

PUBLIC

SAP Disclosure Management

Document Version: DM Stack 23xx – 2025-11-10

Administrator's Guide

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

Content

1 Getting Started. . . . 4
1.1 Important SAP Notes. . . . 4
1.2 History of Changes. . . . 5

2 Technical System Landscape. . . . 6

3 Data Protection and Privacy. . . . 7
3.1 Glossary. . . . 7
3.2 Deletion of Personal Data . . . 9
Calling the API Method to Delete Personal Data. . . . 9
3.3 Change Log and Personal Information. . . . 11

4 Monitoring of SAP Disclosure Management. . . . 12
4.1 Users for Support. . . . 12
4.2 How to Cancel Tasks. . . . 13

5 Management of SAP Disclosure Management. . . . 14
5.1 Starting and Stopping. . . . 14
5.2 Software Configuration. . . . 14
Setting Up SAP Fiori for SAP Disclosure Management. . . . 15
5.3 Administration Tools. . . . 16
5.4 Backup and Restore. . . . 17
5.5 Periodic Tasks. . . . 18
5.6 Load Balancing. . . . 18
5.7 Logging on to SAP Disclosure Management for the First Time. . . . 18
5.8 Displaying the Software Version. . . . 18
5.9 System Administration. . . . 19
Role Administration. . . . 19
Business Role Administration. . . . 21
User Administration. . . . 21
Workflow Administration. . . . 26
Entity Administration. . . . 36
Plugin Administration. . . . 38
Report Type Administration. . . . 41
Configuration Files for Content Refresh. . . . 44
Log File Administration. . . . 47
Extended Audit Trail. . . . 48
Authorization Report Administration. . . . 51

System Configuration. 52
Customization of Language Culture Settings. 59
Reports for System Administration. 62
Automatic Removal of Temporary Data. 65
Publishing Packages in SAP Disclosure Management. 66
Authenticating Using Security Assertion Markup Language 2.0 72
Enabling Active Directory Authentication. 81

6 Task Engine. 83

7 High Availability. 85

8 Software Change Mangement. 86
8.1 Transport and Change Management. 86
8.2 Support Packages and Patch Implementation. 86
8.3 SAP Disclosure Management Installation and Migration Tool. 87
Running the Installation Tool. 87
Custom Execution of Installables. 88

9 Troubleshooting. 90

10 Support Desk Management. 91
10.1 Problem Message Handover. 91

11 Appendix. 93
11.1 Service Interfaces for SAP Disclosure Management. 93
Code Samples. 93
Calling the Content Refresh API Method. 97
API Responses for Content Refresh 97
Values Supported for the TimeZone Field When Creating New Users. 98
11.2 Related Information. 101

1 Getting Started

> ⚠ Caution
>
> This guide does not replace the daily operations handbook that we recommend customers to create for their specific production operations.

About this Guide

Designing, implementing, and running SAP Disclosure Management at peak performance 24 hours a day has never been more vital for your business success than now.

This guide provides a starting point for managing SAP Disclosure Management solutions and maintaining and running them optimally. It contains specific information for various tasks and lists the tools that you can use to implement them. This guide also provides references to the documentation required for these tasks, so you will sometimes also need to check other deliverables on SAP Help Portal.

Target Groups

Technical Consultants
System Administrators
Solution Consultants
Business Process Owner
Support Specialists

1.1 Important SAP Notes

> ⚠ Caution
>
> Check regularly to see which SAP Notes are available for this Administrator's Guide.

Important SAP Notes

SAP Note Number	Title	Comments
1621689	Advice for Server Installation of Disclosure Management 10.0	Contains correction for missing database tables after server component installation.

1.2 History of Changes

> ⚠ Caution
>
> Make sure you use the current version of the Administrator's Guide on *SAP Help Portal* at http://help.sap.com.

The following table provides an overview of the most important changes in prior versions.

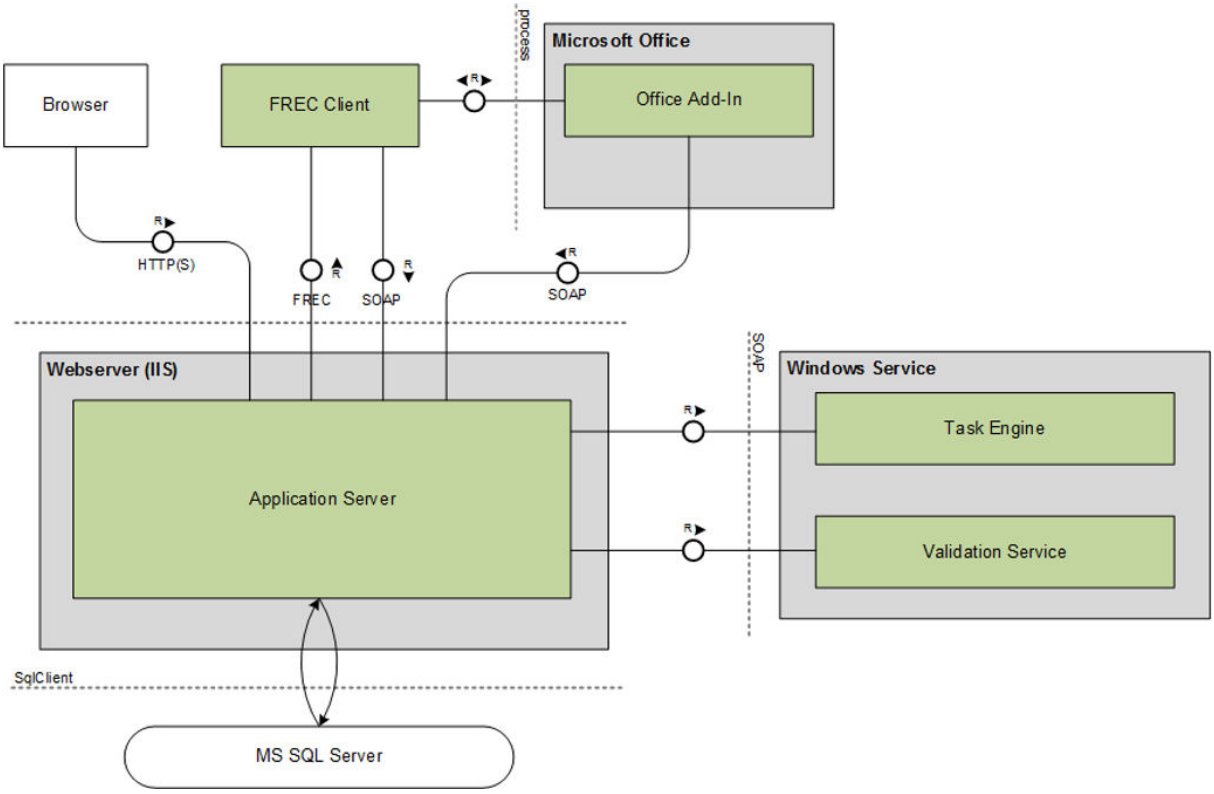
History of Changes

Version	Important Changes
1.0	First version of the SAP Disclosure Management Administrator's Guide

2 Technical System Landscape

The figure below shows an overview of the technical system landscape for SAP Disclosure Management:

For more information about the technical system landscape, see the resources listed in the following table:



Topics	Guide/Tool	Quick Link to the SAP Help Portal
Technical description for SAP Disclosure Management	Inatallation and Upgrade Guide	https://help.sap.com/viewer/p/SAP_DISCLOSURE_MANAGEMENT
Security	See applicable documents	`http://sdn.sap.com/irj/sdn/security`

> **Note**
>
> For a list of the software and hardware requirements for SAP Disclosure Management 10.1 and SAP Disclosure Management XBRL reporting add-ons 1.0, see the SAP Disclosure Management 10.1 Product Availability Matrix (PAM). The Product Availability Essentials presentation also contains information for getting started, and can be found under *General Information* > *Details and Dates* > *Essentials*.

3 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy regulation, it is necessary to consider compliance with industry-specific legislation in different countries. SAP provides specific features and functions to support compliance with regards to relevant legal requirements, including data protection. SAP does not give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, this information does not give any advice or recommendation in regards to additional features that would be required in particular IT environments; decisions related to data protection must be made on a case-by-case basis, under consideration of the given system landscape and the applicable legal requirements.

> ⓘ Note
>
> In the majority of cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion of personal data. SAP does not provide legal advice in any form. Definitions and other terms used in this document are not taken from any given legal source.

3.1 Glossary

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.

Term	Definition
Deletion	The irreversible destruction of **personal data**.
Retention period	The period of time between the end of purpose (EoP) for a data set and when this data set is deleted subject to applicable laws. It is a combination of the residence period and the blocking period.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization (e.g. tax auditors).
Sensitive personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data, data concerning health or sex life or sexual orientation • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts
Residence period	The period of time after the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Where-used check (WUC)	A process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.

3.2 Deletion of Personal Data

This function is used to delete personal data that is stored in SAP Disclosure Management.

It modifies user, report, and chapter data, to remove personal data that belongs to a specific user. For this functionality, an API in available.

To call the API method, you have to set the parameters `UserLogin` or `PeriodName`.

To run the method, Microsoft PowerShell may be used and for scheduled runs, the standard Windows task scheduler may be used.

- If you only set the `UserLogin` parameter, the master data of that user is removed and the account is deactivated. All local and global permissions for that user will be removed. Fiori Launchpad business roles are also deleted. The audit trail entries for the user will also be removed.
- If you set the `PeriodName` parameter, the user master data is untouched, because it is needed for the remaining periods. All local permissions will be removed for this period's reports and chapters. The audit trail entries of the user for the specified period will also be removed.

The chapter history, revisions, and general values of the period will be removed in both cases.

To delete multiple periods or users, you have to run the API call multiple times.

> ⓘ Note
>
> The removal of personal data is not reversible. Use with caution.

3.2.1 Calling the API Method to Delete Personal Data

Prerequisites

The permission object *Delete Personal Data* must be assigned to the authenticated user. The API call first checks the permission of the user, then validates the two parameters and runs the SQL Stored Procedure, which actually removes the data.

After the method has run successfully, the action is written into the audit trail event log.

Procedure

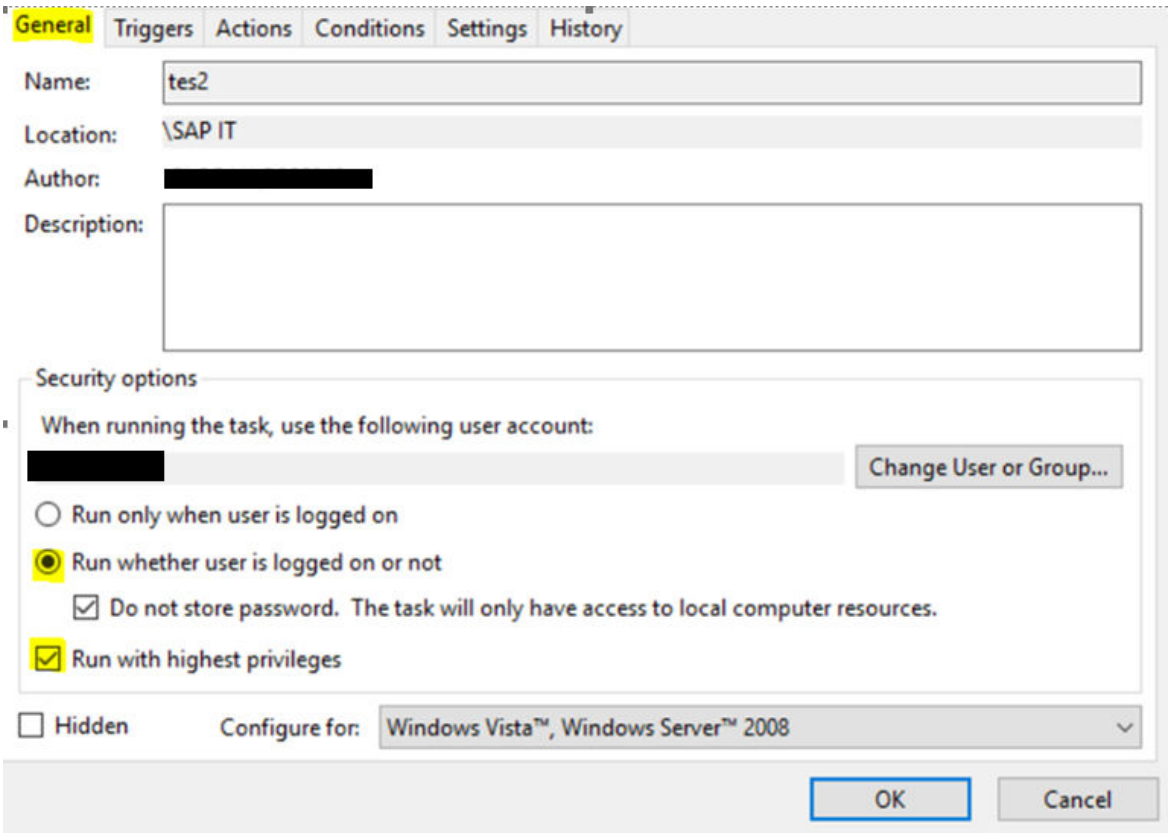
1. Run the MS PowerShell script without any arguments set as shown below:

Sample Code

```
$system = 'http://localhost:8080'
$user = 'AdminLogin'
$pw = "password"
$params = @{username=$user;password=$pw} | ConvertTo-Json
$response = Invoke-WebRequest $system/api/Authenticate -method Post -body
$params
if($response.statuscode -ne 200){
        "Error: $($response.statuscode)"
      exit;
} else {
        $at = $response.headers.access_token
        "authorization token obtained"
}
$response = ""
$params1 = @{"access_token" = $at;"Content-type" = "application/
json";"Accept-Language" = "en-EN" }
$params2 = @{UserLogin='User1'} | ConvertTo-Json
$response = Invoke-WebRequest $system/api/DeletePersonalData -headers
$params1 -method Post -body $params2
if($response.statuscode -ne 200){
        "Error: $($response.statuscode)"
      exit;
} else {
        "anonymization done"
}
```

The script first authenticates the user. If this succeeds, the generated access token is used to call the method using the `UserLogin` or `PeriodName` parameter.

