Oracle Fusion Cloud Applications Suite

Administering Oracle Analytics Publisher in Oracle Transactional Business Intelligence

F41282-23
January 2026

Oracle Fusion Cloud Applications Suite Administering Oracle Analytics Publisher in Oracle Transactional Business Intelligence,

F41282-23

Contents

6 Secure Reports

7 Audit Data of Publisher Catalog Objects

8 Add Translations for the Catalog and Reports

9 Frequently Asked Questions for Publisher

Preface

Learn to administer Publisher for pixel-perfect reporting.

Topics:

Audience

This document is intended for system administrators who are responsible for configuring Publisher.

Related Resources

For a full list of guides, refer to the Books tab on Oracle Transactional Business Intelligence Help Center.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Videos and Images

Your company can use skins and styles to customize the look of the application, dashboards, reports, and other objects. It is possible that the videos and images included in the product documentation look different than the skins and styles your company uses.

Even if your skins and styles are different than those shown in the videos and images, the product behavior and techniques shown and demonstrated are the same.

1

Introduction to Publisher Administration

This topic describes the tasks required to administer Publisher.

Topics:

Introduction

You can author, manage, and deliver pixel-perfect reports such as operational reports, electronic funds transfer documents, government PDF forms, shipping labels, checks, sales and marketing letters.

The administrator sets up and maintains the following system components.

- Data source connections
- Report delivery destinations
- Runtime configuration settings

For other business roles, see the guides that are outlined in the table below for information about using the product.

Role	Sample Tasks	Guide
Data Model developer	Fetch and structure the data to use in reports	*Designing Pixel-Perfect Reports in Oracle Transactional Business Intelligence*
Report consumer	View reports Schedule report jobs Manage report jobs	*Using Oracle Analytics Publisher in Oracle Transactional Business Intelligence*
Report designer	Create report definitions Design layouts	*Designing Pixel-Perfect Reports in Oracle Transactional Business Intelligence*

About the Administration Page

Use the Publisher administration page to configure pixel-perfect reporting.

Navigate to the Administration Pages for Pixel-Perfect Reporting

Administrators set the options for Publisher reports through the administration pages for pixel-perfect reporting.

- On the Publisher Administration page, select the required option.

About the Data Source Connections

Publisher reports rely on XML data. Publisher supports retrieving data from a variety of data sources.

The following data sources connections must be first set up in Publisher through the administration page:

- JDBC and JNDI connections

  You can use the provisioned JDBC and JNDI connections. Only to create audit reports, you are allowed to create JNDI connections to the system-defined data sources to access the audit data source (AuditViewDB). JDBC connections to external databases aren't supported.
- Web Service connections
- HTTP XML connections
- Content Server connections

You can also take advantage of the following data sources:

- Oracle BI Analysis
- Oracle BI Server subject area

About Report Delivery Destinations

The Publisher delivery manager supports multiple delivery channels.

Supported delivery channels include:

- Printer
- Fax
- E-mail
- HTTP notification
- FTP
- Web Folder (or WebDAV)
- Content Server

About Setting Runtime Configuration Properties

Use the Runtime Configuration page to enable configuration settings for your system.

The properties include settings that do the following:

- Control the processing for different output types
- Tune for scalability and performance
- Define font mappings

2

Configure System Maintenance Properties

This topic describes how to configure the Publisher properties.

Topics:

About Scheduler Configuration

You can review the configuration of the scheduler in the System Maintenance page.

The Enterprise Scheduler Service (ESS) manages job requests. If you select Enable Public Output Option, the **Make Output Public** option is available for selection in the Schedule job page.

The **Threads Per JMS Processor** is preconfigured as per your system capacity. The **Threads Per JMS Processor** setting defines the maximum number of scheduled (offline) jobs that can be processed in parallel by the server.

Review Scheduler Diagnostics

The Scheduler diagnostics page provides the runtime status of the scheduler.

The Diagnostics page displays how many scheduled report requests have been received by the JMS queues, how many of them have failed and how many are still running. The JMS status can be viewed at the cluster-instance level enabling you to decide whether to add more instances to scale up by one or more of these JMS processors.

For example, if there're too many requests queued up for the e-mail processor in one instance, you can consider adding another instance and enabling it to handle e-mail processing. Similarly, if there're very large reports being processed and showing in the Report Process queue in running status, then you can add another instance to scale up the Report Process capability.

Also, the Scheduler Diagnostics page reflects the status of each component to show if any component is down. You can see the connection string or JNDI name to the database, which cluster instance associates to which managed server instance, Toplink connection pool configuration, and so on.

If an instance shows a failed status, then you can recover the instance and with the failover mechanism of the JMS set up in the cluster, no jobs submitted are lost. When the server

instance is brought back, it is immediately available in the cluster for service. The instance removal and addition reflects dynamically on the diagnostic page.

When an instance is added to the cluster, the Scheduler Diagnostics page immediately recognizes the new instance and displays the status of the new instances and all the threads running on that instance. This provides a powerful monitoring capability to the administrator to trace and resolve issues in any instance or any component of the scheduler.

The Scheduler Diagnostics page provides information on the following components:

- JMS
- Cluster
- Database

The JMS section provides information on the following:

- JMS Cluster Config: This section provides configuration information for JMS setup:
  - Provider type (Weblogic / ActiveMQ)
  - WebLogic version
  - WebLogic JNDI Factory
  - JNDI URL for JMS
  - Queue names
  - Temporary directory
- JMS Runtime: This provides runtime status of all JMS queues and topics.

The Cluster section provides details on the cluster instance. Use this information to understand the load on each processor.

The Database section provides information on these components.

- Database Config — Connection type, JNDI Name, or connection string
- Toplink Config — Connection pooling, logging level
- Database Schema

Set Report Viewer Properties

On the System Maintenance page, the administrator can set the report viewer properties on the Report Viewer Configuration tab.

If **Show Apply Button** is set to True, reports with parameter options display the **Apply** button in the report viewer. If you change the parameter values, click **Apply** to render the report with the new values.

If **Show Apply Button** is set to False, the report viewer doesn't display the **Apply** button. If you enter a new parameter value, Publisher automatically renders the report after the new value is selected or entered.

You set this property at the report level to override the system setting.

Clear Report Objects from the Server Cache

Use the Manage Cache page to clear the server cache.

The server cache stores report definitions, report data, and report output documents. If you need to manually purge this cache (for example, after patching) use the Manage Cache page.

To clear the report objects from the server cache:

1. From the Administration page, select **Manage Cache**.
2. On the Manage Cache page, click **Clear Object Cache**.

Clear the Subject Area Metadata Cache

You can clear the subject area metadata cache.

BI subject area metadata such as the dimension and measure names are cached at the server to quickly open the report in report designer. You can manually clear this cache if the BI subject area is updated through a binary semantic model (.rpd) file.

To clear the subject area metadata cache:

1. From the Administration page, select **Manage Cache**.
2. On the Manage Cache page, in the Clearing Subject Area Metadata Cache section, click **Clear Metadata Cache**.

Enable Diagnostics

Administrators and BI Authors can enable the diagnostics logs. You can enable and download diagnostics for scheduled jobs and online reports.

Topics:

Enable Diagnostics for Scheduler Jobs

You can enable diagnostics for a scheduler job in the **Schedule Report Job** page, and download the diagnostic logs from **Report Job History**.

You must have BI Administrator or BI Data Model Developer privileges to access the **Diagnostics** tab in the **Schedule Report Job** page. Perform the following steps to enable diagnostics.
To enable and download diagnostics for a scheduler job:

1. From the **New** menu, select **Report Job**.
2. Select the report to schedule, and click the **Diagnostics** tab.
3. Select and enable the required diagnostics.
   - Select **Enable SQL Explain Plan** to generate a diagnostic log with Explain plan/SQL monitor report information.
   - Select **Enable Data Engine Diagnostic** to generate a data processor log.

- Select **Enable Report Processor Diagnostic** to generate FO (Formatting Options) and server related log information.
- Select **Enable Consolidated Job Diagnostic** to generate the entire log, which includes scheduler log, data processor log, FO and server log details.

4. Submit the report.
5. After the report job runs, in the Report Job History page, select your report to view the details.
6. Under Output & Delivery, click **Diagnostic Log** to download the job diagnostic log and view the details.

   Use the Manage Job Diagnostics Log page to purge the old job diagnostic logs.

Enable Diagnostics for Online Reports

In the Report Viewer, you can enable diagnostics for online reports.

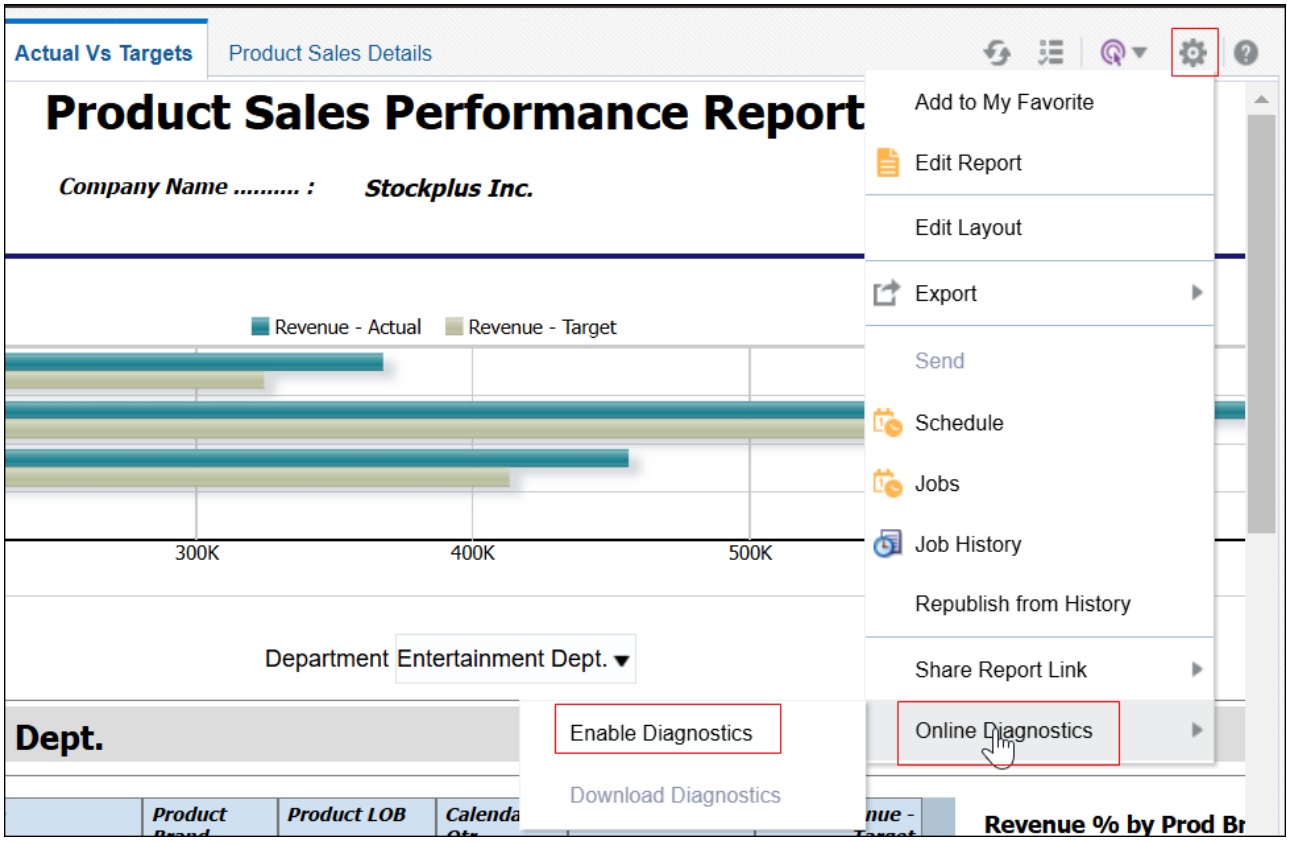
Administrators and BI Authors can enable diagnostics before running the online report, and then download the diagnostic logs after the report finishes. Diagnostics are disabled by default.

