialog box displays. For example, *Edit Login Consent Form* displays.

8) Select **Enable Consent Message** to allow the notice to be shown to users of the selected consent form.

   For Gateway administrators, enable *all* consent forms.

   For Gateway administrators with no data access and Gateway developers, enable all consent forms except **Download Consent**.

   For Gateway users, enable **Login Consent**, and **Download Consent**.

   For Gateway users with no data access, enable **Login Consent** only.

9) Enter and format the text for the consent notice in the **Consent Message** area.

> **Note**: Work with your data security and legal teams to determine the wording of the consent notice.

10) Select **Save**.

11) Continue to configure consent notices for other consent forms.

Auditing Consent Forms for Primavera Gateway

You can see the status of consent acceptance for users. You can also reset consent acceptance for all users if there is a need to regain consent after a consent notice has changed.

To audit consent status for Primavera Gateway:

1) In the sidebar, select **Configuration**.

2) Select the **Consent Forms** tab.

3) In the **Name** column of the top section, select a consent form.

4) Choose any of the following actions in the bottom section:

   ‣ To see the user consent status for the selected consent form, view the **Acceptance Date** and **Reject Date**.

   ‣ Select **Delete** to ensure the consent notice is displayed again for *all* users the next time they access an area of the software.

   A warning message displays, *Deleting all user acceptances to this consent form will require the users to re-accept again prior to accessing the specified area.*

   ‣ Select 🔍 **Search** to locate a user by their user name and view their consent status.

Security Considerations

In This Section

Introduction

For any company that deals with sensitive data, keeping it secure is crucial to success. While hosting Primavera Gateway data on Oracle Cloud provides security measures, it can't do everything. For example, it can't prevent phishing attempts or other attacks that exploit gaps in its users' security awareness. That's why it's important for everyone who works with Primavera Gateway to understand what they can do to keep data secure.

Who this guide is for

Security is everyone's business. This guide is for anyone who uses, manages, or is just interested in Primavera Gateway. If you're a security expert or administrator, this is a good place to start. It should help you see the big security picture and understand the most important guidelines related to security in Primavera Gateway.

Some Security Basics

We'll use the term **administrator** to refer to anyone who's responsible for managing a company's data and who can access that data. For our purposes, administrators includes a wide variety of IT professionals, from those who define roles in the Primavera Gateway application to those who manage company servers.

An **end user** is anyone who uses Primavera Gateway to do their job. This includes developers, adminsistrators, users, and everyone else who logs into Primavera Gateway from an office or jobsite to get their work done.

Administrators should...

▶ **Set up Single Sign-On (SSO) and enable multi-factor authentication** to minimize the number of passwords that users have to remember and to consolidate risk.
▶ **Educate users** on how they can avoid unwittingly helping hackers. One of the best ways application administrators and security advocates can help users is by helping them to prevent security breaches.

▶ **Use a VPN** to encrypt data being sent over the internet.

▶ **Stay up-to-date** about security trends and best practices.

End users should...

▶ **Follow security guidelines** created by their companies and the administrators of any network applications they use.

▶ **Use strong passwords**. The more random-looking the better, and avoid reusing passwords.

▶ **Learn to recognize phishing**. Phishing is when someone disguises an email or some other transmission as a legitimate message in an attempt to get a user to reveal sensitive information. For example, a hacker may send you an email disguised to look like an email from your employer requesting login information. These attacks are becoming more sophisticated, but you can still protect yourself by making sure any emails you receive or websites you visit are legitimate before using them to share sensitive information.

Authentication: How Users Sign On

Authentication refers to the way users sign on. If Primavera Cloud is configured to use Oracle Identity Cloud Service (IDCS), administrators can—and should—implement Single Sign-On (SSO). SSO reduces the number of passwords users have to remember. It can also be used to enable multi-factor login, which is when users are asked to provide some verification in addition to their passwords, like a code that they receive via text or email.

If your Primavera Gateway Cloud environment is provisioned in Oracle Cloud Infrastructure (OCI), it comes with IDCS.

See Oracle Identity Cloud Service https://docs.oracle.com/en/cloud/paas/identity-cloud/index.html in the Oracle Help Center for more information.

Authorization: What Users can Access

Authorization refers to what users can access. Primavera Gateway uses Groups and Roles to restrict access to the application.

Groups: Security groups make it easier for administrators to assign permission sets to multiple users at the same time. In Gateway, administrators can create security groups with permission sets, and then assign users to these groups.

Roles: User roles in Primavera Gateway can be defined with or without data access. Users can be assigned any of the following roles in Primavera Gateway:

▶ **Admin role**: This is a super user role that enables the user to perform all actions in the Primavera Gateway application.

▶ **Admin role with no data access**: This role is identical to the Admin role with the following exception: These users cannot view the details of the data passed in each flow step, or download the details of the log files when monitoring a synchronization job. However, they can view errors and warning messages associated with each step.

▶ **Developer role**: This role enables the user to create data mappings and flow types. Users have access to the data dictionary, workflows, and configuration global settings.

▶ **User role**: This role enables the user to synchronize data between two systems and monitor the results.

▶ **User role with no data access**: This role is identical to the User role with the following exception: These users cannot view the details of the data passed in each flow step or download the details of the log files when monitoring a synchronization job. However, they can view errors and warning messages associated with each step.