2. To schedule the run, maintain the Microsoft PowerShell script using the Windows task scheduler:



The *Actions* tab defines the PowerShell scripts, which call the API, and the

Triggers tab defines the scheduled date of the run.

3.3 Change Log and Personal Information

In SAP Disclosure Management personal data is handled as follows:

Personal Information

You can view and modify your basic personal data by clicking your name on any page of the web application. In addition, with specific permission, administrators can create a complete Audit Trail Log, which shows personal data based on a your actions in the system.

Change Logging

SAP Disclosure Management supports change logging of personal data.

How to Fulfill a Data Subject Access Request

The following steps provide guidance on how to fulfill a data subject access request according to EU GDPR Section 2 "Information and access to personal data", Article 15 "Right of access by the data subject":

- End user: Create a data subject access request (DSAR) for your user - either by creating a ticket or via email to your data controller.
- Admin user with *View Audit Trail* permission:
  1. Go to *Security* > *Audit trail events log*.
  2. Select the period you require the user data for / the user is working with the application.
  3. Download the audit trail log.
  4. Open the downloaded file and in the *Object* column, filter for the user's login name, that is *Loginname*.
  5. Copy the filtered rows into a new MS Excel workbook that is specific to the user.
  6. Provide the user-specific workbook to the user.

Related Information

Extended Audit Trail [page 48]

4 Monitoring of SAP Disclosure Management

Within the management of SAP Technology, monitoring is an essential task. For the monitoring of SAP Disclosure Management, you can create administration users on the various servers. In SAP Disclosure Management, the system administrator can analyze system errors using log files.

Related Information

Users for Support [page 12]
Log File Administration [page 47]

4.1 Users for Support

A user, who performs monitoring and diagnostic services, requires only minimal access to SAP Disclosure Management data. Therefore, it may be advisable to create a user with minimal access rights - particularly for remote monitoring and diagnosis.

The following users are recommended for the monitoring of SAP Disclosure Management:

- Administration user for Microsoft Windows Server
  For more information, see the Microsoft product documentation.
- Administration user for Microsoft Windows SQL Server
  For more information, see the Microsoft product documentation.
- Administration user for SAP Disclosure Management
  Only the *Standard Admin* role shall be assigned to this administration user. For more information about the standard roles, see the section “Authorizations” in the *SAP Disclosure Management Security Guide*. For more information about user creation, see User Administration [page 21].

4.2 How to Cancel Tasks

Context

The admin user can cancel any task with processing status *New*. Users can only cancel the tasks that they have created.

Procedure

1. In SAP Disclosure Management, select the *Monitoring* tab.
2. Select *Task Monitor*.
3. Select the task or tasks that you want to stop. Note that you can only cancel tasks with status *New*.
4. Choose *Cancel*.

5 Management of SAP Disclosure Management

SAP provides you with an infrastructure to help your technical support consultants and system administrators effectively manage all SAP components and complete all tasks related to technical administration and operation.

5.1 Starting and Stopping

The Stop Sequence is in reverse order to the Start Sequence.

Start and Stop Sequences and Tools

Software Component	Sequence	Tool	Detailed Description
SAP Disclosure Management BW connector	Not applicable	Handled by the SAP NetWeaver platform	For more information, see the section "Installation of SAP Disclosure Management BW Connector" in the *SAP Disclosure Management Installation Guide*.
XBRL validation service	Not applicable	Handled by the Microsoft Windows platform (standard Microsoft Windows service)	For more information, see Periodic Tasks [page 18].
SAP Disclosure Management application	Not applicable	Handled by the Microsoft IIS platform	Only the standard IIS service must be started.
Task engine service	Not applicable	Handled by the Microsoft Windows platform (standard Microsoft Windows service)	For more information, see *Starting the Task Engine* in the SAP Disclosure Administrator´s guide.

5.2 Software Configuration

This chapter explains which components or scenarios used by this application are configurable and which tools are available for adjusting.

Software Configuration

Component	Configuration Tool(s)	Detailed Description
SAP Disclosure Management BW connector	SAP Web Application Server configuration tools	Technical configuration of the connector For more information, see the section "Installation of SAP Disclosure Management BW Connector" in the *SAP Disclosure Management Installation Guide*.
SAP Disclosure Management server	Web browser user interface (*Administration* tab)	For more information, see System Administration [page 19] and especially System Configuration [page 52].
SAP Disclosure Management client	Graphical user interface	Configuration of data sources For more information, see the section "Configuration of Data Source Connections" in the *SAP Disclosure Management Installation Guide*.
Interstage XWand Toolkit by Fujitsu	Interstage XWand allows you to create, review, modify, validate, and convert XBRL taxonomies and instances.	For more information, see the latest Interstage XWand Toolkit documentation, which is provided on the Support Portal together with the SAP Disclosure Management software.

5.2.1 Setting Up SAP Fiori for SAP Disclosure Management

Context

To enable user authentication for the SAP Fiori Launchpad on the server where DM APPLICATION SERVER 10.1 runs you can use one of the following:

- the default certificate
- an enterprise certificate
- a self-signed certificate

- The default certificate has already been installed during the setup procedure. The name of this certificate is `APIDisclosureManagement`. This is the default setting after you have installed the DM APPLICATION SERVER 10.1.The configuration section is not visible under the tag `applicationSettings`. You do not have to configure anything else.
- SAP recommends that you use an enterprise certificate for Fiori with DM APPLICATION SERVER 10.1. To use this type of certificate, you have to create a new entry under the section `applicationSettings`:

Sample Code

```
</cundus.enterpriseReporting.Web.Properties.Settings>
  <applicationSettings>
    <cundus.enterpriseReporting.Web.Properties.Settings>
      <setting name="ApiLocalDMCertificateIssuerName" serializeAs="String">
        <value>CN VALUE OF YOUR ENTERPRISE CERTIFICATE</value></
setting>
</cundus.enterpriseReporting.Web.Properties.Settings>
```

The value represents the certificate issuer (CN value) of the enterprise certificate.

- SAP recommends that you use the PowerShell command `New-SelfSignedCertificate` to generate self-signed certificates.

Caution

Use a self-signed certificate only for development, not production.

Sample Code

```
## Replace {certificateName} and {dnsHostname}
New-SelfSignedCertificate -Subject "{certificateName}" -DnsName
"{dnsHostname}" -CertStoreLocation "Cert:\LocalMachine\My"
-KeyExportPolicy Exportable -KeySpec Signature -KeyLength 2048
-KeyAlgorithm RSA -HashAlgorithm SHA256
```

To use a self-signed certificate for Fiori, you have to create a new entry under the section `applicationSettings`.

Sample Code

```
  <applicationSettings>
    <cundus.enterpriseReporting.Web.Properties.Settings>
      <setting name="ApiLocalDMCertificateIssuerName" serializeAs="String">
        <value>SelfSignedDisclosureManagement</value></setting>

    </cundus.enterpriseReporting.Web.Properties.Settings>
```

5.3 Administration Tools

Available Administration Tools

Software Component	Transaction/Tool	Detailed Description
SAP Disclosure Management BW connector	SAP NetWeaver standard tools	For more information, see the section “Installation of SAP Disclosure Management BW Connector” in the *SAP Disclosure Management Installation Guide*.

Software Component	Transaction/Tool	Detailed Description
SAP Disclosure Management server	Web browser interface and configuration files	For more information, see System Administration [page 19] and especially System Configuration [page 52].
SAP Disclosure Management client	Graphical user interface	For more information, see the section "Configuration of Disclosure Management in a Microsoft Office Application" in the *SAP Disclosure Management User Help*.

5.4 Backup and Restore

You need to back up your system landscape regularly to ensure that you can restore and recover it in the case of a failure. The backup and restore strategy for SAP Disclosure Management consists of two parts:

- Backup and restore coverage for each component (see table below)
- Cross-system data dependencies and handling

The backup and restore strategy for your system landscape should not only consider SAP systems but also be embedded in overall business requirements and incorporate your company's entire process flow.

In addition, the backup and restore strategy must cover disaster recovery processes, such as the loss of a data center through fire. It is most important in this context that you ensure that backup devices are not lost together with normal data storage (separation of storage locations).

Backup and Restore Coverage

Component	Data to Be Backed up	Backup Method/Tool	Recommended Backup Frequency	Backup Sequence (If Required)
SAP Disclosure Management BW connector	Definition of Briefing Books	Category: XI SAP Web Application Server	Monthly	Not applicable
SAP Disclosure Management server	Definition of reports and content Replicated data	Category: X Microsoft SQL Server/ file copy	Daily	Not applicable
SAP Disclosure Management client	Configuration files	Category: II File copy	Monthly	Not applicable

5.5 Periodic Tasks

There are no required scheduled or manual periodic tasks.

The standard Microsoft Windows service XBRL validation service, which validates XBRL files, must run continuously and the task engine service, which executes long-running tasks.

You can start or restart these services automatically or manually.

5.6 Load Balancing

Load balancing of SAP Disclosure Management is based on the infrastructure of Microsoft Windows Server and Microsoft SQL Server. For more information, see the Microsoft product documentation.

5.7 Logging on to SAP Disclosure Management for the First Time

Procedure

1. In a Web browser, enter the address of SAP Disclosure Management in the address bar in one of the following forms:
   - Enter the host name.
   - Enter the TCP/IP number, for example, **`172.55.1.123`**.
2. To confirm the address, press [`Enter`].
   The system displays the logon page of SAP Disclosure Management.
3. In the *Name* field, enter your user ID.
4. Enter your password.
5. Click *Login*.

5.8 Displaying the Software Version

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *About*.
   The number of the version and the build information appears.

5.9 System Administration

The *Administration* tab represents the start screen to customize and configure the system settings. This tab is normally reserved for system administrators.

On this tab, you can perform the following tasks:

- Design, create, edit, and validate workflows.
- Define legal entities for XBRL reporting and as authorization objects.
- Select output formats.
- Define the content and output types for reports.
- Configure the settings for the update of datalinked objects in a chapter and report document.
- Display daily error logs.
- Customize system-wide configuration settings.
- Determine language settings for report output.

5.9.1 Role Administration

A role determines a user's rights. A role is a summary of several rights saved under a specific name or as a level of authorization. A user can possess none or all of the already specified roles.

When clicking the *Security* tab you can:

- Create and assign roles to users.
- Create and assign rights to roles.

SAP Disclosure Management offers the following roles:

- Standard Admin - Administers the system.
- Standard Manager - Manages and edits reports.
- Standard Editor - Can only edit chapters.
- Standard Read only - Can only read reports and chapters.
- Standard Transporter - Imports and exports content

> ⚠ Restriction
>
> You cannot delete roles used in the master data settings of users.

For more information, see the section “Authorizations” in the *SAP Disclosure Management User Help*.

5.9.1.1 Creating Roles

Procedure

1. In SAP Disclosure Management, click the *Security* tab.
2. Click *Roles*.
   A list of existing roles appears. Use the icons at the bottom of the list to switch between pages, if necessary.
3. Click *New role*.
4. On the *Roles* tab, enter a *Name* for the role.
   You can enter a *Description*.
5. On the *Permissions* tab, select the *Granted* checkbox for those rights that you want to assign to the role.
6. To save the role, click *OK*.

5.9.1.2 Editing Roles

Procedure

1. In SAP Disclosure Management, click the *Security* tab.
2. Click *Roles*.
3. Select the role you want to edit. Use the icons at the bottom of the list to switch between pages, if necessary.
4. Click *Edit role*.
5. On the *Roles* tab, you can change the name and the description.
6. To change the role rights, click the *Permissions* tab.
7. You can change the rights.
8. To save the changes, click *OK*.

5.9.1.3 Deleting Roles

Procedure

1. In SAP Disclosure Management, click the *Security* tab.
2. Click *Roles*.
3. From the list of roles, select the role you want to delete. Use the icons at the bottom of the list to switch between pages, if necessary.
4. Click *Delete role*.
5. In the *Confirm* dialog box, click *OK*.

5.9.2 Business Role Administration

.

To access apps in the SAP Disclosure Management (SAP DM) Launchpad, you must assign users to business roles. Each business role corresponds to one app. Business roles are predefined and cannot be changed by customers.