If you enable diagnostics for an online report with interactive output, you can:

- Download the following diagnostic logs in a .zip file:
  - SQL logs
  - Data engine logs
  - Report Processor logs
- View the following details in the diagnostic logs:
  - Exceptions
  - Memory guard limits
  - SQL query

To enable diagnostics and download the diagnostic logs for an online report:

1. If the report is running, click **Cancel** to stop the reporting process.
2. Click **Actions** in the Report Viewer.



3. Select **Enable Diagnostics** from the **Online Diagnostics** option.
4. Submit the report.
5. To download the diagnostic logs after the report runs:
    a. Click **Actions** in the Report Viewer.
    b. Select **Download Diagnostics** from the **Online Diagnostics** option.

Purge Job Diagnostic Logs

You can purge old diagnostic logs to increase the available space on your system.

The retention period of job diagnostic logs is set to 30 days, by default. If you frequently enable diagnostic logs, these diagnostic logs might consume space in the database, and you might need to periodically free the space consumed by the old diagnostic logs. You can manually purge the job diagnostic logs older than the retention period .

To purge the job diagnostic logs:

1. On the Administration page, under System Maintenance, select **Manage Job Diagnostics Log**.
2. Click **Purge log beyond retention period**.

Publisher Automatically Purges Transient Data of Old Jobs

Publisher automatically purges the transient data of completed scheduled jobs that are older than 365 days to improve system performance.

The scheduler tables of Publisher store the metadata of scheduled jobs, data XML, report output, diagnostic logs, and the metadata of report delivery. The large transient data in these scheduler tables can cause performance issues.

Once the report output has been purged, it can't be restored. The definitions of the recurring jobs won't be affected, and the recurring jobs run according to the job schedules.

The administrator can configure and reduce the retention period of the metadata of scheduled jobs to 90 days to improve the system performance.

If you need to retain report output beyond the system retention period, you can download the report output. See View Job History for a Specific Report, View Details of a Job History, Download Data from a Report Job, and Send an Output to a New Destination for instructions on how to download reports or deliver report outputs outside the Publisher application.

Manage Metadata of Old Scheduled Jobs

You can configure the retention period of transient data of old scheduled jobs.

1. From the Administration page, under System Maintenance, select **Manage Job Diagnostics Log**.
2. On the Manage Job Diagnostics Log page, in the Manage Scheduler Metadata section, enter the retention period in days.
3. Click **Apply**.

Manage Audit Data

Publisher automatically purges audit data older than 180 days to improve system performance.

You can reduce the retention period of audit data.

1. From the Administration page, under System Maintenance, select **Manage Job Diagnostics Log**.
2. On the Manage Job Diagnostics Log page, in the Manage Audit Data section, enter the retention period in days.
3. Click **Apply**.

Upload and Manage Configuration-Specific Files

Use Upload Center to upload and manage the configuration-specific files for font, digital signature, ICC profile, SSH private key, and SSL certificate.

To upload and manage the configuration-specific files:

1. On the Administration page, under System Maintenance, select **Upload Center**.
2. Click **Browse** and select the file you want to upload.
3. Select the configuration file type.
4. If you want to overwrite an existing file with the new file, select **Overwrite**.
5. Click **Upload**.
6. To manage the uploaded files, use the **Filter By Type** field to filter the files in the table.

3

Set Up Data Sources

This topic describes how to set up data sources for Publisher.

Topics:

Grant Access to Data Sources Using the Security Region

When you set up data sources, you can also define security for the data source by selecting which user roles can access the data source.

You must grant access to users for the following:

- A report consumer must have access to the data source to view reports that retrieve data from the data source.
- A report designer must have access to the data source to create or edit a data model against the data source.

By default, a role with administrator privileges can access all data sources.

The configuration page for the data source includes a Security region that lists all the available roles. You can grant roles access from this page, or you can also assign the data sources to roles from the roles and permissions page.

About Proxy Authentication

Publisher supports proxy authentication for connections to various data sources

Supported data sources include:

- Oracle 10*g* database
- Oracle 11*g* database
- Oracle BI Server

For direct data source connections through JDBC and connections through a JNDI connection pool, Publisher enables you to select "Use Proxy Authentication". When you select Use Proxy Authentication, Publisher passes the user name of the individual user (as logged into Publisher) to the data source and thus preserves the client identity and privileges when the Publisher server connects to the data source.

Enabling this feature requires additional setup on the database. The database must have Virtual Private Database (VPD) enabled for row-level security.

For connections to the Oracle BI Server, Proxy Authentication is required. In this case, proxy authentication is handled by the Oracle BI Server, therefore the underlying database can be any database supported by the Oracle BI Server.

About Connection Creation and Closure Functions

You can define PL/SQL functions for Publisher to run when a connection to a JDBC data source is created (preprocess function) or closed (postprocess function).

These two fields enable the administrator to set a user's context attributes before a connection is made to a database and then to dismiss the attributes after the connection is broken by the extraction engine.

The system variable :xdo_user_name can be used as a bind variable to pass the login username to the PL/SQL function calls. Setting the login user context in this way enables you to secure data at the data source level (rather than at the SQL query level).

For example, assuming the following sample function:

```
FUNCTION set_per_process_username (username_in IN VARCHAR2)
   RETURN BOOLEAN IS
     BEGIN
     SETUSERCONTEXT(username_in);
     return TRUE;
   END set_per_process_username
```

To call this function every time a connection is made to the database, enter the following in the **Pre Process Function** field: set_per_process_username(:xdo_user_name)

Another sample usage might be to insert a row to the LOGTAB table every time a user connects or disconnects:

```
CREATE OR REPLACE FUNCTION BIP_LOG (user_name_in IN VARCHAR2, smode IN
VARCHAR2)
RETURN BOOLEAN AS
   BEGIN
   INSERT INTO LOGTAB VALUES(user_name_in, sysdate,smode);
   RETURN true;
   END BIP_LOG;
```

In the **Pre Process Function** field enter: BIP_LOG(:xdo_user_name)

As a new connection is made to the database, it is logged in the LOGTAB table. The SMODE value specifies the activity as an entry or an exit. Calling this function as a **Post Process Function** as well returns results such as those shown in the table below.

NAME	UPDATE_DATE	S_FLAG
oracle	14-MAY-10 09.51.34.000000000	AMStart
oracle	14-MAY-10 10.23.57.000000000	AMFinish
administrator	14-MAY-10 09.51.38.000000000	AMStart
administrator	14-MAY-10 09.51.38.000000000	AMFinish
oracle	14-MAY-10 09.51.42.000000000	AMStart
oracle	14-MAY-10 09.51.42.000000000	AMFinish

Set Up a Database Connection Using a JNDI Connection Pool

You can create a connection to database using a JNDI connection pool to access data for pixel-perfect reports.

Using a connection pool increases efficiency by maintaining a cache of physical connections that can be reused. When a client closes a connection, the connection gets placed back into the pool so that another client can use it. A connection pool improves performance and scalability by allowing multiple clients to share a small number of physical connections. You set up the connection pool in your application server and access it through Java Naming and Directory Interface (JNDI).

> **Note**
>
> You can create JNDI connections to the user-defined data sources, but you can't create JNDI connections to the system-defined data sources. Only to create audit reports, you are allowed to create JNDI connections to the system-defined data sources to access the audit data source (AuditViewDataSource).

1. From the Publisher Administration page, click **JNDI Connection**.
2. Click **Add Data Source**.
3. Enter a display name for the data source. This name is displayed in the Data Source selection list in the Data Model Editor.
4. Enter the JNDI name for the connection pool. For example, `jdbc/BIPSource`.
5. Select **Use Proxy Authentication** to enable Proxy Authentication.
6. Click **Test Connection**. You see a confirmation message if the connection is established.
7. Define security for this data source connection. Move the required roles from the **Available Roles** list to the **Allowed Roles** list. Only users assigned the roles in the **Allowed Roles** list can create or view reports from this data source.

Set Up a Connection to an HTTP Data Source

You can create a connection to HTTP data source to build data models from XML, JSON, and CSV data over the web by retrieving data through the HTTP GET method.

If you want to use SSL connection for the HTTP data source, set the **Enable SSL for webservice, HTTP Datasource** runtime property to true.

Upload the SSL certificate in Upload Center before you define the SSL connection to the data source.

1. From the Publisher Administration page, click **HTTP Connection**.
2. Click **Add Data Source**.
3. Enter a display name for the data source. This name is displayed in the Data Source selection list in the Data Model Editor.
4. Select the server protocol.
5. Enter the server name and the server port.
6. Enter the URL context for the HTTP data source connection in the **Realm** field.

For example, xmlpserver/services/rest/v1/reports

7. Enter the user name and password required to access the data source on the database.
8. If you want to use SSL connection, from the **SSL Certificate** list, select the SSL certificate you want to use for the data source.
9. If you're using a proxy-enabled server, select **Use System Proxy**.
10. Define security for this data source connection. Move roles from the **Available Roles** list to the **Allowed Roles** list. Only users assigned the roles in the **Allowed Roles** list can create or view reports from this data source.

Set Up a Connection to a Content Server

You can create a connection to a Content Server to retrieve a text attachment stored inOracle WebCenter Content (earlier known as UCM) server, and display the attachment content in a pixel-perfect report.

1. From the Publisher Administration page, select the **Content Server** link.
2. Click **Add Data Source**.
3. Enter the name in the **Data Source Name** field.
4. Enter the URL in the **URI** field.
5. Enter the user name and password in the **Username** and **Password** fields, respectively.
6. Click **Test Connection**.
7. Define security for this data source connection. Move roles from the **Available Roles** list to the **Allowed Roles** list. Only users assigned the roles in the **Allowed Roles** list can create or view reports from this data source.
8. Click **Apply**.

Set Up a Connection to a Web Service

You can create a connection to web service data source to access data for pixel-perfect reports.

If you want to use SSL connection for the web service data source, set the **Enable SSL for webservice, HTTP Datasource** runtime property to true.

Upload the SSL certificate in Upload Center before you define the SSL connection to the data source.

1. From the Publisher Administration page, click **Web Service Connection**.
2. Click **Add Data Source**.
3. Enter a display name for the data source. This name is displayed in the Data Source selection list in the Data Model Editor.
4. Select the server protocol.
5. Enter the server name and the server port.
6. Enter the URL for the web service connection.
7. Optional: Enter the session timeout in minutes.
8. Select the security header from **WS-Security**.

