ORACLE
Primavera

Gateway Administration Guide
Version 18

October 2021

Contents

About the Gateway Application Administration Guide 5

Managing Personally Identifiable Information 7

About Consent Notices 7

About Personally Identifiable Information 7

Cookies Policy in Primavera Gateway 8

Your Responsibilities 8

PII Data in Primavera Gateway 8

Ensuring Privacy of Data Collection 8

Limiting Granular Access to Data 8

Ensuring Data Purging and Data Deletion 9

Ensuring Privacy of Data Portability 9

Ensuring Privacy of End User Access 9

Ensuring Right to Erasure 9

Ensuring Availability 9

Ensuring Secure Encryption 9

Ensuring Secure Logging 9

Configuring Consent Notices for Primavera Gateway 9

Auditing Consent Notices for Primavera Gateway 10

Administering Gateway (Cloud Only) 11

Assigning Application Access to Primavera Gateway (Cloud Only) 11

Setting Up Integrations Using Primavera Gateway (Cloud Only) 12

Business Objects (Cloud Only) 13

Legal Notices 14

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 Personally Identifiable Information

This guide describes how to configure and manage personally identifiable information (PII) in Primavera Gateway.

Gateway administrators and Gateway developers must review this guide.

In This Section

About Consent Notices 7
About Personally Identifiable Information 7
Cookies Policy in Primavera Gateway 8
Your Responsibilities 8

About Consent Notices

Consent notices inform users how personally identifiable information (PII) 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 PII. Primavera Gateway helps you to ensure that you have requested the appropriate consent to collect, process, store, and transmit the PII 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 PII.
- identify whether data will be transferred to named third parties.
- identify PII categories and list the data which will be collected, processed, stored, and transmitted.

About Personally Identifiable Information

Personally identifiable information (PII) 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 personally identifiable information. Depending on local data protection laws, organizations may be responsible for ensuring the privacy of PII wherever it is stored, including in backups, locally stored downloads, and data stored in development environments.

Cookies Policy in Primavera Gateway

Cookies are small text files that are placed on your computer, smartphone or other device when you access the internet. When using Primavera Gateway, the server may generate cookies and send them to the user's browser. The user's machine stores the cookies, either temporarily by the browser, or permanently until they expire or are removed manually.

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 PII 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.

PII Data in Primavera Gateway

PII 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.

PII 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, Prime, 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** column, 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 Notices 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.

Administering Gateway (Cloud Only)

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 Prime Projects integrations

In This Section

Assigning Application Access to Primavera Gateway (Cloud Only)..... 11
Setting Up Integrations Using Primavera Gateway (Cloud Only) 12
Business Objects (Cloud Only) 13

Assigning Application Access to Primavera Gateway (Cloud Only)

You can assign application access to Primavera Gateway in Cloud Administration. See the *Cloud Services Identity Management Administration Guide* for details on using Cloud 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 Cloud Administration. See the *Cloud Services Identity Management Administration Guide* for details.
>
> If you want a Primavera Gateway user to access Oracle Prime Projects, assign access in the Administration app in Oracle Prime Projects. See the *Prime Application Administration Guide* for details.

To assign application access to Primavera Gateway:

1) Log in to Cloud 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 (Cloud Only)

Data can be exchanged between the applications listed below using Primavera Gateway. In addition, applications such as Primavera 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:

- Primavera Unifier and P6 EPPM
- Oracle Prime Projects and P6 EPPM
- Primavera Unifier and File Provider in Primavera Gateway
- Oracle Prime Projects and File Provider in Primavera Gateway

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

Business Objects (Cloud Only)

The *Gateway Provider Reference Guide* provides a comprehensive listing of all of business objects and associated fields that are available in Oracle Prime Projects, 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, log 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 **User Content**.

Legal Notices

Oracle Primavera Gateway Administration Guide