To launch and see apps, users must be assigned to business roles.

The activities users can carry out with the app depend on permissions that have been assigned to them based on the SAP Disclosure Management role and permission concept (see also the chapter *Role Administration*). Hence, activities that users are allowed to perform in an app are consistent with what they are allowed to do in the rest of SAP DM.

For more information on the assignment of business roles, see the chapter *Assignment of Business Roles* in the user guide.

5.9.3 User Administration

To grant rights to users in SAP Disclosure Management, you assign them to roles. If you assign a role in the user's master data, this role and its related rights apply globally. If you assign a role on report or chapter level, this role and its related permissions apply locally. A user can own global and local rights in any kind of combination, for example, it is possible for a user to have local rights, but no global rights. You can also assign users to an entity to restrict their access only to reports created for this entity. Local users need the global permission *Local Permisison* for the entity of this report.

For more information about authorizations in SAP Disclosure Management, see the section “Authorizations” in the *SAP Disclosure Management User Help*.

> ⚠ Restriction
>
> You cannot delete users; you can only deactivate the user ID. You can also anonymize existing users. For more information, see Deletion of Personal Data [page 9].

User list design

The list of available users comprises the following columns:

- *User name* - Displays the user ID.
- *Last name* - Displays the last name of the user.
- *First name* - Displays the first name of the user.
- *Time zone* - Displays the time zone the user is assigned to.
- *Active* - Displays the status of the user.

5.9.3.1 Creating Users

Prerequisites

- Verify that the user ID does not exist on the system.
- Determine the name, e-mail, roles, and entities to assign to the user.

Procedure

1. In SAP Disclosure Management, click the *Security* tab.
2. Click *Users*.
3. Click *New User*.
4. On the *User* tab, enter the *user name*.
   This will be the new user ID.
5. Enter the user's first and last name.
6. Enter an initial password, then re-enter the password for *password confirmation*.
7. Enter the user's e-mail account.

   The e-mail account is important for workflow notifications.
8. You can enter a *Description*.
9. If, for example, the user will start work at a later date, clear the *Active* check box.
10. Do one of the following:
    - To assign roles, click the *Roles* tab and assign one or more roles to the new user account.
    - To assign entities, click the *Entities* tab and assign one or more entities to the new user account. This restricts access only to reports that belong to the selected entities.
11. To save the user account, click *OK*.

5.9.3.2 Creating Users with SAML Authentication

Context

If you use SAML authentication you can select either Basic Authentication or AD Authentication. SAML authentication as a global setting. It overrides the default selected authentication method.

Procedure

1. Enter the user name. This will be the new user ID.
2. Enter the user's first and last name.
3. Enter the incoming user identifier. This is the combination of the definedSAMLUserIdentifier from the Web.config file and the corresponding value thatcomes from the Identity Provider, for example [email=surname.lastname@domain.com].
4. Enter the outgoing user identifier. This is the identifier that will be sent to a BW data source during the authentication process. If you leave this field empty, the value from the Identity Provider will be sent, for example [email=surname.lastname@domain.com].
5. Enter the user's e-mail account. The user's e-mail account is important for workflow notifications.
6. Save your entry.

5.9.3.3 Editing Users

Procedure

1. In SAP Disclosure Management, click the *Security* tab.
2. Click *Users*.
3. From the list of users, select the user whose settings you want to edit.
4. Click *Edit user*.
5. Apply changes as necessary.
6. To save the changes, click *OK*.

5.9.3.3.1 Resetting User Passwords

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Users*.
3. From the list of users, select the user whose password you want to reset.
4. Click *Edit user*.
5. Click the *User* tab.
6. On the *User* tab, enter a *password*, then re-enter the password for *password confirmation*.
7. To save the changes, click *OK*.

5.9.3.3.2 Reactivating Users

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Users*.
3. Select the user for whom you want to edit the settings.
4. Click *Edit user*.
5. Click the *User* tab.
6. On the *User* tab, enter an initial *password*, then re-enter the password for *password confirmation*.
7. A count of the current consecutive failed login attempts are shown below the *Active* checkbox. If a user has reached the Setting up Company Information [page 55] failed login attempts, their user account will be disabled.
8. To activate the user, select the *Active* checkbox.
9. To save the changes, click *OK*.

5.9.3.4 Searching for Users

Context

Instead of using the paging feature to navigate to a specified user, you can also search for users by user name, first name, last name, or both, by using the *Search for User* field. Alternatively you can press ENTER to initiate an immediate search.

- The search is not limited, so you can use multiple search terms.
- The search uses an AND combination of all terms.
- Search terms can be split by one ore more blanks.
- You do not need to type terms in full, for example, you can enter x to find *Max*, *Xaviar*, and *Mr. Xavi*.
- Search results can also be used with the Entity filter selected.

The number of matches found and the filtered user list are displayed. Paging and filtering for entities is also possible.

Procedure

1. In SAP Disclosure Management, choose *Security* > *Users*.
2. Search for a user by paging the screen or by using the *Search User* field at the top right of the screen.

3. Either press ENTER to start the search or wait until the system displays the search result.

5.9.3.5 Deactivating a User

Prerequisites

You can only use this function if the authentication type of the user is *Basic Authentication*.

Procedure

1. In SAP Disclosure Management, click the *Security* tab.
2. Click *Users*.
3. From the list of users, select the user you want to deactivate.
4. Click *Deactivate user*.
5. In the *Confirm* dialog box, click *OK*.

5.9.3.6 Creating an Emergency User

Prerequisites

- A user with the permissions `Configure System` and `Define Roles and Workflows` to create a role for emergency users.
- A user with the permissions `Configure system` and `Define Users` to create an emergency user.

Set Role for Emergency Users Only

To create an emergency user, you need a role that can only be used for emergency users. To do so, open or create a role under the section *Security/ Role* and select the checkbox *Only for Emergency User*. This role can also be used for other emergency users.

It is recommended that you provide the user with sufficient permissions to fulfill the requested tasks. Once the role has been assigned to an emergency user, it can no longer be changed. The active status can no longer be changed either.

To create an emergency user, you need the above permissions and an emergency user role. Open the section *Security / User* and use the filter *Emergency User*.

An emergency user can only be created with basic authentication. The selected role is assigned globally for 'Any Entity' and 'Group'.

Select the role and click *Create*. Once you have created the emergency role, the credentials are displayed once. They must be copied and kept safe together with Machine Secret and CryptoKey from the `web.config` file in the installation folder. If SAML has been enabled, you must disable it to use the emergency user.

The emergency user is unrecognizable as long as it has not been used. As such, it cannot be deactivated either. As soon as the emergency user has logged in for the first time, it becomes visible in the system and can be deactivated. Otherwise, an emergency user cannot be edited or even reactivated.

5.9.4 Workflow Administration

A workflow in SAP Disclosure Management describes the standard life cycle of a report, including the report phases, whicht starts with the creation of the report structure, continues with the update of chapter documents, and terminates with the finalization of the consolidated report content. A workflow is a mandatory characteristic of a report and its chapters.

The workflow contains steps, which are assigned to step statuses. These step-related statuses describe the standard life cycle of a document. For more information about the workflow concept in SAP Disclosure Management, see the section “Workflows” in the *SAP Disclosure Management User Help*.

Workflows are usually designed by subject matter experts (SME). We recommend that administrators have workflows approved by the SMEs and test a workflow in the test environment before installing it in the production system of SAP Disclosure Management.

> ⚠ Restriction
>
> You cannot edit or delete active workflows that are used in reports.

The list of workflows comprises the following columns:

- *Name* - Displays the name of the workflow.
- *Description* - Displays a description of the workflow.
- *System* - Displays *Yes* if the workflow is the system default workflow.
- *Active* - Indicates the workflow status.
- *Outdated* - Outdated: Indicates that a workflow can be set out of date to prevent further use for reports and chapters.

5.9.4.1 Creation of Workflows in SAP Disclosure Management

To create workflows in SAP Disclosure Management, you need knowledge of workflows in the application and workflows approved by SMEs.

You can create a workflow by copying an existing one or by creating it from scratch. From a technical point of view, the easiest way to create the mandatory elements of a workflow is to set up the workflow steps, and then

the activities for the step transitions and the conditions for the activities. Conditions at the step level are not mandatory and therefore handled in the help section related to the configuration of workflows.

Once you have saved your finished workflow, you can test the activities in the production environment, but we recommend that you test the workflow in a test environment to guarantee that the workflow is valid.

5.9.4.1.1 Creating a Workflow from Scratch

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
3. Click *New workflow*.
4. Enter a *Name*, preferably one that refers to the method of approval used in the workflow.
5. Click *OK*.
6. Create the mandatory workflow elements following the instructions in the following sections.
7. To create the workflow steps, do the following:
   a. On the *Steps* tab, click *New step*.
   b. Enter a *Name* for the step.
   c. In the *Linked status* list, click a status for the step and click *OK*.

      The *Activities* tab appears. Ignore this panel for now and create the steps for your workflow.
   d. In the navigation header line, click *Steps* and repeat the previous steps until you have created all your workflow steps.
   e. To display the workflow's general settings, click the *Workflow* tab.
   f. In the *Start step* list, click the first step of your workflow.

      This step is the starting point.
   g. In the *End step* list, click the step that terminates your workflow.
   h. To save the entries, click *OK*.
8. To create the workflow activities, do the following:
   a. On the *Steps* tab, click the start step in the list.
   b. Click *Edit step*, then click the *Activities* tab.
   c. On the *Activities* tab, click *New activity*.
   d. On the *New Activity* tab, enter a *Name*.
   e. In the *Next step* list, click the step to be triggered by the activity.

      This step is the starting point.
   f. In the *End step* list, click the step that terminates your workflow.

      > **Note**
      >
      > These settings are required. You need at least two steps to create an activity. If you do not have any items in this list, you may have only one step in the workflow.

   g. To require a user to add a comment when executing the activity, select the *Comment required* checkbox.

h. To save the changes, click *OK*.
i. In the navigation header line, click the *Steps* link and repeat the previous steps for all workflow steps.

9. To create an activity condition, do the following:
   a. On the *Steps* tab, select the step for which you want to set an activity condition.
   b. Click *Edit step*.
   c. On the *Activities* tab, select an activity and click *Edit activity*.
   d. Click the *Conditions* tab.
   e. Click *New condition*.
   f. On the *Condition* tab, select one of the following *User needs* for executing the activity:
      - Click *Role*, then in the value list, click the role the user must have.
      - Click *Permission*, then click a right the user must have.
   g. To save the changes, click *OK*.
   h. Optionally, in the navigation header line, click *Conditions*, then the *Conditions* tab to define a second condition for the selected activity, or the *Steps* tab to define the condition details of the next activity.

Related Information

Testing Workflow Activities in Foreground [page 34]
Setting Access Rights on Workflow Steps [page 32]
Adding Flowcharts to a Workflow [page 33]

5.9.4.1.2 Creating Workflows from an Existing Workflow

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
3. Select the workflow you want to use to create a workflow.
4. Click *Copy workflow*.
5. On the *Copy workflow* tab, in the *New name* field, enter a name for the new workflow.
6. Click *Copy*.
7. Select the new workflow and click *Edit workflow*.
8. When you have finished updating the settings, for example, *Start step* and *End step*, click *OK*.

Next Steps

Next steps:

- To ensure that the workflow has been set up correctly, validate the workflow.
- When the workflow is validated and you want to use it in a report, you must activate the workflow.

Related Information

Modifying Workflow Steps, Activities, and Conditions [page 31]
Creating a Workflow from Scratch [page 27]
Validating a Workflow in Background [page 29]
Activating Workflows [page 29]
Setting Access Rights on Workflow Steps [page 32]

5.9.4.1.3 Validating a Workflow in Background

Prerequisites

None of the workflows are in edit mode.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
3. Select a workflow.
4. Click *Validate workflow*.

   > **Note**
   >
   > If the *Validate workflow* button does not appear, one or more workflows are in edit mode.

   The background check can take some minutes. If the system detects no errors, it displays an information message that the workflow has been validated. If the system detects errors, it lists the errors.

5.9.4.1.4 Activating Workflows

Prerequisites

The workflow has been validated.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
   In the list of workflows, the entry in the last column indicates whether the workflow is active.
3. Select a workflow and click *Edit workflow*.
4. On the *Workflow* tab, click *Activate workflow*.
   Any errors are listed at the top of the workflow panel. If the activation is successful, the system returns to the initial screen with the workflow list and displays an information message that the workflow has been activated. The entry in the last column of the overview list displays *Yes*.

Related Information

Validating a Workflow in Background [page 29]

5.9.4.2 Configuring Workflows

SAP Disclosure Management allows each kind of workflow component such as steps, activities, and conditions to be changed and deleted. The tasks defined in this section are optional.

> ⓘ Note
>
> When you delete components, you should always validate the workflow to ensure that it is still valid from a technical point of view.

You can add conditions at the step level of a workflow, which determine the user's ability to edit documents. For example, if you want to allow *Standard Editors* to edit documents and *Standard Managers* to activate step transitions, you can create an *Edit Chapter* condition at the step level and an *Edit Report* condition at the activity level.

> ⓘ Note
>
> Before you can edit or delete a workflow, you must deactivate it. You can only deactivate workflows that are not used in reports.