- 2002 — Enables the "WS-Security" Username Token with the 2002 namespace: `http://docs.oasis-open.org/wss/2002/01/oasis-200201-wss-wssecurity-secext-1.0.xsd`
- 2004 — Enables the "WS-Security" Username Token with the 2004 namespace: `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText`

9. Optional: Enter the user name and password for the web service data source.
10. Optional: From the **SSL Certificate** list, select the SSL certificate you want to use for the connection.
11. If you're using a proxy-enabled server, select **Use System Proxy**.
12. Click **Test Connection**.
13. Define security for this data source connection. Move roles from the **Available Roles** list to the **Allowed Roles** list. Only users assigned the roles in the **Allowed Roles** list can create or view reports from this data source.
14. Click **Apply**.

View or Update a Connection to Data Source

You can view or update a connection to data source from the Publisher Administration page.

1. From the Publisher Administration page, select the **Data Source** type to update.
2. Select the name of the connection to view or update. All fields are editable. See the appropriate section for setting up the data source type for information on the required fields.
3. Select **Apply** to apply any changes or **Cancel** to exit the update page.

4

Set Up Delivery Destinations

This topic describes the setup required to deliver Publisher reports. It also describes how to set up the HTTP notification server.

Topics:

Configure Delivery Options

You can define the SSL certicate file and set the general properties for e-mail deliveries and notifications.

1. From the Administration page, select **Delivery Configuration**.
2. If you want to use a self-signed certificate, select a file from **SSL Certificate File**.
3. Enter the From address to appear on e-mail report deliveries.
4. Enter the From address to appear on notifications deliveries.
5. Enter the subject text for notification e-mails when the report status is Success, Warning, Failed, or Skipped.
6. In the **Allowed Email Recipient Domains** field, enter the domains you want to allow email delivery. Separate the email domains by a comma. By default, * allows all domains.

   Note that if you want to ignore email delivery restrictions for a report delivery, select the **Ignore Email domain Restrictions** property of that report.
7. Select **Email Output as URL**, if you want the jobs to email the URL to access the job output instead of attaching the job output to the email.

   The email recipient can view the job output only after logging in with the valid credentials required to access the Publisher report. The recipient must have access to Publisher. If the output of a private job is sent to a user without administrator access, the job succeeds and the recipient receives the email with the URL, but the recipient can't view the job output.
8. Select **Use System Proxy Settings** if the Delivery Manager must look up the proxy server settings from the Java runtime environment.
   - Printer, Fax, WebDAV, HTTP and CUPS servers use proxy settings for HTTP protocol when SSL is not used. When SSL is used, the HTTPS proxy setting is used.

- FTP and SFTP use proxy settings for FTP.
- Contents servers and email servers don't support connection over a proxy, regardless of this setting.

You can override the proxy settings per delivery server, using proxy configuration fields on the individual server setup page. If a proxy server and ports are configured for a delivery server, the Delivery Manager uses the proxy server and port configured for the server instead of the one defined in the Java Runtime environment. In Cloud installations, **Use System Proxy Settings** is always selected, and cannot be turned off or overridden by individual server settings.

If Publisher encounters an issue connecting to the email server, it attempts to send the email again for three times, with a 30-second interval between each attempt.

Add a Printer

You can set up a printer to print reports.

If you want to print checks on a remote printer, configure your print server with a SSL certificate supported by Fusion Truststore. Ensure that your server presents the entire certificate chain during the SSL handshake process. Test and verify that check printing works. In case check printing fails, review the print server logs. If the failure occurs during SSL handshake, then verify your print server configuration and make the necessary corrections.

1. From the Administration page, under **Delivery**, select **Printer**, and then click **Add Server**.
2. Enter the server name and URI of the printer.
3. Optional: If your printer or print server doesn't support printing PDF, enter a filter to call a conversion utility to convert the PDF to a file format supported by your specific printer type.
   - PDF to PostScript
   - PDF to PCL

   Use the PDF to PCL filter only if you have a requirement to select fonts for printing check using embedded PCL command. For generic printing requirements, use the PDF to PostScript filter.
4. Enter the user name, password, authentication type (Basic, Digest), and encryption Type (SSL).
5. Optional: In the Access Control section, deselect **Public**.
6. From the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and click **Move** to add them to the **Allowed Roles** list.
7. Click **Apply**.

Add a Fax Server

You must set up Common Unix Printing Service (CUPS) and the fax4CUPS extension, if you want to send fax.

1. From the Administration page, under **Delivery**, select **Fax**, and then click **Add Server**.
2. Enter the server name and the URI (Uniform Resource Identifier) of the fax server.
3. Enter the user name and password.
4. Optional: Enter the authentication type (Basic, Digest), and encryption Type (SSL) of the fax server.

5. Optional: If your fax server doesn't support printing PDF, select a print filter (PDF to PostScript, PDF to PCL, or None) to call a conversion utility to convert the PDF to a file format supported by your specific fax server.

   The **Filter Command** field isn't editable. The value of the **Filter Command** field is defined by what you select for the **Filter** field.

6. Optional: In the Access Control section, deselect **Public**.
7. From the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and click **Move** to add them to the **Allowed Roles** list.
8. Click **Apply**.

Configure an Email Server

You can configure the provisioned email server to provide access to the roles.

1. From the Administration page, under **Delivery**, select **Email**, and then select the default email server.
2. In the Access Control section, deselect **Public**, if selected.
3. From the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and click **Move** to add them to the **Allowed Roles** list.
4. Click **Test Connection**.
5. Click **Apply**.

Add a WebDAV Server

You add a WebDAV server from the Administration page.

To add a WebDAV server:

1. From the Administration page, select **WebDAV** to display the list of servers that have been added. Select **Add Server**.
2. Enter the **Name** and **Host** for the new server.
3. Optionally enter the following fields if appropriate:
   - General fields — **Port**
   - Security fields — **Authentication Type** (Basic, Digest) and **Encryption Type** (SSL).
4. Enter **User Name** and **Password**.

Add an HTTP or HTTPS Server

The administrator can add an HTTP or HTTPS sever to send a notification request to after the report completes.

You can register an application URL or postprocess HTTP or HTTPS URL as an HTTP server.

The HTTP notification sent by Publisher posts a form data for Job ID, report URL and Job Status to the HTTP Server URL page.

1. From the Administration page, under **Delivery**, select **HTTP**, and then click **Add Server**.
2. Enter the server name and the URL of the server.

3. Enter the user name and password.
4. Enter the host, port, authentication type (Basic, Digest), and and encryption type (SSL) of the server.
5. In the Access Control section, deselect **Public**.
6. From the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and click **Move** to add them to the **Allowed Roles** list.
7. Click **Apply**.

Add an FTP or SFTP Server

You can add an FTP server or SFTP server as a delivery channel for Publisher.

If the destination file name supplied to the scheduler contains non-ascii characters, UTF-8 encoding is used to specify the file name to the destination FTP server. Your FTP server must support UTF-8 encoding or the job delivery will fail with "Delivery Failed" error message.

Publisher doesn't support FTP over TLS / SSL (FTPS). You can't use FTP over TLS or SSL for delivery. Use SFTP for secure file transfer.

1. From the Administration page, under **Delivery**, select **FTP**, and then click **Add Server**.
2. Enter the server name, host name, and port number for the FTP or SFTP server.

   The default port for FTP is 21. The default port for Secure FTP (SFTP) is 22.
3. To enable Secure FTP (SFTP), select **Use Secure FTP**.
4. If the FTP server is behind a firewall, select **Use Passive Mode** .
5. Select **Create files with Part extension when copy is in process** to create a file on the FTP server with a .part extension while the file is transferring.

   When the file transfer is complete, the file is renamed without the .part extension. If the file transfer doesn't complete, the file with the .part extension remains on the server.
6. Optional: Enter the security information.
   a. If your server is password protected, enter the User name and Password.
   b. Select the **Authentication Type**: Private Key or Password
   c. Depending on the authentication type selection, select the private key file or specify the private password.
7. Optional: To deliver PGP encrypted documents to the FTP server:
   a. From the **PGP Key** list, select the PGP keys you uploaded in Security Center.

      This step updates the filter command in the **Filter Command** field.
   b. To sign the encrypted document, select **Sign Output**.

      This step adds a `-s` parameter to the existing filter command in the **Filter Command** field.
   c. If you want to deliver PGP encrypted document in ASCII armored format, select **ASCII Armored Output**.

      This step adds a `-a` parameter to the existing filter command in the **Filter Command** field.
8. In the Access Control section, deselect **Public**.

9. From the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and click **Move** to add them to the **Allowed Roles** list.
10. Click **Test Connection**.

    If the connection test is successful, the **Host Key Fingerprint** field is populated. You can't save the server configuration if the**Host Key Fingerprint** field isn't populated.

    When Publisher delivers jobs to the SFTP server, the **Host Key Fingerprint** value saved with the server configuration is compared with the fingerprint of the host key returned by the SFTP server. If the SFTP server host key's fingerprint doesn't match the fingerprint saved in the server connection configuration, the connection will be rejected.
11. Click **Apply**.

SSH Options For SFTP

Secure File Transfer Protocol (SFTP) is based on the Secure Shell technology (SSH). Publisher supports the following SSH options for SFTP delivery.

Key Exchange Method (Diffie-Hellman)	Server Public Key	Encryption (Cipher Suites)	Message Authentication Code (MAC)
• diffie-hellman-group14-sha1 • diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group1-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512	• ssh-rsa (up to 2048 bit) • ssh-dss (1024 bit) • rsa-sha2-256 • rsa-sha2-512	• aes128-gcm (aes128-gcm@openssh.com) • aes256-gcm (aes256-gcm@openssh.com) • aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • 3des-cbc • blowfish-cbc	• hmac-sha1 • hmac-sha2-256 • hmac-sha2-512

The following algorithms are available only when Publisher is running on a JVM on which the Java Cryptography Extension (JCE) unlimited strength jurisdiction policy files are installed:

- diffie-hellman-group-exchange-sha256
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- rsa-sha2-256
- rsa-sha2-512
- aes192-ctr
- aes256-ctr
- hmac-sha2-256
- hmac-sha2-512

Add a Custom Connection to Content Server

You can use a custom connection for Oracle WebCenter Content server to deliver files from Publisher to Oracle WebCenter Content server.

When you use a content server as a delivery destination, at runtime, the report consumer can tag the report with Security Group and Account metadata (if applicable) to ensure that the appropriate access rights are applied to the document when delivered.

Publisher communicates with Oracle WebCenter Content Server using the Remote Intradoc Client (RIDC). The connection protocols therefore follow the standards required by the RIDC.

FA_UCM_PROVISIONED, a provisioned connection to Oracle WebCenter Content server, uses a provisioned FUSION_APPS_OBIA_BIEE_APPID user to connect to Oracle WebCenter Content server with security groups and accounts to support the most common use cases. You can't delete or modify the FA_UCM_PROVISIONED connection, but you can disable the connection.

Configure a custom connection to Oracle WebCenter Content server using user credentials other than FUSION_APPS_OBIA_BIEE_APPID, if you want to access Oracle WebCenter Content server or to deliver PGP encrypted files from Publisher.

The custom connection to Oracle WebCenter Content server must use the same Uniform Resource Identifier (URI) as the provisioned connection, but should have its own user name and password.

1. In the Publisher Administration page, navigate to the Content Server tab in the Delivery section, and click **Add Server**.
2. Enter the same URI used by the provisioned FA_UCM_PROVISIONED Oracle WebCenter Content server.

   Every time you upgrade, verify the URI of the provisioned FA_UCM_PROVISIONED Content Server, and make sure the URI of the custom connection is similar to the URI of the provisioned FA_UCM_PROVISIONED Content Server.
3. Enter the server name, user name, and password.
4. Leave **Enable Custom Metadata** deselected. Custom metadata isn't used.
5. Optional: To deliver PGP encrypted documents to the content server:
   a. From the **PGP Key** list, select the PGP keys you uploaded in Security Center.