End Point Security

From laptops to cellphones, organizations have to keep track of data on more devices than ever, and more devices means more risk. That's why its important to implement Enterprise Mobility Management (EMM) tools and policies.

Inherent Risks and Practical Policies

No automated security system or protocol can make a system fully secure if those with legitimate access exploit it for illegitimate purposes or if a device falls into the wrong hands. Here are some general "common sense" guidelines you should follow when it comes to endpoint security:

Grant security permission conservatively. Don't give everyone permission to everything just to avoid perceived complexity. Remember, one breach can be many times more costly and time consuming than setting and following standard security protocols.

Keep up with organizational changes. If a user no longer needs access to a part of the app, for whatever reason, update that user's permissions accordingly.

Privacy and Personal Information

Closely related to security are matters of privacy and personal information.

View the section *Managing Personal Information* in Primavera Gateway in this guide to learn about what information is collected and what you can do to monitor personal information in Primavera Gateway.

Integration with Other Applications

The ability to connect and exchange information with other apps is powerful, but it also presents some potential security issues that administrators must manage. It is important to understand which data flows between applications to ensure compliance with policies and regulations related to security and privacy.

For more information on integration, refer to the *Setup Guide* or *Business Flow Designer Guide* corresponding to the applications you choose to integrate with using Primavera Gateway.

Security for Developers - API Security

With APIs, developers can use some of the data and functionality of Primavera Gateway outside of the limitations—and relative safety—of the Primavera Gateway environment. This opens many possibilities. But as with any situation where data can move in potentially unpredictable ways, it presents risk. That's why anyone who uses Primavera Gateway API should understand the security fundamentals provided in this section.

Refer to these sections and topics from the *Primavera Gateway REST API Guide*:

▸ Transport Level Security using HTTPS
▸ Application Level Security
▸ HTTP Basic Authentication and HTTPS (Traditional)
▸ Cookies

Establishing Security Contacts

While the apps used by your organization may have some security features of their own, most security issues ultimately come down to the people who use them. When your company establishes its security procedures, it's important to also establish in-house security experts to whom other members can turn when they have security questions. Security points of contact should be continuously learning about security trends and how they can educate users to keep their data and network secure. Security contacts should also routinely update and maintain protocols that suit the security needs of their organizations.

Administering Gateway

Primavera Gateway facilitates the sharing and synchronization of project and resource data between Primavera applications and other enterprise applications.

This chapter provides information and procedures for:

▸ Assigning application access for Primavera Gateway users
▸ P6 EPPM and Primavera Unifier integrations
▸ P6 EPPM and Oracle Primavera Cloud integrations
▸ Primavera Unifier and Oracle Primavera Cloud integrations
▸ Primavera Unifier and 0P_ProdName_OPP_Suite> integrations

In This Section

Assigning Application Access to Primavera Gateway (Cloud Only)

You can assign application access to Primavera Gateway in Primavera Administration. See the *Primavera Administration Identity Management Guide* for details on using Primavera Administration.

> **Note**: Users with application access to Primavera Gateway do not require application access to the source and destination applications in order to map or exchange data.
>
> If you want a Primavera Gateway user to access P6 EPPM applications or Primavera Unifier, assign access in Primavera Administration.
>
> If you want a Primavera Gateway user to access Oracle Primavera Cloud, assign access in the Administration app in Oracle Primavera Cloud. See the *Primavera Cloud Application Administration Guide* for details.

To assign application access to Primavera Gateway:

1) Log in to Primavera Administration.
2) Add or modify a user account.
3) Assign application access for that user account to one of the following access types:
    ▸ Primavera Gateway Production Administrator
    ▸ Primavera Gateway Production Developer
    ▸ Primavera Gateway Production User
    ▸ Primavera Gateway Production Administrator (Limited Access)

▸ Primavera Gateway Production User (Limited Access)

> **Note**: Limited access types have no access to view actual data passed in Primavera Gateway.

Setting Up Integrations Using Primavera Gateway

Data can be exchanged between the applications listed below using Primavera Gateway. In addition, applications such as Oracle Primavera Cloud, <)0P_ProdName_Unifier>, and P6 EPPM allow you to connect with Primavera Gateway from within their native user interfaces.

You can integrate the following applications using Primavera Gateway:

▸ Oracle Primavera Cloud and Primavera Unifier
▸ Oracle Primavera Cloud and P6 EPPM
▸ Primavera Unifier and P6 EPPM
▸ Primavera Unifier and File Provider
▸ Oracle Primavera Cloud and File Provider
▸ P6 EPPM and File Provider

See the corresponding *Setup Guide* in the Primavera Gateway documentation library for details on setting up any of these integrations.

Business Objects

The *Gateway Providers Data Dictionary* provides a comprehensive listing of all of business objects and associated fields that are available in Oracle Primavera Cloud, P6 EPPM, and Primavera Unifier. Review the list of supported business objects in each application to determine the data that needs to be supported for integration in Primavera Gateway.

To view these business objects in the Primavera Gateway user interface, sign in to Primavera Gateway and select the **Data Dictionary** menu.

To view these business objects in the documentation library, go to the Primavera Gateway documentation and expand the **Using** section.

Copyright

Oracle Primavera Gateway Administration Guide

Copyright © 2021, Oracle and/or its affiliates.
Oracle and Java 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, 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 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 failsafe, 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.

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