5.9.4.2.1 Deactivating Workflows

Prerequisites

The workflow is not started in a report.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
3. Select the workflow to be deactivated, and click *Edit Workflow*.
4. On the *Workflow* tab, click *Deactivate*.
5. In the *Confirm* dialog box, click *OK*.

   The system checks whether the workflow is started in a report. This can take some minutes. If the workflow is still in use and cannot be deactivated, an error message appears.

   1. Click *Test workflow*. The *Workflowtest* dialog box appears.
   2. To display the reports that use the workflow, click *Where-used list*.

   If the workflow has not started, the system displays an information message that the workflow has been deactivated. The last column in the overview list displays *No*.

Results

> **Note**
>
> To reset the workflow to the open status, click *Reload*.

5.9.4.2.2 Modifying Workflow Steps, Activities, and Conditions

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
3. Select a workflow to edit.
4. Click *Edit workflow*.
5. Click the *Steps* tab.
   An overview of all existing steps appears.
6. To delete a step, do the following:
   a. Select the step from the workflow.
   b. Click *Delete step*.
   c. Verify that the revised transitions for the predecessor and subsequent steps work correctly.
   d. If you want to edit existing settings, click *Edit step*.
7. To delete an activity, do the following:
   a. Select the step with the activity you want to delete.

b. Click *Edit step*.
c. Click the *Activities* tab.
d. On the *Activities* tab, select the activity you want to delete and click *Delete activity*.
e. In the *Confirm* dialog box, click *OK*.
f. To return to the workflow's tab, click the  home icon.
g. To ensure that the workflow is technically complete, select the workflow and click *Validate workflow*.

8. To delete a condition, do the following:
   a. Select the step with the conditions you want to delete.
   b. Click *Edit step*.
   c. To delete an activity condition, do the following:
      1. On the *Activities* tab, select the required activity, and click *Edit activity*.
      2. On the *Conditions* tab, select the condition you want to delete, and click *Delete condition*.
      3. In the *Confirm* dialog box, click *OK*.
      4. To return to the workflow overview, click the  home icon.
      5. To ensure that the workflow is technically complete, select the workflow and click *Validate workflow*.
   d. To delete a step condition, do the following:
      1. On the *Conditions* tab, select the condition you want to delete and click *Delete condition*.
      2. In the *Confirm* dialog box, click *OK*.
      3. To return to the workflow overview, click the  home icon.
      4. To ensure that the workflow is technically complete, select the workflow and click *Validate workflow*.

Related Information

Creating a Workflow from Scratch [page 27]

5.9.4.2.3 Setting Access Rights on Workflow Steps

Prerequisites

The workflow is not used in reports and has been deactivated.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.

2. Click *Workflow*.
   In the workflows list, the last column indicates whether the workflow is active.
3. Select a workflow.
4. Click *Edit workflow*.
5. On the *Steps* tab, select the required step, and click *Edit step*.
6. On the *Conditions* tab, click *New condition*.
7. On the *Condition* tab, select one of the following *user needs* for executing a specified action on step level:
   - To select a user role, select the *Role* radio button.
   - To select a specific right, select the *Permission* radio button.

   > **Note**
   >
   > The *Value* list options are determined by the selected condition.
8. Select an activity from the *Activity* list.
9. To save the changes, click *OK*.
10. Do one of the following:
    - To define a second condition for the selected step, click the *Conditions* tab.
    - To return to the step overview and define the details of the condition of the next step, in the navigation header line, click *Steps*.

Related Information

Deactivating Workflows [page 30]

5.9.4.2.4 Adding Flowcharts to a Workflow

Prerequisites

The workflow is not in any reports and is deactivated.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
   In the list of workflows, the last column indicates whether the workflow is active.
3. Select a workflow.
4. Click *Edit workflow*.
5. On the *Workflow* tab, below the *Image* area, click *Browse*.

6. In the *Choose File to Upload* dialog box, navigate to and select the file, and click *Open*.
   Allowed file formats are JPG, GIF and PNG. The required directory is entered in the *File* field.
7. Click *Add picture*, then *OK*.

Results

> **Note**
>
> You cannot delete the flowchart. To remove the flowchart, upload a file with a white background or a file saying “No flowchart available”.

Related Information

Deactivating Workflows [page 30]

5.9.4.2.5 Testing Workflow Activities in Foreground

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
   The system displays a list of existing workflows.
3. Select a workflow.
4. Click *Edit workflow*.
5. On the *Workflow* tab, click *Test workflow*.
   The test starts with the first step of the workflow and its related activities. In the *Workflowtest* dialog box, the system lists for each activity the step that it triggers, the required conditions, and whether a comment is required.
6. Click an activity link.
   The system loads the settings of the triggered step.
7. Continue to run through the workflow steps by clicking the appropriate links.
8. To finish the test and return to the *Workflow* tab, click *Close*.

> **Caution**
>
> The test does not validate the workflow.

Related Information

Validating a Workflow in Background [page 29]

5.9.4.2.6 Checking Use of Workflows in Reports

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
   The system displays a list of existing workflows.
3. Select a workflow.
4. Click *Edit workflow*.
5. On the *Workflow* tab, click *Test workflow*.
6. In the *Workflowtest* dialog box, click *Where-used list*.
   The search can take a few minutes.The system displays the following:
   - A list of reports that use the workflow
   - The period each report belongs to
   - Whether the workflow is used at the chapter level
   - The status of the workflow
7. To close the dialog box and return to the *Workflow* tab, click *Close*.

5.9.4.2.7 Deleting a Workflow

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Workflow*.
   The system displays a list of existing workflows.
3. Select the workflow you want to delete.
4. Click *Delete workflow*.
5. In the *Confirm* dialog box, click *OK*.

Results

The system checks whether the workflow is used by a report. If the workflow is not used, the system displays an information message that the workflow has been deleted. If the workflow is used, the system displays the reports that use the workflow. You must delete the reports first, and then delete the workflow.

5.9.5 Entity Administration

Entities are the legal entities of a group or holding, which not only provide data for group reporting but also produce reports for local reporting purposes.

The use of entities in the framework of XBRL reporting facilitates the data exchange between groups and their members. SAP Disclosure Management allows you to copy group reports (such as the report and chapter structure) to one or more entities in one step.

Once entities are set up on the system, they can be used for access purposes. To avoid users having access to the reports of other group entities, you can assign users to only the entity they work for, and even allow access only to reports created for these entities.

> **Note**
>
> You cannot delete entities that are used by reports.

The entity list comprises the following columns:

- *Name* - Displays the name of the entity.
- *Specific ID* - Displays the unique identifier assigned to the company within the group.
- *XBRL company code* - Displays the official identification code for XBRL reporting to regulators, for example, the NYSE security identification number for SEC reporting.

5.9.5.1 Adding Entities

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Entities*.
   A list of existing entities appears.
3. Click *New Entity*.
4. On the *New Entity* tab, in the *Name* field, enter the legal company name.
5. In the *Specific ID* field, enter the group-specific identifier of the company.
6. In the *XBRL Company Code* field, enter the official external identifier of the company for XBRL reporting.
7. To save the entity, click *Add*.

5.9.5.2 Editing Entity Master Data and Displaying Usage Details

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Entities*.
3. On the *Entities* tab, select an entity.
4. Click *Edit entity*.
5. On the *Edit entity* tab, depending on whether you change the settings or display the usage of the entity, do the following:
   - On the entity's main tab, update the name and ID, as necessary.

     > **Note**
     >
     > You cannot use just any XBRL-related code. You must use an assigned code.

   - To display users assigned to an entity, click the *Users* tab.
     The screen displays all users assigned to the entity. The system lists the general settings such as the name, time zone, roles, and whether the user is activated for each user.

5.9.5.3 Deleting Entities

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Entities*.
3. Select the checkbox of the entity you want to delete.
4. Click *Delete entity*.
5. In the *Confirm* dialog box, click *OK*.

5.9.5.4 Importing Entity Structures

Prerequisites

- A valid CSV file must consist of one worksheet with three columns, which list the name, ID, and XBRL company code of each entity.
- The columns shall not have a header row.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Entities*.
   A list of existing entities appears.
3. To navigate to the CSV file, on the *Import* tab, click *Browse*.
4. Select the appropriate file, and click *Open*.
   The system closes the dialog box and the required directory is entered in the *File* field.
5. To upload the file into the application, click *Import*.
   The system displays an information message that the file has been successfully uploaded.

5.9.6 Plugin Administration

In order to generate or preview a report, you need a plugin to render data. You can download default plugins from SAP Support Portal (https://support.sap.com) and upload them to SAP Disclosure Management.

You can also design your own plugins and upload them to SAP Disclosure Management.

The plugin types listed below are also supported:

Plugin Type	Description
Renderer	Plugin is used by SAP Disclosure Management server to create reports
RenderAndExtend	Plugin is used by SAP Disclosure Management server to create, validate, and submit reports
Creation TaskEngine	SAP Disclosure Management server requests task engine to create a report using this plugin
ValidationTaskEngine	SAP Disclosure Management server requests task engine to validate a report using this plugin
PreviewTaskEngine	SAP Disclosure Management server requests task engine to create a preview for a report using this plugin

The plugin list comprises the following columns:

- *Active* - Indicates whether the plugin is active.
- *Name* - Displays the name of the plugin.
- *Description* - Displays a short description of the plugin.
- *Status* - Displays the status of the plugin:
  - *Registered* - The plugin is registered and active.
  - *Not registered* - The plugin is available but cannot be used.
  - *New version available* - A new version is available, which needs to be registered.
- *Type* - Displays the purpose of the plugin, for example, output generation or a filter for content generation.
- *Author* - Displays the creator of the plugin.
- *Assembly info* - Displays information contained in the DLL file such as version, culture, and public token.
- *File* - Displays the directory and the name of the DLL file, which stores the plugin information.

5.9.6.1 Registering Plugins

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Plugins*.
   A list of existing plugins appears. The *Status* column in the list displays either *New version available* or *Not registered*.
3. Click *Register all plugins*.

   > ⓘ Note
   >
   > Before registering new plugins, make sure that they are not in use by a user. Basically it is possible to register plugins while they are used. However, this may lead to unexpected results.

   The register action can take a few minutes. The system displays a message that the new version of the plugins has been registered successfully. The plugins are now *Active* and the status has been changed to *Registered.*

5.9.6.2 Uploading Plugins

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Plugins*.
3. To navigate to the plugin file, click *Browse*.
4. Select the file and click *Open*.
   The system closes the dialog box and the required directory is entered in the *File* field.
5. Click *Upload file*.
   The system displays an information message that the plugin has been uploaded successfully.

Next Steps

You must register the plugins.

Related Information

Registering Plugins [page 39]

5.9.6.3 E-Bilanz Plugin Administration

Note the following prerequisites for data exchange with ERiC:

- The maximum volume of uncompressed data that can be transferred to ERiC is 60 MB. ELSTER's data acceptance server rejects compressed data exceeding 15 MB.
- Data transfer between SAP Disclosure Management and ELSTER's data acceptance servers requires the following IP addresses to be opened in the firewall configuration for the function:

Function	IP Addresses	Port	Protocol
`Transfer`	datenannahme1.elster.de, datenannahme2.elster.de, datenannahme3.elster.de, datenannahme4.elster.de	443	https

As of version 27, ERiC only allows Transport Layer Security (TLS) version 1.2 with perfect forward secrecy for the HTTPS protocol. It only supports the following ciphers:

- `ECDHE-ECDSA-AES128-GCM-SHA256`
- `ECDHE-ECDSA-AES256-GCM-SHA384`
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Ensure that your system landscape supports these settings.

You can define the E-Bilanz parameters on the *Configuration* tab of the E-Bilanz plugin. The parameters are as shown below:

SAP DM Parameters for E-Bilanz

Parameter Name	Range of Values (Examples)	Description
`Stylesheet name`		Stylesheet used for XBRL factory protocol creation.
`Proxy host`	Example internal.proxy	(IP) address or host name of proxy.
`Proxy user`	Example proxy_user	User name for logging on to the proxy (if required).
`Proxy authentication`	Any, Basic, Digest, NTLM, DigestIE (default: any)	Optional: Multiple values must be separated by commas. The values are not case-sensitive. Note: If transfer problems occur, contact the network administrator.

Parameter Name	Range of Values (Examples)	Description
`Proxy port`	Example 8080	Proxy port
`Use proxy server`	Yes/No	"Yes" if a proxy server has to be used for data transfer from the (company) network.
`Encryption`	Currently there is only one choice available.	You can specify the encryption you want to use by choosing the respective value from the dropdown box.
`Proxy password`	Example ******	Password for logging on to the proxy (if required).

> **Note**
>
> You can find the log files for the E-Bilanz plugin and ERiC at this location: `<ServerInstallationPath>\Data\Plugins\SAPBO.DisclosureManagement.EBilanz.Plugin\<Version>\SAPBO.DisclosureManagement.EBilanz.Plugin\Logs` or `\ERIC_LOG`.

Permissions

The SAP E-Bilanz plugin requires the following permissions for specific subfolders of `<Plugins folder>\<E-Bilanz plugin>\<version>\<E-Bilanz plugin>\`:

- `ERIC_DATA read write`
- `ERIC_DLL read execute`
- `ERIC_LOG read write`
- `Logs read write`
- `Viewer read`

5.9.7 Report Type Administration

Report types define the content and output formats for a report.