      This step updates the filter command in the **Filter Command** field.
   b. To sign the encrypted document, select **Sign Output**.

      This step adds a `-s` parameter to the existing filter command in the **Filter Command** field.
   c. If you want to deliver PGP encrypted document in ASCII armored format, select **ASCII Armored Output**.

      This step adds a `-a` parameter to the existing filter command in the **Filter Command** field.
6. Optional: Select **Use Logged in user as Author** to set the logged in user as the author of the report sent to the Content Server. If **Use Logged in user as Author** isn't selected, the reports sent to the Content Server contain the name of the report author.
7. In the Access Control section, deselect **Public**, if selected.

8. From the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and click **Move** to add them to the **Allowed Roles** list.
9. Click **Test Connection** to ensure that you can connect to Oracle WebCenter Content server.
10. Click **Apply**.

5

Define Runtime Configurations

This topic describes processing properties for PDF document security, FO processing, PDF accessibility, and specific properties for each output type.

Topics:

Set Runtime Properties

The Runtime Configuration page enables you to set runtime properties at the server level.

These same properties can also be set at the report level, from the report editor's Properties dialog. If different values are set for a property at each level, then report level takes precedence.

PDF Output Properties

Generate the type of PDF files you want by setting the PDF output properties.

Property Name	Description	Default
Compress PDF output	Specify "true" or "false" to control compression of the output PDF file.	true
Hide PDF viewer's menu bars	Specify "true" to hide the viewer application's menu bar when the document is active. The menu bar option is only effective when using the Export button, which displays the output in a standalone Acrobat Reader application outside of the browser.	false
Hide PDF viewer's tool bars	Specify "true" to hide the viewer application's toolbar when the document is active.	false
Replace smart quotes	Specify "false" if you don't want curly quotes replaced with straight quotes in the PDF output.	true
Disable opacity and gradient shading for DVT chart	Specify "true" if you don't want opacity and gradient shading for the PDF output. This reduces the size of the PostScript file.	false
Enable PDF Security	Specify "true" if you want to encrypt the PDF output. You can then also specify the following properties: • Open document password • Modify permissions password • Encryption Level	false
Open document password	This password is required for opening the document. It enables users to open the document only. This property is enabled only when "Enable PDF Security" is set to "true". When you set the Encryption level to Low, Medium, or High, the password must contain only Latin-1 characters and shouldn't be more than 32 bytes long. When you set the Encryption level to Highest, if your password exceeds 127 bytes, only the first 127 bytes of the password are used for authentication.	N/A

Property Name	Description	Default
Modify permissions password	This password enables users to override the security setting. This property is effective only when "Enable PDF Security" is set to "true". When you set the Encryption level to Low, Medium, or High, the password must contain only Latin-1 characters and shouldn't be more than 32 bytes long. When you set the Encryption level to Highest, if your password exceeds 127 bytes, only the first 127 bytes of the password are used for authentication. If you set a password in the `pdf-open-password` property without setting a password in the `pdf-permissions-password` property, or if you set the same password in both the `pdf-open-password` and `pdf-permissions-password` properties, the user gets full access to the document and its features, and permission settings such as "Disable printing" are bypassed or ignored.	N/A
Encryption level	Specify the encryption level for the output PDF file. The possible values are: • 0: Low (40-bit RC4, Acrobat 3.0 or later) • 1: Medium (128-bit RC4, Acrobat 5.0 or later) • 2: High (128-bit AES, Acrobat 7.0 or later) • 3: Highest (256-bit AES, Acrobat X (10) or later) This property is effective only when "Enable PDF Security" is set to "true". When Encryption level is set to 0, you can also set the following properties: • Disable printing • Disable document modification • Disable context copying, extraction, and accessibility • Disable adding or changing comments and form fields When Encryption level is set to 1 or higher, the following properties are available: • Enable text access for screen readers • Enable copying of text, images, and other content • Allowed change level • Allowed printing level	2 - high
Disable document modification	Permission available when "Encryption level" is set to 0. When set to "true", the PDF file cannot be edited.	false
Disable printing	Permission available when "Encryption level" is set to 0. When set to "true", printing is disabled for the PDF file.	false
Disable adding or changing comments and form fields	Permission available when "Encryption level" is set to 0. When set to "true", the ability to add or change comments and form fields is disabled.	false

Property Name	Description	Default
Disable context copying, extraction, and accessibility	Permission available when "Encryption level" is set to 0. When set to "true", the context copying, extraction, and accessibility features are disabled.	false
Enable text access for screen readers	Permission available when "Encryption level" is set to 1 or higher. When set to "true", text access for screen reader devices is enabled.	true
Enable copying of text, images, and other content	Permission available when "Encryption level" is set to 1 or higher. When set to "true", copying of text, images, and other content is enabled.	false
Allowed change level	Permission available when "Encryption level" is set to 1 or higher. Valid Values are: • 0: none • 1: Allows inserting, deleting, and rotating pages • 2: Allows filling in form fields and signing • 3: Allows commenting, filling in form fields, and signing • 4: Allows all changes except extracting pages	0
Allowed printing level	Permission available when "Encryption level" is set to 1 or higher. Valid values are: • 0: None • 1: Low resolution (150 dpi) • 2: High resolution	0
Use only one shared resources object for all pages	The default mode of Publisher creates one shared resources object for all pages in a PDF file. This mode has the advantage of creating an overall smaller file size. However, the disadvantages are the following: • Viewing may take longer for a large file with many SVG objects • If you choose to break up the file by using Adobe Acrobat to extract or delete portions, then the edited PDF files are larger because the single shared resource object (that contains all of the SVG objects for the entire file) is included with each extracted portion. Setting this property to "false" creates a resource object for each page. The file size is larger, but the PDF viewing is faster and the PDF can be broken up into smaller files more easily.	true
PDF Navigation Panel Initial View	Controls the navigation panel view presented when a user first opens a PDF report. The following options are supported: • Panels Collapsed - displays the PDF document with the navigation panel collapsed. • Bookmarks Open (default) - displays the bookmark links for easy navigation. • Pages Open - displays a clickable thumbnail view of each page of the PDF.	Bookmarks Open

PDF Digital Signature Properties

You set the properties to enable a digital signature for PDF reports and to define the placement of the signature in the output PDF report.

At the instance level or at the report level, you can set the properties to enable a digital signature for PDF reports. You must first register at least one digital signature, so you can select the one to you use in your instance or reports. To implement the digital signature for a report based on a PDF layout template or an RTF layout template, set the **Enable Digital Signature** property on the report to "true."

You also must set the appropriate properties to place the digital signature in the desired location on your output report. Your choices for placement of the digital signature depend on the template type. The choices are as follows:

- (PDF only) Place the digital signature in a specific field by setting the **Existing signature field name** property.
- (RTF and PDF) Place the digital signature in a general location of the page (top left, top center, or top right) by setting the **Signature field location** property.
- (RTF and PDF) Place the digital signature in a specific location designated by x and y coordinates by setting the **Signature field x coordinate** and **Signature field y coordinate** properties.

  If you choose this option, you can also set **Signature field width** and **Signature field height** to define the size of the field in your document.

Property Name	Description	Default
Enable Digital Signature	Set this to "true" to enable a digital signature for PDF reports.	false
Digital signature name	Select a registered digital signature file.	N/A
Existing signature field name	This property applies to PDF layout templates only. If the report is based on a PDF template, then you can enter a field from the PDF template in which to place the digital signature.	N/A
Signature field location	This property can apply to RTF or PDF layout templates. This property provides a list that contains the following values: Top Left, Top Center, Top Right. Choose one of these general locations and Publisher inserts the digital signature to the output document, sized and positioned appropriately. If you choose to set this property, do not enter X and Y coordinates or width and height properties.	N/A
Signature field X coordinate	This property can apply to RTF or PDF layout templates. Using the left edge of the document as the zero point of the X axis, enter the position in points that you want the digital signature to be placed from the left. For example, if you want the digital signature to be placed horizontally in the middle of an 8.5 inch by 11 inch document (that is, 612 points in width and 792 points in height), enter 306.	0

Property Name	Description	Default
Signature field Y coordinate	This property can apply to RTF or PDF layout templates. Using the bottom edge of the document as the zero point of the Y axis, enter the position in points that you want the digital signature to be placed from the bottom. For example, if you want the digital signature to be placed vertically in the middle of an 8.5 inch by 11 inch document (that is, 612 points in width and 792 points in height), enter 396.	0
Signature field width	Enter in points (72 points equal one inch) the desired width of the inserted digital signature field. This applies only if you're also setting the **Signature field x coordinate** and **Signature field Y coordinate** properties.	0
Signature field height	Enter in points (72 points equal one inch) the desired height of the inserted digital signature field. This applies only if you're also setting the **Signature field x coordinate** and **Signature field Y coordinate** properties.	0

PDF Accessibility Properties

Set the properties described in the table below to configure PDF accessibility.

Property Name	Description	Default
Make PDF output accessible	Set to “true” to make the PDF outputs accessible. Accessible PDF output contains the document title and PDF tags.	False
Use PDF/UA format for accessible PDF output	Set to “true” to use the PDF/UA format for the accessible PDF outputs.	False

PDF/A Output Properties

Set the properties described in the table below to configure PDF/A output.

Property Name	Description	Default
PDF/A version	Set the PDF/A version.	PDF/A-1B

Property Name	Description	Default
PDF/A ICC Profile Data	The name of the ICC profile data file, for example: CoatedFOGRA27.icc The ICC (International Color Consortium) profile is a binary file describing the color characteristics of the environment where this PDF/A file is intended to be displayed. The ICC profile that you select must have a major version below 4. To use a specific profile data file other than the default settings in the JVM, obtain the file and place it under `<bi publisher repository>/Admin/Configuration`. When you set this property, you must also set a value for PDF/A ICC Profile Info (`pdfa-icc-profile-info`).	Default profile data provided by JVM
PDF/A ICC Profile Info	ICC profile information (required when pdfa-icc-profile-data is specified)	sRGB IEC61966-2.1
PDF/A file identifier	One or more valid file identifiers set in the xmpMM:Identifier field of the metadata dictionary. To specify more than one identifier, separate values with a comma (,).	Automatically generated file identifier
PDF/A document ID	Valid document ID. The value is set in the xmpMM:DocumentID field of the metadata dictionary.	None
PDF/A version ID	Valid version ID. The value is set in the xmpMM:VersionID field of the metadata dictionary.	None
PDF/A rendition class	Valid rendition class. The value is set in the xmpMM:RenditionClass field of the metadata dictionary.	None

PDF/X Output Properties

Configure PDF/X output by setting the properties described below. The values that you set for these properties will depend on the printing device.

Note the following restrictions on other PDF properties:

- `pdf-version` — Value above 1.4 is not allowed for PDF/X-1a output.
- `pdf-security` — Must be set to False.
- `pdf-encryption-level` — Must be set to 0.
- `pdf-font-embedding` — Must be set to true.