When creating a report, select at least one output format. There can only be one default output format, which is called the native output format. Output formats are defined by the registered plugins. Possible actions when defining output formats are *Create*, *Preview*, and *Validation*.

> **Note**
>
> You can select only one validation output format, but several output types for the preview. The types for Renderer and Task Engine are not allowed to be mixed.

> **Note**
>
> You cannot delete report types that are used in the master data settings of reports.

The report type list comprises the following columns:

- *Name* - Displays the name of the report type.
- *Description* - Displays a short description indicating the purpose of the report type, if maintained.
- *Supported chapter content* - Displays the applications supported for the content deployment.
- *Supported renderer-types* - Displays the supported export output formats.
- *Category type* - Displays one of the three categories used to determine the access to the report documents.
- *Outdated* - Indicates that a report type can be set out of date to prevent further use in reports and chapters.

5.9.7.1 Creating Report Types

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Report types*.
   A list of existing report types appears. Use the icons at the bottom of the list to switch between pages, if necessary.
3. Click *New report type*.
4. On the *Report type* tab, enter a name and, optionally, a short description.
5. From the *Category type* list, select a form of access to the report documents:
   - If the report is used to produce a text-based output, select *Document*.
   - If the report is a standalone data cache, which holds the quantitative data of other reports, select *DataCache*.
   - If the report is used to produce an XBRL-based output, select *Taxonomy*.
6. On the *Output formats* tab, select the checkboxes next to the formats that you want to be available for reports.

   > **Caution**
   >
   > Ignore any warning or information message.
7. On the *Report type* tab, select a *Native output format* from the list.
8. On the *Chapter content* tab, in the work area, a list of supported applications is displayed.
9. Select the checkboxes for the applications to be used to produce all relevant types of content in reports.
10. To save the settings, click *OK*.

5.9.7.2 Editing Report Types

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Report types*.
3. Select a report.
4. Click *Edit report type*.
5. Apply the required changes to the settings displayed on the various tabs.

   You can change any settings regardless if the report type is used by reports with chapters in progress. On the *Chapter content* tab, you cannot remove any content types that are already used in reports.

   > ⓘ Note
   >
   > The settings in the *Output formats* tab influence the settings of the native output format.

6. To save the changes, click *OK*.
   The system displays the information message that the report type has been saved.

Related Information

Creating Report Types [page 42]

5.9.7.3 Deleting Report Types

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Report types*.
3. Select the report you want to delete.
4. Click *Delete report type*.
5. In the *Confirm* dialog box, click *OK*.

   > ⓘ Note
   >
   > The deletion process can take a few minutes because the system checks whether the report type is used by reports.

   The system displays the information message that the report type has been deleted.

5.9.8 Configuration Files for Content Refresh

In SAP Disclosure Management, you can update datalinked quantitative data by performing a server content refresh.

The BIP_WordTableDef.doc table Design File

Usually, quantitative report data is stored in Microsoft Word tables. To eliminate the need to format tables every time, and to ensure a consistent corporate design in a report, it is possible to store the required design formats in a Word document. All other users who work with SAP Disclosure Management will use this table design when editing their documents.

Related Information

Setting the Directory to Content Refresh Configuration Files [page 59]

5.9.8.1 Defining Data Sources as External or Internal

You can determine data sources as internal or external in SAP Disclosure Management in the SAP Disclosure Management Office Client under *Manage Datasources*. If a datasource is determined as internal, linked data caches provided by this particular data source will be cached to increase performance during the content refresh process. Please note, however, that the first content refresh run for internal data sources can be more time-consuming than one for external data sources.

As long as a DM data source has not been tested, it remains undetermined. DM date sources become undetermined after an update or if the URL or port has been changed.

> ⚠ Restriction
>
> When you roll forward a period, copy a report, or create reports from templates, undefined data sources will cause errors if used in the content of the chapters.

5.9.8.2 Data Sources on the DM Server

You can add, edit, or remove data sources from the DM Server only via the DM Client. To do so, you must create a local DM data source with the corresponding connection data. After a successful connection, switch to server mode. The connecting user needs the permission *Administration* > *Configure content refresh* to add, edit, or remove data sources. You can't upload the list of all data sources. During the DM Server update to DM Stack 15xx, all allowed data sources are migrated from the `config20.xml file`.

When you create data sources, the following rules apply:

- Processing is only possible with the above authorization.
- The name of the data source is unique.
- A data source can always be deleted.
- Additional validation takes place on the server, resulting in a possible reload of the data sources.

5.9.8.2.1 Enabling Server Content Refresh for SAP ERP Data Sources

Prerequisites

You have created an SAP ERP data source, as described in Creating a Local Data Source.

Context

To use an SAP ERP data source, you must ensure that the SAP ERP system is connected to the DM server. Additionally, you must deploy files to support the used SAP ERP protocol. These files are automatically installed on clients by SAP GUI. On the server side, you must download these files from SAP.

5.9.8.2.1.1 Stack 1100 and Lower

Context

The following steps are relevant for SAP Disclosure Management Stack 1100 and lower.

> **Note**
>
> Both versions of the library mentioned below have the same file name, but a different file size.

Procedure

1. Ensure that you have the latest Visual C++ 2005 runtime.
2. Download the files attached in 2561865.
3. Copy the downloaded 64-bit version of `librfc32.dll` to the `<WindowsDir>\System32` folder.
4. Copy the downloaded 32-bit version of `librfc32.dll` to the `<WindowsDir>\SysWOW64` folder.

5.9.8.2.1.2 Stack 1200 and Higher

Context

The following steps are relevant for SAP Disclosure Management Stack 1200 and higher.

In SAP Disclosure Management Stack 1200, the NetWeaver RFC Protocol (NWRFC) is also supported.

> **Note**
>
> You can also use Single Sign-On (SSO) if you have activated a secure network connection (SNC) similar to SAP Logon.

Procedure

1. Ensure that you have the latest Visual C++ 2013 runtime.
2. Enable the *Use NW Protocol* in the SAP ERP data sources.
3. To use the ERP data source with NWRFC in the SAP Disclosure Management Server 64-Bit system, you need two versions of the following files: `sapnwrfc.dll`, `icuuc*.dll`, `icudt*.dll`, and `icuin*.dll`. The asterisks refer to the Software Development Kit (SDK) version. All files are available for x64 and x86. You can find the SDK in 2573790. Click the link to the installation files on the SAP Support Portal.and choose the latest available SAP NW RFC SDK, then choose the version *Windows Server On IA32 32 BIT* and *Windows ON X64BIT* to download the SDKs. Search for the above-mentioned files in the downloaded zip files.
4. Copy the 64-bit version of the files to the `<WindowsDir>\System32 folder`. The 32-Bit version must be copied to the `<WindowsDir>\SysWOW64 folder`.

5.9.8.2.2 Using SAP ERP Data Sources with Secure Network Communication for Server Content Refresh

Prerequisites

You have created an SAP ERP data source with Secure Network Communication (SNC), as described in Creating a Local Data Source.

Context

You must install a provider for the SNC connection, for example, `SapSncClientEncryption`. It should be the same as the one you use for the client side. Check whether the **SNCLibraryPath** file in the data source exists and whether the IIS application pool user has read access to the folder.

5.9.9 Log File Administration

System errors are saved in a log file. The system creates a log file every day. The log file is a text file that you can download to your local drive.

The log file list comprises the following columns:

- *File* - Displays the name of the file.
- *Last changed on* - Displays the time stamp for the last file modification.
- *Size* - Displays the size of the file.

> ⓘ Note
>
> The SAP Disclosure Management logger component has a fixed free disk space minimum of 100 MB. If the log files target drive (see `Log.config`) has less than 100 MB of free space available, logging is interrupted. This measure does not apply to shared network folders (Uniform Naming Convention paths).

> → Recommendation
>
> Please follow the recommendations below about hardening log files:
>
> - Define a specific folder for all SAP Disclosure Management log files for every single DM component. It is strongly recommended that this folder should be on either a different disk or partition than the DM component or on a network shared folder (UNC path).
>   Make sure that the assigned user for the SAP Disclosure Management Application Pool has read and write permissions on the folder. To prevent manipulation of logs, you should restrict the permissions as much as possible.

- It is strongly recommended that you apply notification events when low disk space has been reached for the log file target drive (see `Log.config`). Make sure to apply these settings to all used DM components and scenarios.

5.9.9.1 Downloading Log Files

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Log files*.
3. In the log file list, click a file.
4. Click *Download*.
5. In the *File Download* dialog box, click *Save*.
6. Navigate to the location where you want to store the log file.
7. In the *File name* field, change the file name, if necessary.
8. Click *Save*.

5.9.10 Extended Audit Trail

The Audit Trail in SAP Disclosure Management covers all actions that a user can perform to administer and secure data. All available audit trail items stored within SAP Disclosure Managment can be viewed using an audit trail report. You can download the report under *Security* > *Audit trail events log*. To view the audit trail, the user reuires *View Audit Log* permission.

The audit trail report is a Microsoft Excel workbook and consists of two worksheets containing the following information:

Header Information:

- **System name**: Name of the SAP Disclosure Management system where the report was created
- **Date of creation**: Date when the report was created
- **Time of creation**: Time when the report was created
- **Creating user**: User who created the report
- **Scope value**: Time interval that was selected when the report was created

Audit Log:

- **Date:** Date of the audit event
- **Time**: Time of the audit event
- **Executing user**: User who executed the event
- **Area type**: Type of the area where the event was executed (for example, chapter)
- **Area**: Name/path of the area where the event was executed

- **Object type**: Type of the object on which the event was executed (for example, user)
- **Object**: Name of the object on which the event was executed
- **Sub-object type**: Type of the subobject on which the event was executed (for example, role)
- **Sub-object**: Name of the sub-object on which the event was executed
- **Action**: The event itself
- **Action value 1**: Additional information about the event. (for example, old value of a changed property)
- **Action value 2**: Additional information about the event (for example, new value of a changed property)
- **Logging**
  The audit trail logs the following activities:

Category 1	Category 2	Action A	Action B	Description
Settings	Manage reports	New period		Name of new period
Settings	Manage reports	Edit period	Change name	From name X to name Y
Settings	Manage reports	New report		Name of new report
Settings	Manage reports	Edit report	Change name	From name X to name Y
Settings	Manage reports	Edit report	Change description	From description X to description Y
Settings	Manage reports	Edit report	Change period	From period X to period Y
Settings	Manage reports	Edit report	Change workflow	From name X to name Y
Settings	Manage reports	Delete report		Name of deleted report
Settings	Manage reports	Copy report		From report X to report Y
Settings	Manage Periods	Roll forward		
Settings	Manage Periods	Publish		
Security	Roles	New role		Name of new role, added permissions
Security	Roles	Edit role	Change name	From name X to name Y
Security	Roles	Edit role	Change permissions	Deleted or added permissions

Category 1	Category 2	Action A	Action B	Description
Security	Roles	Delete role		Name of deleted role
Security	Users	Edit user	Last name or first name	From last name X to last name Y; from first name X to first name Y
Security	Users	Edit user	Change e-mail	From e-mail X to e-mail Y
Security	Users	Edit user	Change activation date	From activation date X to activation date Y
Security	Users	Edit user	Change expiration date	From expiration date X to expiration date Y
Security	Users	Edit user		From *Checked* to *Unchecked*; from *Unchecked* to *Checked*
Security	Users	Global permission	Delete permission	Name of deleted role
Security	Users	Local permission	Add permission	Name of report/chapter, user, and assigned role
Security	Users	Change password		
Security	Users	Login		
Security	Users	Logout		
Security	Users	Local permission	Delete permission	Name of deleted role
Security	Policy	All policies	All possible changes	
Administration	Workflow	New workflow		Name of new workflow
Administration	Workflow	Edit workflow		Changes in workflow steps
Administration	Workflow	Delete workflow		Name of deleted workflow
Report	Chapters	New chapter		Name of new chapter
Report	Chapters	Edit chapter	Change chapter name	From name X to name Y

Category 1	Category 2	Action A	Action B	Description
Report	Chapters	Revisions	Download	Name of downloaded chapter
Report	Chapters	Permissions	Add user	Name and added role
Report	Chapters	Permissions	Edit user	User name and assigned/removed role
Security	Users	Login	Unauthorized access detected	Detected resource access attempt after user has actively logged out.

5.9.11 Authorization Report Administration

The authorization report in SAP Disclosure Management is an Excel sheet that contains authorization information. You can save and open it after the download. It enables administrators to get an overview of all users and assigned global and local permissions. The report is a list of all available users and is divided up as follows:

- General user information
- Global permissions and roles assigned to users
- Local permissions and roles assigned to users, including the respective reports and chapters

> **Note**
>
> The local permissions displayed in the report are limited to those entities that the administrator is assigned to. The system only displays the reports of users who belong to the same entity as the administrator.

To view the report, the administrator must have the permission *Authorization Report View*:

1. Choose *Security* > *Roles*.
2. Create or edit the role that you want to assign to the authorization report.
3. Select the *Permission* tab.
4. Select the *Authorization Report View* field.
5. Go back to the *Role* tab.
6. Choose *OK*.