Property Name	Description	Default
PDF/X ICC Profile Data	(Required) The name of the ICC profile data file, for example: CoatedFOGRA27.icc. The ICC (International Color Consortium) profile is a binary file describing the color characteristics of the intended output device. For production environments, the color profile may be provided by your print vendor or by the printing company that prints the generated PDF/X file. The file must be placed under `<bi publisher repository>/Admin/Configuration`. Profile data is also available from Adobe support or colormanagement.org.	None
PDF/X output condition identifier	(Required) The name of one of the standard printing conditions registered with ICC (International Color Consortium). The value that you enter for this property is a valid "Reference name," for example: FOGRA43. Choose the appropriate value for the intended printing environment. This name is often used to guide automatic processing of the file by the consumer of the PDF/X document, or to inform the default settings in interactive applications.	None
PDF/X output condition	A string describing the intended printing condition in a form that will be meaningful to a human operator at the site receiving the exchanged file. The value is set in OutputCondition field of OutputIntents dictionary.	None
PDF/X registry name	A registry name. Set this property when the `pdfx-output-condition-identifier` is set to a characterization name registered in a registry other than the ICC registry.	http://www.color.org
PDF/X version	The PDF/X version set in GTS_PDFXVersion and GTS_PDFXConformance fields of Info dictionary. PDF/X-1a:2003 is the only value currently supported.	PDF/X-1a:2003

DOCX Output Properties

The table below describes the properties that control DOCX output files.

Property Name	Description	Default
Enable change tracking	Set to "true" to enable change tracking in the output document.	false
Protect document for tracked changes	Set to "true" to protect the document for tracked changes.	false

Property Name	Description	Default
Default font	Use this property to define the font style and size in the output when no other font has been defined. This is particularly useful to control the sizing of empty table cells in generated reports. Enter the font name and size in the following format <FontName>:<size> for example: Arial:12. Note that the font you choose must be available to the processing engine at runtime.	Arial:12
Open password	Use this property to specify the password that report users must provide to open any DOCX report.	NA

RTF Output Properties

Configure RTF output files by setting the properties described in the table below.

Property Name	Description	Default
Enable change tracking	Set to "true" to enable change tracking in the output RTF document.	false
Protect document for tracked changes	Set to "true" to protect the document for tracked changes.	false
Default font	Use this property to define the font style and size in RTF output when no other font has been defined. This is particularly useful to control the sizing of empty table cells in generated reports. Enter the font name and size in the following format <FontName>:<size> for example: Arial:12. Note that the font you choose must be available to the processing engine at runtime. See Define Font Mappings for information about installing fonts and for the list of predefined fonts.	Arial:12
Enable widow orphan	Set to "true" to ensure that the document includes no “hanging paragraphs”. Suppose the last para in a page contains an orphaned line and the remaining lines of the paragraph continue on the next page. With this setting enabled, the starting line of the paragraph moves to the next page to keep all the lines of the paragraph together for improved readability.	false

PPTX Output Properties

The table below describes the properties that control PPTX output files.

Property Name	Description	Default
Open password	Use this property to specify the password that report users must provide to open any PPTX report.	NA

HTML Output Properties

The table below describes the properties that control HTML output files.

Property Name	Description	Default
Show header	Set to "false" to suppress the template header in HTML output.	true
Show footer	Set to "false" to suppress the template footer in HTML output.	true
Replace smart quotes	Set to "false" if you don't want curly quotes replaced with straight quotes in the HTML output.	true
Character set	Specify the output HTML character set.	UTF-8
Make HTML output accessible	Set to "true" to make the HTML output accessible.	false
Use percentage width for table columns	Set to "true" to display table columns according to a percentage value of the total width of the table rather than as a value in points. This property is especially useful if the browser display tables with extremely wide columns. Setting this property to true improves the readability of the tables.	true
View Paginated	When you set this property to true, HTML output will render in the report viewer with pagination features. These features include: • Generated table of contents • Navigation links at the top and bottom of the page • Ability to skip to a specific page within the HTML document • Search for strings within the HTML document using the browser's search capability • Zoom in and out on the HTML document using the browser's zoom capability Note that these features are supported for online viewing through the report viewer only.	false
Reduce Padding in Table-cell	When you set this property to true, cells in HTML tables are displayed without padding, which maximizes the page space available for text.	false
Embed images and charts in HTML for offline viewing	When you set this property to true, charts and images are embedded in the HTML output, which is suitable for viewing offline.	false
Use SVG for charts	When you set this property to true, charts display as a SVG (Scalable Vector Graphic) to provide a higher resolution in the HTML output. When you set this property to false, charts display as a raster image.	true
Keep original table width	When you set this property to true, if a column in a table is deleted, the original width of the table is maintained.	true
Enable horizontal scrollbar automatically for html table	When you set this property to true, a horizontal scroll bar is added to a table that doesn't fit within the current size of the browser window.	false

Property Name	Description	Default
Enable html table column size auto adjust	When you set this property to true, the column widths in a table are automatically adjusted to the size of the browser window.	false
Set zero height for empty paragraph	When you set this property to true and the output is HTML, the height of an empty paragraph (that is, a paragraph without text) is set to zero points.	true

FO Processing Properties

The table below describes the properties that control FO processing.

Property Name	Description	Default
Use BI Publisher's XSLT processor	Controls the use of parser. If set to "false", uses the non packaged XDK parser. If set to "true", uses the 11g parser packaged in Publisher. If set to "12c", uses the 12c parser packaged in Publisher. You can set this property at the server level or at the report level. If the data size is more than 2GB, set to "12c". If you set this property to "12c" at report level, ensure that you set the **Set ACCESS_MODE to FORWARD_READ on XSLT processor property** to '"false" at the server level and '"true" at the report level.	true
XML parser 11g compatibility mode	When set to "true", if the **Use BI Publisher's XSLT processor** property is set to "12c" or "false", the group-by attribute string is modified to ensure that the XDK 12c parser is compatible with the XML 11g parser.	True
Enable scalable feature of XSLT processor	Controls the scalable feature of the XDO parser. The property "Use BI Publisher's XSLT processor" must be set to "true" or "12c" for this property to be effective. The value of this property should be "true" at both server level and report level. If you set to "false", FO processor uses memory (heap) instead of disk, and might cause out-of-memory issues.	false
Enable XSLT runtime optimization	When set to "true", the overall performance of the FO processor is increased and the size of the temporary FO files generated in the temp directory is significantly decreased. Note that for small reports (for example 1-2 pages) the increase in performance isn't as marked. To further enhance performance when you set this property to true, set the **Extract attribute sets** property to "false".	true
Enable XPath Optimization	When set to "true", the XML data file is analyzed for element frequency. The information is then used to optimize XPath in XSL.	false

Property Name	Description	Default
Pages cached during processing	This property is enabled only when you specify a Temporary Directory (under General properties). During table of contents generation, the FO Processor caches the pages until the number of pages exceeds the value specified for this property. It then writes the pages to a file in the Temporary Directory.	50
Bidi language digit substitution type	Valid values are "None" and "National". When set to "None", Eastern European numbers are used. When set to "National", Hindi format (Arabic-Indic digits) is used. This setting is effective only when the locale is Arabic, otherwise it's ignored.	National
Disable variable header support	When set to true, prevents variable header support. Variable header support automatically extends the size of the header to accommodate the contents.	false
FO Parsing Buffer Size	Specifies the size of the buffer for the FO Processor. When the buffer is full, the elements from the buffer are rendered in the report. Reports with large tables or pivot tables that require complex formatting and calculations may require a larger buffer to properly render those objects in the report. Increase the size of the buffer at the report level for these reports. Note that increasing this value affects the memory consumption of the system.	1000000
FO extended linebreaking	When set to true, punctuation, hyphenation, and international text are handled properly when line breaking is necessary.	true
Enable XSLT runtime optimization for sub-template	Provides an option to perform XSL import in FOProcessor before passing only one XSL to XDK for further processing. This allows xslt-optimization to be applied to the entire main XSL template which already includes all its sub templates. The default is true. If you call the FOProcessor directly, the default is false.	true
Report Timezone	Valid values: User or JVM. When set to User, Publisher uses the User-level Report Time Zone setting for reports. The User Report Time Zone is set in the user's Account Settings. When set to JVM, Publisher uses the server JVM timezone setting for all users' reports. All reports therefore display the same time regardless of individual user settings. This setting can be overridden at the report level.	User
Set ACCESS_MODE to FORWARD_READ on XSLT processor	If you set the **Use BI Publisher's XSLT processor** property to "12c" at report level, ensure that the **Set ACCESS_MODE to FORWARD_READ on XSLT processor** property is set to "false" at the server level and "true" at the report level.	false
PDF Bidi Unicode Version	Specifies the Unicode version (3.0 or 4.1) used to display the BIDI strings in the PDF output.	4.1

RTF Template Properties

Configure RTF templates by setting the properties described in the table below.

Property Name	Description	Default
Extract attribute sets	The RTF processor automatically extracts attribute sets within the generated XSL-FO. The extracted sets are placed in an extra FO block, which can be referenced. This improves processing performance and reduces file size. Valid values are: • Enable - extract attribute sets for all templates and subtemplates • Auto - extract attribute sets for templates, but not subtemplates • Disable - do not extract attribute sets	Auto
Enable XPath rewriting	When converting an RTF template to XSL-FO, the RTF processor automatically rewrites the XML tag names to represent the full XPath notations. Set this property to "false" to disable this feature.	true
Characters used for checkbox	The default PDF output font doesn't include a glyph to represent a checkbox. If the template contains a checkbox, use this property to specify a Unicode font for the representation of checkboxes in the PDF output. You must specify the Unicode font number for the "checked" state and the Unicode font number for the "unchecked" state using the following syntax: `fontname;<unicode font number for true value's glyph>;<unicode font number for false value's glyph>` The font that you specify must be available for generating the PDF output at runtime. Example: Go Noto Current Jp;9745;9744	Go Noto Current Jp;9745;9744
Barcode encoder	Select the barcode encoder for generating the barcodes in reports. Oracle recommends that you use the Libre encoder.	Libre

XPT Template Properties

Configure XPT templates by setting the properties described in the table below.

Property Name	Description	Default
XPT Scalable Mode for Offline Reports	When you set this property to true, the scheduled reports that use the XPT template and include a large amount of data run without memory issues. The first 100,000 rows of data in the report are stored in memory and the remaining rows are stored in the file system. When you set this property to false, the scheduled reports that use XPT template are processed in-memory. Set this property to false for reports that contain less data.	False
XPT Scalable Mode for Online Static Output	When you set this property to true, the online reports that use the XPT template and include a large amount of data run without memory issues. The first 100,000 rows of data in the report are stored in memory and the remaining rows are stored in the file system. When you set this property to false, the online reports that use XPT template are processed in-memory. Set this property to false for reports that contain less data.	False
Enable Asynchronous Mode for Interactive Output	When you set this property to true, interactive reports that use the XPT template make asynchronous calls to Oracle WebLogic Server. When you set this property to false, interactive reports that use the XPT template make synchronous calls to Oracle WebLogic Server. Oracle WebLogic Server limits the number of synchronous calls. Any calls that are stuck expire in 600 seconds.	True

PDF Template Properties

Generate the types of PDF files you want by setting available PDF template properties.

Property Name	Description	Default
Remove PDF fields from output	Specify "true" to remove PDF fields from the output. When PDF fields are removed, data entered in the fields cannot be extracted.	false
Set all fields as read only in output	By default, all fields in the output PDF of a PDF template is read only. If you want to set all fields to be updatable, set this property to "false".	true
Maintain each field's read only setting	Set this property to "true" if you want to maintain the "Read Only" setting of each field as defined in the PDF template. This property overrides the settings of "Set all fields as read only in output."	false

Excel Template Properties

Configure Excel templates by setting the properties described in the table below.