To generate and download the authorization report, proceed as follows:

1. Choose *Security* > *Authorization Report*.
2. Select a period.
3. Choose *Download*.

5.9.12 System Configuration

The administrator of SAP Disclosure Management must customize the following system settings:

- Application details, report limitations, and online help access on the *Misc* tab
- E-mail notifications on the *E-mail* tab
- Directories to system files on the *Licenses* tab, *Content refresh* tab, *Plugins* tab, and *Upload* tab
- XBRL and PDF component activation

5.9.12.1 Password Policy

To enforce a global password policy, you have to set the *Enforce Password Policy* parameter to *Yes* on the *Password Policy* tab. Choose *Administration* > *System configuration* > *Password Policy*. This parameter is set to *No*, by default, after you have installed the SAP Disclosure Management. If the parameter is set to *Yes*, you can define the following policy parameters:

Global Password Definition

Password Syntax	Description	Default Value	Minimum Value
Minimum length of password	Sets the minimum length of the password (minimum number of characters).	0	1
Minimum amount of lower-case letters	Sets the minimum amount of lower-case letters contained in a password.	0	1
Minimum amount of upper-case letters	Sets the minimum amount of upper-case letters contained in a password.	0	1
Minimum amount of Arabic numerals	Sets the minimum amount of Arabic numerals contained in a password.	0	1
Minimum amount of special characters	Sets the minimum amount of special characters contained in a password.	0	1
Leading positions with difference to user name	Number of leading characters that must be different in password and user name.	0	2
Number of leading non-identical characters	Number of positions that must **not** be identical at the beginning.	0	2

You can also define a lifecycle for the passwords:

Lifecycle of Passwords

Password Lifecycle	Definition	Default Value
Maximum Age of Password	Validity period of password in days	0

Password Lifecycle	Definition	Default Value
Number of Days for Password Expiration Warning	Number of days before actual password expiration that a warning message should appear after successful logon to the SAP Disclosure Management server	7
Maximum Number of Passwords to be Stored in Password History	Number of passwords to be stored in the password history. Passwords cannot be reused while they are stored in the history.	0

To deactivate any of the above-mentioned parameters, insert the value 0. The specific requirement will then be ignored during the password policy validation process. Once you have completed the policy definition, choose *Save* to implement all settings. Once the parameters have been set and saved, a pop-up is displayed, where you can define whether all users should be prompted to change their passwords after their next logon. If you choose *Yes*, every user will be redirected to a *Change User Information* form the next time they log on to SAP Disclosure Management. On this form, users can change the password according to the enforced password policy.

If a user's password has expired, they are automatically redirected to the *Change User Information* form the next time they log on to the SAP Disclosure Management server. Here, they can change their password, as required.

The characters below can be used in passwords:

Character Specification

Character Type	Character Definition
Lower-Case Letters	All lower-case letter characters (a - z, ä, ö, ü, ß)
Upper-Case Letters	All upper-case letter characters (A - Z, Ä, Ö, Ü)
Arabic Numerals	All Arabic numeral characters (0, 1 - 9)
Special Characters	All characters that are neither a letter nor a number (^, °, !, ", §, $, %, &, /, (,), =, ?, [,],)

In addition you can define password hashes.

You can define the password hash algorithm used to generate password hashes. You have the following options:

- SHA-1 (HMACSHA1)
- SHA-2 algorithms :HMACSHA256 and HMACSHA512
- PBKDF2
  The PBKDF2 Password Storage Scheme provides a mechanism for encoding user passwords using the `PBKDF2` message digest algorithm. `PBKDF2` is the short name for `PBKDF2-HMAC-SHA512`.

> **Note**
>
> A change of the hash algorithm results in a reset of all user passwords to the default password defined under *Administration* > *System configuration* > *Misc* > *Default Initial Password*. Make sure that you edit this parameter before you change the algorithm.

Password Hashes

Password Hashes	Description	Default Value
Password Hash Algorithm	Select the hash algorithm used for generating user password hashes.	PBKDF2

5.9.12.2 Account Policy

To define a user account policy, choose the *Account Policy* tab in the *Administration* area and define the parameters according to your requirements.

Account Policy

Parameter	Definition	Default Value
Maximum Number of Days Allowed for Account Inactivity	Time in days after last successful logon to SAP Disclosure Management (SAP DM) and calendar date the user is allowed not to log on to SAP DM. If the defined time span is exceeded, the user account will be locked during the next logon process.	0
Number of Days for Account Expiration Warning	Number of days before the user account expiration date that a warning message should appear after successful logon to SAP DM. The account expiration date can be set in the user administration area. If no expiration date is set, the user account will never expire. If a user account has expired, it will be locked upon the next logon to SAP DM. This parameter is related to the *User Account Expiration Date*, which must be set in the user administration for every user.	7
Maximum Number of Failed Login Attempts	Maximum number of failed logon attempts allowed before the user account is locked.	3
Grace period for password changes in days	Number of days a user has time to change his or her password, beginning with the day he or she is requested to do so or the activation date. If the grace period ends with no change, the account is deactivated.	0

> **Note**
>
> You can deactivate any individual parameter of the policy by entering *0* as a parameter. To persist all policy definitions, choose *Save*.

> **Note**
>
> The *Number of days for account expiration warning* parameter refers to the *User Account Expiration Date*, which has to be set on the *User* tab for every user.

5.9.12.3 Setting up Company Information

Context

We recommend that you enter the following information at the beginning of the application implementation because it appears in the address of the Web browser:

SAP Disclosure Management offers application help, which you can access under https://help.sap.com/. The user can also access the help by clicking the help icon in SAP Disclosure Management. When the user clicks the help icon, the current application help is displayed. However, the administrator can also deploy the current application help locally if users have no internet connection.

For more information on deploying the application help locally see Deploying the Application Help Locally [page 56].

The default settings of SAP Disclosure Management only allow consolidated report documents to be created when the workflows, of all related chapters, have reached the final step. If required, by subject matter experts, the administrator can deactivate this setting to allow for the creation of the report document at any stage.

> **Note**
>
> This setting is system-wide and not report-specific.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *System configuration*.
3. Click the *Misc* tab.
4. Enter a description in the *Application´s description* field. This description is used as the second header title displayed in the browser preview window for SAP DM. Very often customers use both a production and a test environment for SAP Disclosure Management. To distinguish the two systems by name and not only by TCP-IP number, enter the purpose and type of environment.

   > **Example**
   >
   > Enter a system purpose such as quality assurance or production.

5. Enter the name of the application in the *Application´s name* field. This name is used as the first header title which is displayed in the browser preview window for SAP DM.

6. Enter the URL of the server for the Web service in the *Root folder for the Web service* field. This URL is used to establish the connection between the client and the server. Enter the directory to the server location that stores the web services.
7. In the *Company name* field, enter the name of your company.
8. In the *Create report, only when all chapters reach the end step* field, make a selection.
    - To allow the generation of the consolidated document only when all chapter documents have reached the final step of their workflow, click *Yes*.
    - To allow the generation of the consolidated document at any stage of the chapter-related workflows, click *No*.
9. In the *Enable "SOAP SSL Certificate" Checks* field, select *Yes* or *No*.
10. In the *Root folder for the webhelp* field, enter the directory of the network location, which stores the online help.
11. In the *Task engine web service URL* field, enter the new URL of the task engine web service, if you have modified the URL. For more information, see Task Engine [page 83]).
12. In the *Default Initial Password* field, enter the default password.
13. To save the settings, click *Save*.

5.9.12.3.1 Deploying the Application Help Locally

Context

The SAP Disclosure Management (SAP DM) application help is available in several different languages on the SAP Disclosure Management product page located under SAP Help Portal.

The languages available are German, English, Spanish,French, Italian, Portuguese, Russian, Chinese and Japanese. If a language is selected, which is not listed above, the system defaults back to English.

If your users don't have Internet access, the help files locally can be saved locally:

Procedure

1. Download the current SAP Disclosure Management application help zip file, in the language relevant for your users, from the SAP Website SAP Help Portal and copy it to a folder in the IIS DM Application.

    > **Note**
    >
    > The folder path name must be the same as the version installed such as `10.1_SP10` or `10.1_SP11`.

    > **Example**
    >
    > IIS DM Installation Folder /DMApplication/help/10.1_SP10/en-US/

2. Unzip the downloaded SAP Disclosure Management application help zip file into:

> ✤ Example
>
> `IIS DM Installation Folder /DMApplication/help/10.1_SP10/en-US/`

3. Rename the `context.htm` file to `index.htm`.
4. Finally, under *SAP Disclosure Management* > *Administration* > *System configuration* > *Root folder for the Web Help* enter the relevant link.

> ✤ Example
>
> `http://localhost/DMApplicationInstallation/help/`.

Results

You have deployed the application help locally and the users have access to it, when clicking the help icon.

5.9.12.4 Setting up E-Mail Notifications

Context

By default, when executing the activity for step transition, the system does not send any notification to the owners of the next workflow steps. If required by the subject matter experts, the administrator can change this setting and install either a mandatory or an optional notification service. The latter requires an appropriate user confirmation each time the activity for a step transition is executed. To activate the e-mail service, the administrator must set up the SMTP server as well as the standardized e-mail text and subject content.

> ⓘ Note
>
> This setting is system-wide and not report-specific.

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *System configuration*.
3. On the *E-Mail* tab, make the following settings:

Field	Description
Host	TCP-IP number or the name of the SMTP server.

Field	Description
SMTP User	If necessary: User ID for logging in to the SMTP server.
SMTP Password	If necessary: Password for logging in to the SMTP server.
From	E-mail address of the sender of the e-mail notification.
Display name	Name of the sender to display to recipients of the e-mail notifications.
Workflow Status Subject	Text to appear in the subject for e-mails to be sent for standard status changes.
Workflow Status Template	Directory to a file that contains the body text for standard e-mails.
Report Locking Subject	Text to appear in the subject for e-mails to be sent when a report is locked.
Report Locking Template	Directory to a file that contains the body text for e-mails to be sent when a report is locked.
Report Unlocking Subject	Text to appear in the subject for e-mails to be sent when a report is unlocked.
Report Unlocking Template	Directory to a file that contains the body text for e-mails to be sent when a report is unlocked.

> ⓘ Note
>
> You can edit the text in the e-mail template files and replace it with your own text.

4. To save the settings, click *Save*.
5. To test e-mail notifications, click *Test E-Mail*.

5.9.12.5 Setting the File Storage Folder

Context

This folder contains all uploaded and system configuration files.

Procedure

1. In SAP Disclosure Management, choose the *Administration* tab.
2. Choose *System Configuration*.
3. On the *Upload* tab, in the *Common* field, enter the directory of the server location where you want to store files.

> ⓘ Note
>
> Additional temporary files and folders will be created in this folder at runtime, and these will be deleted automatically by the application. If, due to an error, these files and folders in this folder are not deleted, the administrator must delete them manually.

4. In the *Root* field, enter the directory of the server location where you want to store the installation settings.
5. To save the settings, choose *Save*.

5.9.12.6 Setting the Directory to Plug-In Files

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *System configuration*.
3. On the *Plugins* tab, in the *Directory* field, enter the directory to the server location where you want to store the plug-in DLL files.
4. To save the settings, click *Save*.

5.9.12.7 Setting the Directory to Content Refresh Configuration Files

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *System configuration*.
3. On the *Content refresh* tab, enter the directories to the server locations where you want to store the following:
   - In the *ConfigFile* field, enter the `config20.xml` file directory.
   - In the *BIP_WordTableTagging* field, enter the `BIP_WordTableTagging.xml` file directory.
   - In the *BIP_WordTableDef* field, enter the `BIP_WordTableDef.doc` file directory.
4. To save the settings, click *Save*.

5.9.13 Customization of Language Culture Settings

To facilitate the production of the official reports, you can customize the language options.

> ⓘ Note
>
> You cannot delete the customized language setting if it is still used in other settings. When you delete customized language settings, you do not delete the language itself but only the selected customized settings. The language and its standard settings are still available on the system.

The list of customized languages comprises the following columns:

- *Culture* - Displays the name of the language.
- *Decimal symbol* - Displays the decimal separator.
- *Digit grouping symbol* - Displays the thousand separator.
- *Negative sign symbol* - Displays the signs to be used for the representation of negative numbers.
- *Sign space* - Indicates whether there is a space between the sign and the number.
- *Currency align* - Indicates whether and where the currency is displayed.
- *Currency sign* - Defines the symbol or code to be displayed instead of the currency's name, for example, $ or €. You can enter up to three characters. If you leave this field empty, the system enters a default currency sign for the respective country.
- *Currency space* - Defines the space character to be displayed between the currency value and the currency sign.
- *Null value* - Determines the representation of zero values.
- *Number format* - Displays the appearance of positive numbers based on the actual settings.
- *Negative number format* - Displays the appearance of negative numbers based on the actual settings.
- *Tabledirection* - Indicates the direction of the table.
- *Position of Percent* - Indicates the position of the percentage sign if the negative sign symbol is a parenthesis.

5.9.13.1 Customizing Settings for a Language Culture

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Language options*.
3. On the *Language options* tab, select a language from the *Culture* list.
   The list contains all languages for which standard settings have not yet been customized.
4. Click *Customize language*.
5. On the *Table* tab, customize the standard settings to correspond with your Microsoft Office Word tables.

   > ⚠ Restriction
   >
   > You cannot use the same character for the decimal and thousand separators additionally.

   a. Select a *Decimal symbol*.
   b. Select a *Digit grouping symbol*.
   c. Select a *Negative sign symbol*:

Option	Description
Minus	Sign represented by standard minus sign (-)
Non-breaking hyphen	Sign represented by standard hyphen, no break allowed

Option	Description
(-) En dash	Sign represented by standard dash with width of one en (half of one em)
Em dash	Sign represented by standard dash with width of one em
Parenthesis	Paragraph characters at the beginning and end of number
Non	No sign
Hyphen	Sign represented by standard hyphen
Hyphen minus	Sign represented by the consolidated hyphen (2DHex in ASCII)

d. Select a *Sign space*:

Option	Description
Space	Normal space (ASCII 0x20)
Non-breaking space	Same as space but no break allowed
Em space	Space has width of one em
En space	Space has width of one en (half of one em)
Quarter of Em space	Space has the width of a quarter of an em space
Non	No space

e. Select a *Currency align* option.
f. Select a *Null value*.
g. Choose a table direction.
h. Choose the position of the percentage sign.

6. On the *Floating text* tab, define the parameters for the representation of numbers in floating text.
7. To save the settings, click *OK*.

5.9.13.2 Editing the Configuration of Customized Language Cultures

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Language options*.
   A list of customized languages appears.
3. Select the required language.
4. Click *Edit customized language*.
5. On the *Table* tab, update the settings for numbers in Microsoft Office Word tables, as necessary.

6. Click the *Floating text* tab.
7. Update the settings for the numbers in active text fields used in Microsoft Office Word documents, as necessary.
8. To save the settings, click *OK*.

Related Information

Customizing Settings for a Language Culture [page 60]

5.9.13.3 Deleting Language Cultured

Procedure

1. In SAP Disclosure Management, click the *Administration* tab.
2. Click *Language options*.
3. Select the language whose customized settings you want to delete.
4. Click *Delete customized language*.
5. To delete the customized settings of the language, in the *Confirm* dialog box, click *OK*.

> ⓘ Note
>
> You have not deleted the language from the system, you only delete the customized settings.

5.9.14 Reports for System Administration

The report configuration monitor provides information on the configuration of a system or a specific report. Using this report you can, for example, easily check whether users have been set up with the correct permissions or which workflows have already been set up on the system but have not yet been activated.

System Configuration

- Permissions: The report displays all active and inactive users with their assigned roles. Inactive users have master data on the system but cannot use it, yet.
- Roles: The report displays all roles with their assigned global permissions. The global permissions are part of the users' master data and have been set up by the system administrator. Global access is not period- or report-specific.

- Workflows: The report displays all active and inactive workflows with their steps, activities, and conditions. Inactive means that the workflow has already been created on the system but cannot currently be used. Activities and conditions determine the way of transition between the workflow steps.

Report Configuration

- Permissions: The report displays all users with both global and local permissions on report and chapter level.
- Configuration of Parameters: The report displays the output rendering settings for the native and supported formats on report and chapter level.
- Workflows: The report displays the workflow settings both on report and chapter level.
- Content refresh: The report displays whether the content of the chapter has been updated.

More Information

- Section “Authorizations” in the *SAP Disclosure Management User Help*
- Section “Workflows” in the *SAP Disclosure Management User Help*

5.9.14.1 Displaying the System Configuration Report

Context

To display an overview on the current system configuration that contains all users with their permissions as well as all available roles and workflows:

Procedure

1. In SAP Disclosure Management, on the *Monitoring* tab, click *Report Configuration*.
2. To generate the report in XML format, on the *System Configuration Report* tab, click *Generate report*.

   > ⓘ Note
   >
   > The loading process can take several seconds.

   The system opens a new window that contains detailed information about the current configuration of SAP Disclosure Management including permissions, roles and workflows.

   The report header displays the date and time at which the report was created and the name of the user who created the report. All available workflows appear at the top as active links that allow direct access to the details of the workflow.

3. To display information on permissions, roles, and workflows, or the workflow-related details, scroll to and click the appropriate link.

   User permission details:

Login	Displays the user ID.
Firstname	Displays the first name of the user.
Lastname	Displays the last name of the user.
Active	Displays *True* or *False* to indicate whether the user ID is active or inactive.
Roles	Displays the roles assigned to the user ID.

   Role details:

Role	Displays all available roles.
Description	Provides a short description of each of the available roles.
global Permission	Lists the global permissions assigned to the roles. For more information on the authorizations, see the *General* online help.

   Workflow details:

Name	Displays the name of the workflow.
Description	Provides a short description of the workflow. Optional.
isActive	Displays *True* or *False* to indicate whether the workflow is active or inactive.
Steps	Displays the individual workflow steps and for each step the transition activities and their related conditions. For more information on workflows, see the *General* online help.

4. Close the window with the configuration information at any time and return to the *System Configuration Report* tab.

5.9.14.2 Displaying a Report on Report Configurations

Context

To display an overview on the current report configuration, which contains report and chapter workflows, permissions, and configuration parameters:

Procedure

1. In SAP Disclosure Management, on the *Monitoring* tab, click *Report Monitor*.

2. On the *Document Configuration Report* tab, select a *Period*, then a *Report*.
3. To generate the report in XML format, click *Generate report*.

   > **Note**
   >
   > The loading process can take several minutes.

   The system opens a window that contains detailed information about the current configuration of the permissions, configuration parameters, and workflows at the report and chapter levels.

   The report header displays the date and time at which the report was created and the name of the user who created the report. All available chapters appear below the diagram as links that allow you to access the details of the chapter.
4. To display the chapter-related details, scroll to and click the appropriate link in the chapter list.
5. To display all information on report and on chapter level, use the horizontal scrollbar.

   Information at the report level:
   - Permissions: This table lists users and their global and local access rights defined at the report level.
     - User: Displays the user ID.
     - Source: Displays whether the permissions have been assigned by the system administrator for the entire system (global) or whether the permissions have been assigned at the report level (local).
     - Chapter: The green checkmark indicates access rights granted at the chapter level.
     - Report: The green checkmark indicates access rights granted at the report level.
   - Custom Metadata: This table lists all settings related to the configuration parameters at the report level.
   - Workflow: This table displays a flowchart of the workflow assigned at the report level. For more information about workflows, see the General help.

   Information at the chapter level:
   - Custom Metadata: Displays information on parameters configured at the chapter level, which overrule the settings at the report level.
   - Workflow: Displays information whether the chapter has inherited the workflow from a higher level or whether it has its own workflow. The system also displays the name of the workflow.
   - Permissions: Displays information regarding any inherited permissions and any user permissions set up only for this chapter.
6. Close the window with the configuration information at any time and return to the *Document Configuration Report* tab.

5.9.15 Automatic Removal of Temporary Data

SAP Disclosure Management provides a function to remove temporary data automatically. The DM_Cleanup.bat tool is deployed to the following folder: *Administration* > *System Configuration* > *Compare* > *Temp folder*.

Manual Removal of Temporary Data

To remove temporary data manually, navigate to the temp folder and execute the DM_Cleanup.bat tool. The tool removes all temporary files in the temp folder except all subfolders.

Periodic Removal of Temporary Data

To remove temporary data on a regular basis, you can use the Windows Task Scheduler. The Windows Task Scheduler allows you to create a task and set up a trigger. This makes it possible to execute the DM_Cleanup.bat tool periodically and to automatize the removal of temporary data.

On Microsoft Windows Server 2003 you find the Windows Task Scheduler under *Programs* > *Accessories* > *System Tools* > *Scheduled Tasks*.

On Microsoft Windows Server 2008 (R2) you find the Windows Task Scheduler under *Programs* > *Accessories* > *System Tools* > *Task Scheduler*.

> ⚠ Caution
>
> Do not execute the DM_Cleanup.bat tool during the active and productive use of Disclosure Management. Define a maintenance time frame for the task. Otherwise, the tool can delete temporary data that is currently in use.

5.9.16 Publishing Packages in SAP Disclosure Management

SAP Disclosure Management (SAP DM) is a document management system with an export function. This function creates an archive containing binary files and meta-information for a specified period.

> ⓘ Note
>
> If you want to publish packages, you have to install and configure the task engine. For more information about the task engine, see Task Engine [page 83].

In SAP DM the period concept is used as a hierarchical top node for structuring reports. There can be 1:n periods in an instance of SAP DM. For each period there can be 1:n reports, and each report can contain 1:n chapters. Reports and chapters can represent certain document types, such as Microsoft Word, Microsoft Excel, or XML files. The chapters of a report can be structured as a hierarchy.

> ✤ Example
>
> [Period] (for example, “Q4 2013”)
>
> [Report] (for example, “Consolidated financial statements”)
>
> [Chapter] (for example, “Income statements”)

Datalinking and Data Sources

Chapters can be linked to other chapters within SAP DM, or other data sources such as an ERP system.

> ✤ Example
>
> In a Microsoft Word chapter there is a table containing data taken from a Microsoft Excel chapter as a data source. The data in the two chapters is linked. The link is saved in the metadata of the chapter and can be used to refresh the data from the data source. The data source chapters can be located in different reports and periods. Each chapter can be linked n times to other data source chapters.

Publishing Package

A publishing package is the result of a function triggered by the user in the period management view. The user selects the period and its report(s) for publication. The resulting package is saved at the location specified in the system configuration. The chapters of a report can be optionally included in the package.

5.9.16.1 Structure of a Publishing Package

The package usually contains the following content, depending on the report content:

- \<Report name>
  - \Chapters\
    - \HTML\
      - HTML representation of Word files and Excel tables marked with a specific Excel name
    - Chapter revision binaries (Word, Excel, PPT etc.)
  - \DataCache\
    - \HTML\
      - HTML representation of Excel tables marked with a specific Excel name
    - Data source chapter binaries (Excel)
  - Report revision content as binary (Word, Excel, XML etc.)
  - Report meta information file (XML)
  - Chapter hierarchy information file (XML)
  - Data sources meta information file (XML)
  - Log file with status information of the publication process (XML)
- Log file with status information of the publication process for all reports (XML)

Depending on the permissions of the user triggering the publication, files can be excluded.

Naming Conventions

The package name is derived from the period name and the UTC date and time of the creation in the format `_yyyy-MM-dd_HHmmss.zip` as shown in the table below:

Log File Messages

Part	Content	Length
yyyy	year	4 digits
MM	month	2 digits
dd	day	2 digits
HH	hours	2 digits (24-hour format)
mm	minutes	2 digits
ss	seconds	2 digits

Example

A package for the period with name Q4 2013 created on January 27 in 2014 at 3.09 pm has the following name: *Q4 2013_2014-01-27_150900.zip*

Note

During the creation process the file extension is `.lock` instead of `.zip`. Once the package creation is completed, the package extension is changed to `.zip`.

Chapter Output

You can include chapters in the package by selecting the *Include chapters in package* field in the report selection dialog once you have selected the period to publish. The file extension and format depend on the chapter type selected in SAP Disclosure Management.

HTML Output

HTML output depends on the chapter type. HTML output can only be created for Microsoft Word and Excel chapters.

- HTML output is created automatically for each **Microsoft Word** chapter in the same way that Word saves documents as HTML.
- HTML output is only created for a **Microsoft Excel** chapter if it contains at least one Excel name using SAP DM naming conventions.

5.9.16.2 Object Infos for Publishing

The ObjectInfo.xml file that is included in a report folder contains datalinking and source information. If the report does not have a revision or is not linked to a data source, the file is not created for the report. The XML schema is included in the *Schema* folder. Additionally, the *XML Examples* folder contains some examples of Microsoft Word and Excel files, which cover the most common cases.

Characteristics for Some XML Elements

ObjectType

- Table
- FloatingText

- FormulaField
- ExcelMeta

DataSource

- DmDataSource
- BwDataSource
- ErpDataSource
- Warning

DataSourceType

- SAP_DM
- SAP_BW
- SAP_ERP

Remarks on Specific XML ElementsDataProvider

If there is a SAP Disclosure Management (SAP DM) data source, the DataProvider can be one of the following types:

1. A table range marked by a Microsoft Excel name (SAP DM naming convention starting with "BIP_" , for example, "BIP_Table").
2. A table range marked by a Microsoft Excel name (SAP DM naming convention starting with "ER_"; for more information about ER ranges, see the SAP DM documentation).
3. A Microsoft Excel sheet with a custom name.

ID

The ID of an object depends on the ObjectType. For Microsoft Word the object ID is the same as the Word bookmark*. For SAP DM there are only three relevant name types:

Name Types

ObjectType	ID
Table	DOC_TBLnnnnn (with n = 0-9)
FloatingText	BIP_SELnnn
FormulaField	DOC_FLDnnnnn

Tables can have IDs, for example *DOC_TBL00001_1_1*, which indicates that there are bookmarks for each cell of the table. The object is only listed without the row and column markers in the ObjectInfo XML file, for example *DOC_TBL00001*.