Property Name	Description	Default
Enable Scalable Mode	When set to true, large reports that use Excel template run without out of memory issues. Data overflows automatically into multiple sheets if a group of data in a sheet exceeds 65000 rows. This overcomes the Microsoft Excel limitation of 65000 rows per sheet. When set to false, large reports that use Excel template can cause out of memory issues.	false

CSV Output Properties

The table below describes the properties that control comma-delimited value output.

Property Name	Description	Default
CSV delimiter	Specifies the character used to delimit the data in comma-separated value output. Other options are: Semicolon (;), Tab (\t) and Pipe (|).	Comma (,)
Remove leading and trailing white space	Specify "True" to remove leading and trailing white space between data elements and the delimiter.	false
Add UTF-8 BOM Signature	Specify "False" to remove the UTF-8 BOM signature from the output.	true

Excel Output Properties

You can set specific properties to control Excel output.

Property Name	Description	Default
Show grid lines	Set to true to show the Excel table grid lines in the report output.	false
Page break as a new sheet	Set to "True" if you want a page break specified in the report template to generate a new sheet in the Excel workbook.	true
Minimum column width	Set the coulmn width in points. When the column width is less than the specified minimum and it contains no data, the column is merged with the preceding column. The valid range for this property is 0.5 to 20 points.	3 (in points, 0.04 inch)
Minimum row height	Set the row height in points. When the row height is less than the specified minimum and it contains no data, the row is removed. The valid range for this property is 0.001 to 5 points.	1 (in points, 0.01 inch)

Property Name	Description	Default
Keep values in same column	Set this property to True to minimize column merging. Column width is set based on column contents using the values supplied in the Table Auto Layout property. Output may not appear as neatly laid out as when using the original layout algorithm.	False
Table Auto Layout	Specify a conversion ratio in points and a maximum length in points, for example 6.5,150. See example. For this property to take effect, the property "Keep values in same column" must be set to True. This property expands the table column width to fit the contents. The column width is expanded based on the character count and conversion ratio up to the maximum specification. Example: Assume a report with two columns of Excel data -- Column 1 contains a text string that's 18 characters and Column 2 is 30 characters long. When the value of this property is set to 6.5,150, the following calculations are performed: Column 1 is 18 characters: Apply the calculation: 18 * 6.5pts = 117 pts The column in the Excel output will be 117 pts wide. Column 2 is 30 characters: Apply the calculation: 30 * 6.5 pts = 195 pts Because 195 pts is greater than the specified maximum of 150, Column 2 will be 150 pts wide in the Excel output.	N/A
Maximum allowable nested table row count	Specify the maximum allowable row count for a nested table. Allowed values are 15000 to 999,999. During report processing, nested inner table rows cannot be flushed to the XLSX writer, therefore they stay in-memory, increasing memory consumption. Set this limit to avoid out-of-memory exceptions. When this limit is reached for the size of the inner table, generation is terminated. The incomplete XLSX output file is returned.	20,000
Open password	Use this property to specify the password that report users must provide to open any XLSX output file. Configuration name: `xlsx-open-password`	NA
Enable row split	Set to "true" to avoid stretching a row to a large height, and allow the row to be split into multiple rows.	True

EText Output Properties

The table below describes the properties that control EText output files.

Property Name	Description	Default
Add UTF-8 BOM Signature	When set to true, the Etext output is in UTF-8 Unicode with BOM format.	false
Enable bigdecimal	When set to true, you enable high-precision numeric calculation of the Etext output.	false

All Outputs Properties

The properties in the table below apply to all outputs.

Property Name	Description	Default
Use 11.1.1.5 compatibility mode	Reserved. Don't update unless instructed by Oracle.	False
Ignore case for catalog object path	Specifies whether to ignore the case of the catalog object path while locating a catalog object.	False
Allow fallback to seeded report	Specifies whether to fallback on or to skip execution of the corresponding seeded report (pre-defined report) when you don’t have permission to run the custom report. When set to true and the user doesn’t have permission to run the custom report, the corresponding seeded report executes. When set to false, you get an error when the custom report execution fails.	True
Webservice optimization	When set to true, Publisher caches the report definition and avoids multiple requests to the catalog when the same report runs multiple times within a short interval of time. Caching helps to improve the system performance.	True

Memory Guard Properties

The Runtime Configuration page lists the default values of the memory guard properties.

Property	Description	Default Value
Maximum report data size for online reports	Limits the data size for online reports.	300MB
Maximum report data size for offline (scheduled) reports	Limits the data size for scheduled reports.	500MB
Maximum report data size for bursting reports	Limits the data size for bursting reports.	Maximum report data size for offline (scheduled) reports
Free memory threshold	Ensures a minimum available free memory space.	500MB

Property	Description	Default Value
Maximum report data size under the free memory threshold	Limits the data size of a report when the Free memory threshold property is set to a positive value.	free_memory_threshold/ 10
Minimum time span between garbage collection runs	Ensures a minimum time gap in seconds between any two subsequent garbage collection runs.	300 (seconds)
Maximum wait time for free memory to come back above the threshold value	Limits the time in seconds for a run-report request to wait for the free JVM memory to exceed the threshold value. This property value takes effect only if you specify a positive value for the Free memory threshold property. If free memory is still below the threshold value after the specified wait time, the run-report request is rejected.	30 (seconds)
Timeout for online reports	Specifies the timeout value in seconds for processing an online report (includes the time for data extraction and report generation).	535 (seconds)
Maximum rows for CSV output	Limits the rows for reports in CSV format.	1000000

Data Model Properties

The Runtime Configuration page lists the values of the data model properties. The values of the data model properties depend on the compute shape used for your instance.

Property	Description	Default
Maximum data size limit for data generation	Limits the size of XML data that can be generated by executing a data model.	500MB
Maximum sample data size limit	Limits the size of a sample data file that can be uploaded from the data model editor.	1MB
Enable Data Model scalable mode	Prevents out of memory conditions. When set to true, the data engine takes advantage of the disk space while processing data.	True
Enable Auto DB fetch size mode	Avoids out of memory conditions, but can significantly increase the processing time. This setting is recommended only for frequently processing complex queries of hundreds of columns. When set to true, the database fetch size is set at runtime according to the total number of columns and the total number of query columns in the dataset. Ignores the **DB fetch size** setting. This property overrides the data model-level database fetch size properties.	True
DB fetch size	Limits the database fetch size for a data model. This property value takes effect only when **Enable Auto DB fetch size mode** is set to False.	20 (rows)
SQL Query Timeout	Specifies the timeout value for SQL queries for scheduled reports.	600 seconds

Property	Description	Default
Enable Data Model diagnostic	Writes the dataset details, memory, and SQL processing time information to the log file when set to true. Oracle recommends setting this property to true only for debugging purposes. If you enable this property, the processing time is increased. After you enable this property, click **View Engine Log** in the data model editor to view the data engine log file. See About the Data Model Editor Interface.	False
Enable SQL Session Trace	Writes a SQL session trace log to the database when set to true for every SQL query that's processed. A database administrator can examine the log.	False
Enable SQL Pruning	Reduces the processing time and the memory usage, if you enable this property. Applies only to the Oracle Database queries that use Standard SQL. If your query returns many columns but only a subset are used by your report template, SQL pruning returns only those columns required by the template. SQL pruning is not applicable for PDF, Excel, and E-text template types.	False
Enable Data Chunking	Enables XML data chunking for individual data models, reports, and report jobs, if you set this property to true. If you set this property to true, specify an appropriate value for the **Data Chunk Size** property to process large and long-running reports.	False
Data Chunk Size	Specifies the data size for each data chunk. Applies only when the **Enable Data Chunking** property is set to true.	300MB
DV Data Row Limit	Limits the number of rows that can be retrieved from a dataset.	2000000
Trim Leading and Trailing Spaces From Parameter Value	Trims the leading and trailing spaces from the parameter values of data models.	True
Exclude Line Feed And Carriage Return for LOB	Excludes carriage returns and line feeds in the data, if you set this property to true.	False
Enable SSL for webservice, HTTP Datasource	Supports SSL connection for webservice and HTTP data source, and automatically imports the self-signed SSL certificate from the server, if you set this property to true. If the certificate isn't self-signed, use Upload Center to upload the SSL certificate, and use the uploaded SSL certificate to configure the connection.	False

Report Delivery Properties

The properties in the table below apply to report delivery.

Property Name	Description	Default
Enable FTP/SFTP delivery retry	If a delivery through an FTP or SFTP delivery channel fails, Publisher makes another attempt to deliver, 10 seconds after the first attempt fails. This setting affects all FTP and SFTP delivery requests, and can't be configured for individual servers.	True

Define Font Mappings

Map base fonts in RTF or PDF templates to target fonts to be used in the published document.

You can specify font mapping at the site or report level. Font mapping is performed only for PDF output and PowerPoint output.

There're two types of font mappings:

- RTF Templates — for mapping fonts from RTF templates and XSL-FO templates to PDF and PowerPoint output fonts
- PDF Templates — for mapping fonts from PDF templates to different PDF output fonts.

Use Upload Center to upload custom fonts. See Upload and Manage Configuration-Specific Files.

Set Font Mapping at the Site Level or Report Level

A font mapping can be defined at the site level or the report level.

- To set a mapping at the site level, select the **Font Mappings** link from the Administration page.
- To set a mapping at the report level, view the Properties for the report, then select the **Font Mappings** tab. These settings apply to the selected report only.

The report-level settings take precedence over the site-level settings.

Create a Font Map

Provide the base font and target font.

1. From the Administration page, under **Runtime Configuration**, select **Font Mappings**.
2. Under RTF Templates or PDF Templates, click **Add Font Mapping**.
3. Provide the details for the base font.
    - **Base Font**: Enter the font family to map to a new font. You must provide the exact font family name that’s used in the RTF template. For example, Arial.
    - **Style**: Normal or Italic (Not applicable to PDF Template font mappings)
    - **Weight**: Normal or Bold (Not applicable to PDF Template font mappings)
4. Provide the details of the target font.
    - **Target Font Type**: Type 1 or TrueType
    - **Target Font**: Select a target font.

If you selected TrueType, you can enter a specific numbered font in the collection. Enter the **TrueType Collection (TTC) Number** of the desired font.

Predefined Fonts

The following Type1 fonts are built-in to Adobe Acrobat and by default the mappings for these fonts are available for publishing.

You can select any of these fonts as a target font with no additional setup required.

The Type1 fonts are listed in the table below.

Font Family	Style	Weight	Font Name
serif	normal	normal	Time-Roman
serif	normal	bold	Times-Bold
serif	italic	normal	Times-Italic
serif	italic	bold	Times-BoldItalic
sans-serif	normal	normal	Helvetica
sans-serif	normal	bold	Helvetica-Bold
sans-serif	italic	normal	Helvetica-Oblique
sans-serif	italic	bold	Helvetica-BoldOblique
monospace	normal	normal	Courier
monospace	normal	bold	Courier-Bold
monospace	italic	normal	Courier-Oblique
monospace	italic	bold	Courier-BoldOblique
Courier	normal	normal	Courier
Courier	normal	bold	Courier-Bold
Courier	italic	normal	Courier-Oblique
Courier	italic	bold	Courier-BoldOblique
Helvetica	normal	normal	Helvetica
Helvetica	normal	bold	Helvetica-Bold
Helvetica	italic	normal	Helvetica-Oblique
Helvetica	italic	bold	Helvetica-BoldOblique
Times	normal	normal	Times
Times	normal	bold	Times-Bold
Times	italic	normal	Times-Italic
Times	italic	bold	Times-BoldItalic
Symbol	normal	normal	Symbol
ZapfDingbats	normal	normal	ZapfDingbats

The TrueType fonts are listed in the table below. All TrueType fonts are subset and embedded into PDF.

Font Family Name	Style	Weight	Actual Font	Actual Font Type
Go Noto Current Jp	normal	normal	GoNotoCurrentJp.ttf	TrueType (Japanese flavor)
Go Noto Current Kr	normal	normal	GoNotoCurrentKr.ttf	TrueType (Korean flavor)
Go Noto Current Sc	normal	normal	GoNotoCurrentSc.ttf	TrueType (Simplified Chinese flavor)
Go Noto Current Tc	normal	normal	GoNotoCurrentTc.ttf	TrueType (Traditional Chinese flavor)

Open-Source Fonts Replace Licensed Monotype Fonts

In Oracle Transactional Business Intelligence, Oracle has replaced Monotype fonts with open-source fonts in PDF reports in Oracle Analytics Publisher, analyses, and dashboards.

The Go Noto font is the default fallback font for PDF reports in Oracle Analytics Publisher, analyses, and dashboards. Test the open-source fonts in your reports and correct the formatting in the report templates.

What do I need to know about fonts in reports?

The following table lists the replacement for Monotype fonts in Oracle Transactional Business Intelligence.

Monotype Fonts	Replacement Fonts
Monotype Albany fonts	Google Noto fonts
Monotype Barcode fonts	Libre Barcode fonts

Oracle Transactional Business Intelligence reports use the Go Noto font as the fallback font for PDF reports to support non-English languages and some special characters of English and Western European languages. The system uses the fallback font when the default PDF fonts (such as Helvetica, Times Roman, and Courier) or user-provided fonts can’t render the characters included in the data while generating the PDF output.

Use Libre Barcode fonts to generate barcodes.

What can I do now about fonts in my reports?

Oracle recommends that you review all your critical reports and edit the layout to format the reports as required. The impact of replacing the licensed Monotype fonts with the open-source fonts in analyses reports and dashboards is expected to be minimal because these reports don’t include pixel-perfect layouts.

The Google Noto fonts and the Monotype Albany fonts are similar; however, there are a few minor differences in the height, width, and weight for characters in some non-English languages. In some cases, these differences might impact the pixel-perfect PDF output. You might have to edit the layout template of these reports to use the Google Noto fonts. Note that Publisher doesn't support bold type for the Google Noto fonts.

Go Noto font is the default fallback font for analyses, dashboards, and Publisher reports.

Monotype Barcode Fonts	Replacement Fonts
128R00.ttf	LibreBarcode128-Regular.ttf
B39R00.ttf	LibreBarcode39Extended-Regular.ttf
UPCR00.ttf	LibreBarcodeEAN13Text-Regular.ttf

Define Currency Formats

Currency formats defined in the Administration Runtime Configuration page are applied at the system level. Currency formats can also be applied at the report level.

The report-level settings take precedence over the system-level settings here.

Understand Currency Formats

The Currency Formats tab enables you to map a number format mask to a specific currency so that your reports can display multiple currencies with their own corresponding formatting. Currency formatting is only supported for RTF and XSL-FO templates.

To apply currency formats in the RTF template, use the format-currency function.

To add a currency format:

1. Click the **Add** icon.
2. Enter the ISO currency code, for example: USD, JPY, EUR, GBP, INR.
3. Enter the format mask to apply for this currency.

   The Format Mask must be in the Oracle number format. The Oracle number format uses the components "9", "0", "D", and "G" to compose the format, for example: 9G999D00

   where

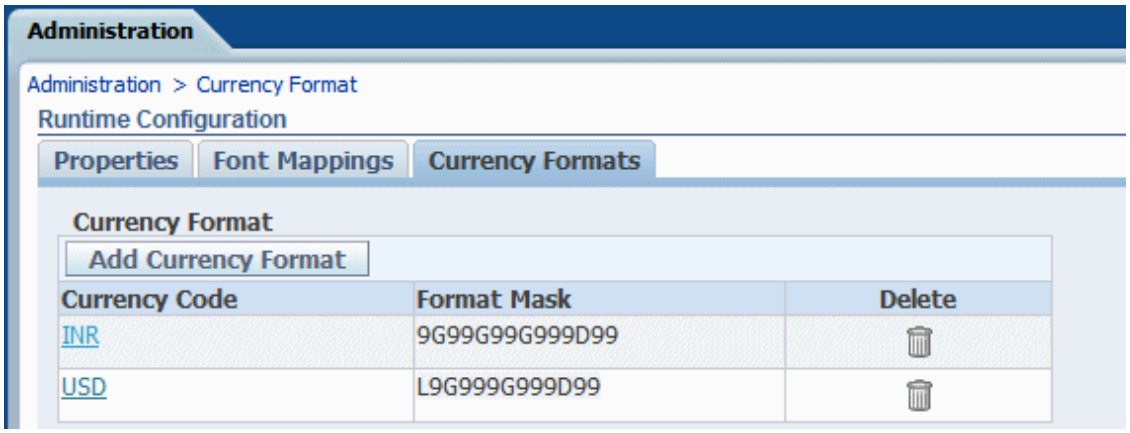
   9 represents a displayed number only if present in data

   G represents the group separator

   D represents the decimal separator

   0 represents an explicitly displayed number regardless of incoming data

The figure below shows sample currency formats.



6

Secure Reports

This topic describes how to secure pixel-perfect reporting.

Topics:

Use Digital Signatures in PDF Reports

You can apply a digital signature to a PDF report.

Digital signatures enable you to verify the authenticity of the documents you send and receive. You can upload your digital signature file to a secure location, and at runtime sign the PDF report with the digital signature. The digital signature verifies the signer's identity and ensures that the document hasn't been altered after it was signed.

For additional information, refer to the Verisign and Adobe websites.

Prerequisites and Limitations of Digital Signatures

When you use digital signatures with PDF reports in Publisher, you must be aware of a few limitations.

A digital signature is obtained from a public certificate authority or from a private/internal certificate authority (if for internal use only).

Keep the following limitations in mind:

- Only the reports scheduled in Publisher can include the digital signature.
- You can register multiple digital signatures and enable a digital signature at the instance level. At the report level, you can choose the digital signature you want to apply for the report. Multiple templates assigned to the same report share the digital signature properties.

Obtain Digital Certificates

You can obtain a digital certificate either by purchasing one or by using the self-sign method.

- To obtain a digital certificate, perform one of the following:
  - Purchase a certificate from an authority, verify and trust the authenticity of the certificate, and then use Microsoft Internet Explorer to create a PFX file based on the certificate you purchased.
  - Create a self-signed certificate using a software program such as Adobe Acrobat, Adobe Reader, OpenSSL, or OSDT as part of a PFX file, and then use the PFX file to sign PDF documents by registering it with Publisher. Bear in mind that anyone can create a self-signed certificate, so use care when verifying and trusting such a certificate.

Create PFX Files

If you obtained a digital certificate from a certificate authority, you can create a PFX file using that certificate.

You don't need to create a PFX file if a self-signed certificate PFX file already exists.

To create a PFX file with Microsoft Internet Explorer:

1. Ensure that your digital certificate is saved on your computer.
2. Open Microsoft Internet Explorer.
3. From the Tools menu, click **Internet Options** and then click the Content tab.
4. Click Certificates.
5. In the Certificates dialog, click the tab that contains your digital certificate and then click the certificate.
6. Click **Export**.
7. Follow the steps in the Certificate Export Wizard. For assistance, refer to the documentation provided with Microsoft Internet Explorer.
8. When prompted, select **Use DER encoded binary X.509** as your export file format.
9. When prompted, save your certificate as part of a PFX file to an accessible location on your computer.

After you create your PFX file, you can use it to sign PDF documents.

Apply a Digital Signature

You can set up and sign your PDF reports with a digital signature.

You can upload and register multiple digital signatures, set one as the default signature for the instance, and choose a digital signature you want to apply for a report.

1. Upload the digital signature files in Upload Center.
2. Register the digital signature in the Publisher Administration page and specify the roles that are authorized to sign reports.
3. If you have registered multiple digital signatures, set one as the default signature for the instance.
    a. In the Administration page, navigate to **Security Center**, and click **Digital Signature**.
    b. In the Digital Signature tab, select the digital signature file you want to set as default, and click **Set as Default**.
    c. In the Runtime Configuration page, set the **Enable Digital Signature** property to true.
4. To configure a digital signature for a report, select the report and set the digital signature properties.
    a. In the Report Properties dialog, select the Formatting tab.
    b. Set the **Enable Digital Signature** property to true for the report.
    c. Select the digital signature for the report.
    d. Specify the display field name and location.

5. Log in as a user with an authorized role and submit the report through the Publisher scheduler, choosing the PDF report. When the report completes, it's signed with your digital signature in the specified location of the report.

Register Your Digital Signature and Assign Authorized Roles

Register a digital signature and assign roles that can have the authority to sign documents with this digital signature.

You must upload the digital signature file in Upload Center.

1. On the Administration tab, under **Security Center**, click **Digital Signature**.
2. Select the digital signature file you uploaded in Upload Center and enter the password for the digital signature.
3. Enable the Roles that must have the authority to sign documents with this digital signature. Use the shuttle buttons to move Available Roles to the Allowed Roles list.
4. Click **Apply**.

Specify the Signature Display Field or Location

You must specify the location for the digital signature to appear in the completed document. The methods available depend on whether the template type is PDF or RTF.

If the template is PDF, use one of the following options:

- Specify a template field in a PDF template for the digital signature.
- Specify the location for the digital signature in the report properties.

If the template is RTF, specify the location for the digital signature in the report properties.

Specify a Template Field in a PDF Template for the Digital Signature

Include a field in the PDF template for digital signatures.

Report authors can add a new field or configure an existing field in the PDF template for the digital signature. See Add or Designate a Field for a Digital Signature.

Specify the Location for the Digital Signature in the Report

You can specify the location for the digital signature in the report.

When you specify a location in the document to place the digital signature, you can either specify a general location (Top Left, Top Center, or Top Right) or you can specify x and y coordinates in the document.

You can also specify the height and width of the field for the digital signature by using runtime properties. You don't need to alter the template to include a digital signature.

1. In the catalog, navigate to the report.
2. Click the **Edit** link for the report to open the report for editing.
3. Click **Properties** and then click the Formatting tab.
4. Scroll to the **PDF Digital Signature** group of properties.
5. Set **Enable Digital Signature** to **True**.

6. Specify the location in the document where you want the digital signature to appear by setting the appropriate properties as follows (note that the signature is inserted on the first page of the document only):
   - **Existing signature field name** — Doesn't apply to this method.
   - **Signature field location** — Provides a list containing the following values:

     Top Left, Top Center, Top Right

     Select one of these general locations and Publisher places the digital signature in the output document sized and positioned appropriately.

     If you set this property, then don't enter X and Y coordinates or width and height properties.
   - **Signature field X coordinate** — Using the left edge of the document as the zero point of the X axis, enter the position in points to place the digital signature from the left.

     For example, to place the digital signature horizontally in the middle of an 8.5 inch by 11 inch document (that is, 612 points in width and 792 points in height), enter 306.
   - **Signature field Y coordinate** — Using the bottom edge of the document as the zero point of the Y axis, enter the position in points to place digital signature from the bottom.

     For example, to place the digital signature vertically in the middle of an 8.5 inch by 11 inch document (that is, 612 points in width and 792 points in height), enter 396.
   - **Signature field width** — Enter in points the desired width of the inserted digital signature field. This applies only if you're setting the X and Y coordinates.
   - **Signature field height** — Enter in points the desired height of the inserted digital signature field. This applies only if you're setting the X and Y coordinates.

Run and Sign Reports with a Digital Signature

If you've been assigned a role that's been granted the digital signature privilege, you can sign a generated report with a signature, if the report has been configured to include signatures. You can sign only scheduled reports with signatures.

To sign reports with a digital signature:

1. Log in as a user with a role granted digital signature privileges.
2. In the catalog, navigate to the report that has been enabled for digital signature, and click **Schedule**.
3. Complete the fields on the Schedule Report Job page, select **PDF output**, and then submit the job.

   The completed PDF displays the digital signature.

Use PGP Keys for Encrypted Report Delivery

You can deliver PGP encrypted reports through FTP server or Content server.

You can configure the FTP server and Content server delivery channels to use the PGP public keys to deliver PGP encrypted files in binary or ASCII format.

Use Security Center to upload and download the PGP keys. The "BI Publisher Public Key" file is verifying the signature on signed files. If you configure a delivery channel to send signed documents, download the "BI Publisher Public Key" file (either in binary or ASCII format), and

import the keys in the destination PGP system used to verify signature and decrypt the files delivered by Publisher.

Manage PGP Keys

You can upload and delete your PGP keys.

1. From the Administration page, under **Security Center**, select **PGP Keys**.
2. To upload PGP keys to keystore, click **Choose File**, select the PGP key file, and then click **Upload**.
3. To delete the PGP keys you uploaded, in the PGP Keys table, click the delete icon corresponding to the PGP keys.
4. To download the PGP public keys for signature verification, click the download icon corresponding to the public key file.

Encrypt Data Files

Encrypt the data files used as data source for data models.

If you enable data file encryption, Publisher can encrypt the data files (XML, Excel, or CSV) uploaded as data source for data models, and then decrypt the data files to generate reports.

> **Note**
>
> You can set the password only once and the password you set can't be changed. Note down the encryption password for future use because the password can't be recovered.

1. From the Administration page, under Security Center, select **File Data Encryption**.
2. Select **Enable File Data Encryption**.
3. Enter the encryption password and click **Apply**.

7

Audit Data of Publisher Catalog Objects

An administrator can enable or disable viewing of the audit data of Publisher catalog objects, configure a connection to the audit data, and create reports to view the audit data.

Topics:

About Audit Data of Publisher Catalog Objects

You can use the sample reports to view the audit data of Publisher catalog objects.

You can find out the time of access and who accessed the Publisher catalog objects such as reports, data models, sub-templates, style templates, and folders.

Audit data helps you track:

- Report start, process, end, and download
- Report job pause, resume, and cancellation
- Publisher resource creation, modification, copy, and deletion
- Publisher resource access

> **Note**
>
> User session data (User Login and User Logout events) isn't included in the audit data. Only the reporting activities performed in the *host*:*port*/xmlpserver Publisher interface pages are included in the audit data. The reporting activities performed in the *host*:*port*/analytics interface pages aren't included in the audit data.

Enable or Disable Viewing of Publisher Audit Data

Administrators can enable or disable viewing the audit data of publishing activities.

1. Navigate to the Server Configuration page.
2. To enable viewing of audit data, select **Enable Monitor and Audit** and set **Audit Level** to **Medium**.
3. To disable viewing of audit data, deselect **Enable Monitor and Audit**.

Specify the Data Source Connection for Publisher Audit Data

Configure a data source connection for the audit data.

1. In the Administration page, click **JNDI Connection**.
2. Click **Add Data Source**.
3. In the **Data Source Name** field, enter AuditViewDB.
4. In the **JNDI Name** field, enter `jdbc/AuditViewDataSource`.
5. Click **Test Connection** to confirm the connection to the audit data source.
6. Define security for this data source connection. Move the required roles from the **Available Roles** list to the **Allowed Roles** list. Only users assigned the roles on the **Allowed Roles** list can create or view reports from this data source.
7. Click **Apply**.

View Publisher Audit Data

You can download and use the sample reports for viewing the audited information.

Make sure you select **Enable Monitor and Audit** in the Server Configuration page to log audit data, and then configure the JNDI connection to the AuditViewDB data source to view the audit data.

The sample reports use the JNDI connection to fetch data from the data source for auditing. The report layout and data model are pre-designed in the sample reports. You can customize the report layout, but don't change the data model in the sample reports. The sample reports are configured to run as a scheduled job because the size of auditing data can be large. If you want to view an audit report online, select the **Run Report Online** property and make sure you don't select the **Auto Run** property of the report.

1. Download the sample audit reports from the Oracle Analytics Publisher Downloads page.
2. Upload the sample audit reports to a shared folder in the catalog.
3. Schedule the sample audit reports you want to view.
   a. Navigate to the sample audit report in the catalog.
   b. Click **Schedule**.
   c. In the General tab, specify the dates for the **Date From** and **Date To** parameters.
   d. In the Output tab, make sure the output format is PDF.

      You can add delivery destinations if required.
4. After the scheduled job completes, view the report in the Report Job History page.

8

Add Translations for the Catalog and Reports

This topic describes how to export and import translation files both for the catalog and for individual report layouts.

Topics:

About Translation in Publisher

Publisher supports two types of translation: Catalog Translation and Template (or layout) Translation.

Catalog translation enables the extraction of translatable strings from all objects contained in a selected catalog folder into a single translation file; this file can then be translated and uploaded back to Publisher and assigned the appropriate language code.

Catalog translation extracts not only translatable strings from the report layouts, but also the user interface strings that are displayed to users, such as catalog object descriptions, report parameter names, and data display names.

Users viewing the catalog see the item translations appropriate for the UI Language they selected in their My Account preferences. Users see report translations appropriate for the Report Locale that they selected in their My Account preferences.

Template translation enables the extraction of the translatable strings from a single RTF-based template (including sub templates and style templates) or a single Publisher layout template (.xpt file). Use this option when you only need the final report documents translated. For example, your enterprise requires translated invoices to send to German and Japanese customers.

Limitations of Catalog Translation

If you have XLIFF file translations for specific reports and then you import a catalog translation file for the folder in which the existing translations reside, you overwrite the existing XLIFF files.

Translate Templates

You can translate the RTF and Publisher (.xpt) templates from the Properties page.

Template translation includes:

- RTF templates
- RTF sub templates
- Style templates

- Publisher templates (.xpt)

To access the Properties page, click the **Properties** link for the layout in the Report Editor, as shown below.

From the Properties page you can generate an XLIFF file for a single template. Click **Extract Translation** to generate the XLIFF file.

Generate the XLIFF File from the Layout Properties Page

Generate the XLIFF file for report layout templates, style templates, and sub templates.

1. To generate the XLIFF file for report layout templates, perform these steps.
   a. Navigate to the report in the catalog and click **Edit** to open it for editing.
   b. From the thumbnail view of the report layouts, click the **Properties** link of the layout (RTF or XPT) to open the Layout Properties page.
   c. In the **Translations** region, click **Extract Translation**.

      Publisher extracts the translatable strings from the template and exports them to an XLIFF (.xlf file).
   d. Save the XLIFF to a local directory.
2. To generate the XLIFF file for style templates and sub templates, perform these steps.
   a. Navigate to the style template or sub template in the catalog and click **Edit** to open the Template Manager.
   b. In the **Translations** region, click **Extract Translation**.

      Publisher extracts the translatable strings from the template and exports them to an XLIFF (.xlf file).
   c. Save the XLIFF to a local directory.

Translate the XLIFF File

When you download a XLIFF file, it can be sent to a translation provider, or using a text editor, you can enter the translation for each string.

A "translatable string" is any text in the template intended for display in the published report, such as table headers and field labels. Text supplied at runtime from the data is not translatable, nor is any text that you supply in the Microsoft Word form fields.

You can translate the template XLIFF file into as many languages as desired and then associate these translations to the original template.

Upload the Translated XLIFF File to Publisher

You can run the Template Manager to upload the translated XLIFF file to Publisher.

1. Navigate to the report, sub template, or style template in the catalog and click **Edit** to open it for editing.

   For reports only:

   From the thumbnail view of the report layouts, click the **Properties** link of the layout to open the Template Manager.
2. In the Translations region, click the **Upload** toolbar button.
3. In the Upload Translation File dialog, locate the file in the local directory and select the **Locale** for this translation.
4. Click **OK** to upload the file and view it in the Translations table.

Use a Localized Template

You can create localized templates for reports.

If you need to design a different layout for the reports that you present for different localizations, then you can create new RTF file designed and translated for the locale and upload this file to the Template Manager.

The localized template option is not supported for XPT templates.

Design the Localized Template File

Use the same tools that you used to create the base template file, translating the strings and customizing the layout as desired for the locale.

Upload the Localized Template to Publisher

Upload localized template files in rtf format to Publisher.

1. Navigate to the report, subtemplate, or style template in the catalog and click **Edit** to open it for editing.

   For reports only:

   From the thumbnail view of the report layouts, click the **Properties** link of the layout to open the Template Manager.
2. In the Templates region, click the **Upload** toolbar button.

3. In the Upload Template File dialog, locate the file in the local directory, select **rtf** as the Template Type and select the **Locale** for this template file.
4. Click **OK** to upload the file and view it in the Templates table.

9

Frequently Asked Questions for Publisher

This section provides answers to frequently asked questions for configuring and managing Publisher.

Topics:

Top FAQs to Configure and Manage Publisher

The top FAQs for configuring and managing Publisher are identified in this topic.

How do I configure a delivery channel for Publisher?

Use the Publisher administration page to add a connection to a delivery channel and test the connection.

How do I restrict access to delivery channels?

You can configure role-based access for delivery channels. In the delivery channel configuration page, from the **Available Roles** list, select one or more roles you want to provide access to the delivery channel, and add them to the **Allowed Roles** list.

How do I configure FTP and SFTP delivery retry?

If you set the **Enable FTP/SFTP delivery retry** runtime property to true, Publisher makes another attempt to deliver reports to the FTP or SFTP delivery channel, if the first attempt fails.

How can I enable the viewing of audit data in Publisher?

Use the **Enable Monitor and Audit** property in the Publisher Server Configuration page to enable or disable viewing of the audit data of Publisher catalog objects.

How do I upload the configuration-specific files?

Use Upload Center in the Publisher system administration page to upload and manage configuration–specific files for font, digital signature, ICC profile, SSH private key, SSL certificate, and JDBC client certificate.

How do I disable sending mails?

As an administrator, you can stop Publisher from sending mails.

1. In the Publisher Administration page, select the email server connection.
2. Deselect **Public** and remove all the Allowed roles for the email server connection.
3. Click **Apply** to save the changes.

What is the size limit for emails?

15MB is the maximum size of an e-mail message that Oracle.com will accept from the Internet or deliver from Oracle.com. That means the sum of the sizes of message text, headers, attachments, and any embedded images must be less than 15MB.

Which authentication mechanism does Publisher web services support for Oracle Transactional Business Intelligence?

Publisher web services support basic authentication mechanism for Oracle Transactional Business Intelligence.