5.9.16.3 Log File Messages for Publishing

There can be several reasons why content cannot be included during the package compilation process. A message is created for each issue. The log file is in XML format. There are two types of log file:

- A package log file located in the root folder of the package with all messages from all reports
- A report log file located in the report folder with all messages for this report only

Message code table

For machine readability the XML messages have a message code, which can be used to determine the issue. The XML schema is included in the *Schema* folder.

Log File Messages

Message Type	Message Code	Message Text
Info	0	Package created successfully
Info	1	Report completed without warnings/errors
Error	11	Failed to init WordReader for report [...]
Warning	21	Object not datalinked to DM data source: <object name>
Warning	22	Invalid ReportID provided: <id>
Warning	23	Report <report name> is not linked to any data source
Warning	24	Report <report name> has no revision
Warning	25	Chapter <report\chapter name> was checked out at package creation time. Included revision: <revision number>
Warning	26	Chapter <report\chapter name> was checked out at package creation time. No revision available.
Warning	27	No chapters available for report <report name>. Check report hierarchy and permissions.
Warning	28	Chapter <report\chapter name> was excluded because of missing permission
Info	29	Chapter <report\chapter name> does not include a SAP DM Excel name range. HTML output skipped. Check documentation.
Warning	31	Excluded file: <file name>. Reason: An error occurred during HTML conversion. Check TaskEngine log file.
Warning	32	Excluded file: <file name>. Reason: View permission is missing.
Warning	33	Excluded file: <file name>. Reason: Technical error occurred. Check TaskEngine log file.
Warning	34	Excluded file: <file name>. Reason: The report is not data linked.
Warning	35	Excluded file: <file name>. Reason: The chapter has no content.

5.9.16.4 Package Folder Hierarchies

Below is a simple example with the following content:

- Include chapters: disabled
- Publish directory: Z:\Share
- HTML content

Example report hierarchy	Resulting package
Period01 • Report01 (DataCache) o DC1.xlsx (including several "BIP_"-Ranges) o DC2.xls • Report02 (Word) o Chapter01.docx (linked to DC1) o Chapter02.doc (link to DC2)	Z:\Share\Period01\Period01_yyyy-mm-dd_HHmmss.zip: • Report01 o ChapterHierarchy.xml o Log.xml o ReportInfo.xml • Report02 o \Data Cache ▪ \HTML • DC1\ o BIP_Table1.html o BIP_Table2.html ▪ DC1.xlsx ▪ DC2.xls o \HTML ▪ Report02.html o ChapterHierarchy.xml o Log.xml o ObjectInfo.xml o Report02.docx o ReportInfo.xml

There is also a complex example with the following content:

- Include chapters: enabled
- Publish directory: Z:\Share
- HTML content

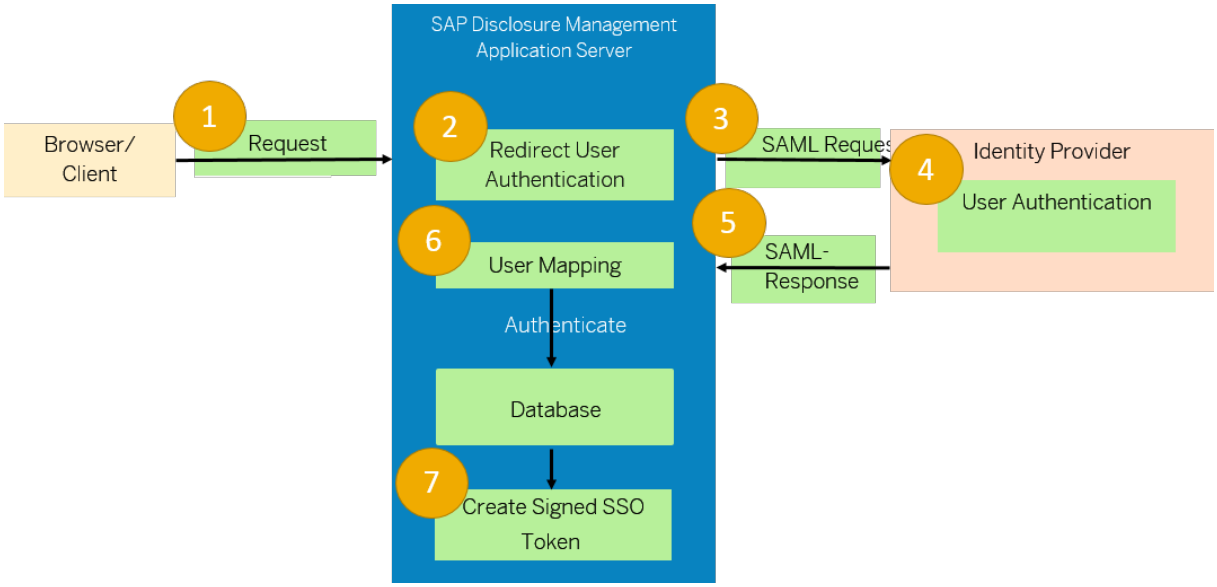
Example report hierarchy	Resulting package
Period01 • Report01 (DataCache) o DC1.xlsx (including "BIP_"-Ranges) o DC2.xls • Report02 (Word) o Chapter01.docx (linked to DC1) o Chapter02.doc (link to DC2)	Z:\Share\Period01\Period01_yyyy-mm-dd_HHmmss.zip: • Report01 o \Chapters ▪ \HTML • DC1\ o BIP_Table1.html o BIP_Table2.html ▪ DC1.xlsx ▪ DC2.xls o ChapterHierarchy.xml o Log.xml o ReportInfo.xml • Report02 o \Chapters ▪ \HTML • Chapter01.html • Chapter02.html ▪ Chapter01.docx ▪ Chapter02.doc o \Data Cache ▪ \HTML • DC1\ o BIP_Table1.html o BIP_Table2.html ▪ DC1.xlsx ▪ DC2.xls o \HTML ▪ Report02.html o ChapterHierarchy.xml o Log.xml o ObjectInfo.xml o Report02.docx o ReportInfo.xml

5.9.17 Authenticating Using Security Assertion Markup Language 2.0

You can use Security Assertion Markup Language 2.0 authentication (SAML 2.0 authentication) as a global setting for authentication in SAP Disclosure Management. When a Web browser or an SAP Disclosure Management client sends an authentication request to the SAP Disclosure Management application server, the system follows the authentication steps as shown below:

> ⓘ Note
>
> SAML 2.0 authentication requires HTTPS.

The process steps are as follows:



- Authenticating Using Security Assertion Markup Language 2.0 [page 72]
- Authenticating Using Security Assertion Markup Language 2.0 [page 72]
- Authenticating Using Security Assertion Markup Language 2.0 [page 72]
- Authenticating Using Security Assertion Markup Language 2.0 [page 72]
- Authenticating Using Security Assertion Markup Language 2.0 [page 72]
- Authenticating Using Security Assertion Markup Language 2.0 [page 72]
- Authenticating Using Security Assertion Markup Language 2.0 [page 72]

1. The client sends a request to the application server.
2. The application server redirects the user request to the defined identity provider (IDP).
3. The redirect works by creating an SAML request and sending this request to the IDP.
4. The IDP follows its configured steps to authenticate the user.
5. The IDP sends an SAML response back to the application server.
6. If the SAML response is a valid response with a successful authentication result, the application server tries to map the received authentication information to the defined SAP Disclosure Management user. If the mapping is successful, the application server tries to authenticate the mapped user in the SAP Disclosure Management database. This is an internal authentication. The internal authentication is considered to be successful if the following statements apply:
   - The mapped user is a valid user in the SAP Disclosure Management database.
   - The user account of the mapped user is active.
7. If the internal authentication is successful, the application server creates a signed SSO token, which is used to authenticate the user against other application servers and data sources in the landscape.

5.9.17.1 Enabling Security Assertion Markup Language (SAML) in SAP Disclosure Management

To enable SAML in SAP Disclosure Management (SAP DM) complete the following processes:

1. Creating and importing a certificate
2. Updating the web.Config file

> ### Note
>
> Before you enable SAML in SAP Disclosure Management, ensure that there is at least one SAML user in the system who has the authority to assign all necessary permissions to other users. In addition, ensure that the business role *Assignment Role* , in the Fiori Launchpad, has been assigned to a SAML user. By default, this role is assigned to the admin user.

1. The SAP DM server can create its own SAML tokens. These tokens are generated based on the original SAML token that the server received from the defined identity provider. These newly generated tokens must be signed with a server certificate to ensure that they are trustworthy. To create a server certificate, you can use the Windows tool `makecert.exe`.

   > ### Example
   >
   > ```
   > makecert.exe c:\temp\DisclosureManagement.crt -r -pe -n
   > "CN=DisclosureManagement" -a sha1 -e 01/01/2019 -eku 1.3.6.1.5.5.7.3.2 -ss My
   > -sr localmachine
   > ```
   >
   > This creates a certificate that is stored in the local computer's personal certificate folder. The certificate is also stored in the C.\temp path.
   >
   > > ### Note
   > >
   > > SAP DM supports the SHA-1 and SHA256 algorithms, but not MD5. Make this setting accordingly. You have to define the Issuer Name of the local SAP DM signing certificate with the -n parameter. This name must conform to the X.500 standard as in the example above.

2. To enable SAML authentication for the SAP DM server, update the web.Config file in the website's root folder. The config file is XML based and you have to add a new XML node at the end of the file.

   > ### Note
   >
   > In the certificate creation example described above, the value of `SAMLLocalDMCertificateIssuerName` would correspond to `DisclosureManagement` or `CN=DisclosureManagement`.

```
<applicationSettings>
    <cundus.enterpriseReporting.Web.Properties.Settings>
      <setting name="SAMLIdentityProviderURL" serializeAs="String">
        <value>https://<tenantsub>.accounts.ondemand.com/saml2/idp/sso/
<tenantsub>.accounts.ondemand.com</value>
      </setting>
      <setting name="SAMLIdentityProviderCertificatePath" serializeAs="String">
        <value>D:\****\IdentityProviderPublicCertificate.cer</value>
      </setting>
      <setting name="SAMLUserIdentifier" serializeAs="String">
```

```
        <value>mail</value>
      </setting>
      <setting name="SAMLAuthenticationEnabled" serializeAs="String">
        <value>true</value>
      </setting>
      <setting name="SAMLIssuer" serializeAs="String">
        <value>yourhostname</value>
      </setting>
      <setting name="SAMLLocalDMCertificateIssuerName" serializeAs="String">
        <value>DisclosureManagementSAMLTestCert</value>
      </setting>
      <setting name="SAMLUseRequestSignature" serializeAs="String">
        <value>True</value>
      </setting>
    </cundus.enterpriseReporting.Web.Properties.Settings>
  </applicationSettings>
```

Related Information

http://msdn.microsoft.com/en-us/library/windows/desktop/aa386968(v=vs.85).aspx

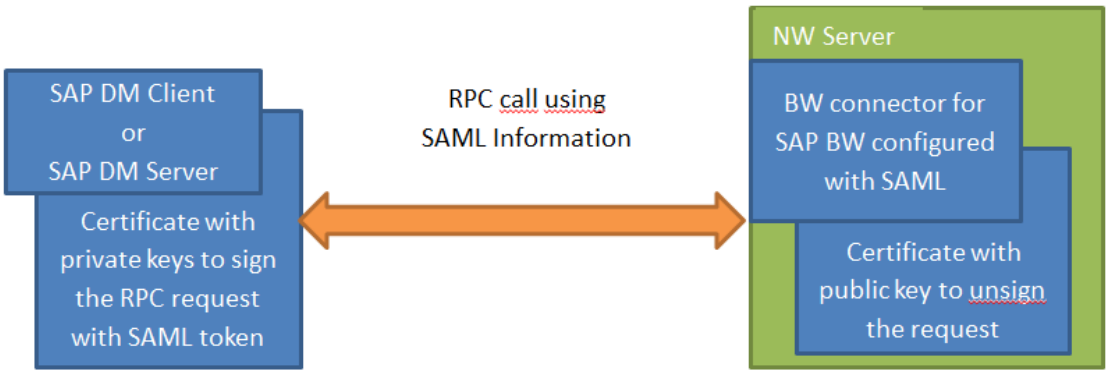
5.9.17.2 Using Security Assertion Markup Language (SAML) for the Connection Between SAP Disclosure Management (SAP DM) and SAP Business Warehouse (SAP BW)

You can also use SAML with your BW connector. To do so, you have to do the following:

- Enable your SAP Disclosure Management (SAP DM) server with SAML authentication.
- Configure the Web services on your BW connector.
  You must use the procedure *Sender-Vouches Subject Confirmation Method* and authorize the user to use the Web services. For more information on configuring SAML for SAP BW, see SAP Note 2117679.

> **Note**
>
> To determine whether the BW datasource uses SAML or not, the web.config file SAMLUseBasicAuthforBW is used. For more information, see Configuring SAML Authentication Using SAP IAS Tenant [page 77].

The figure below shows this process.



- When the user checks out a chapter from the SAP DM server, the SAML information is passed from the SAP DM server to the SAP DM client via the document. The user identifier is extracted from this information and is then used by the SAP DM client to communicate with the BW connector.

> ⓘ Note
>
> SAML authentication only works when the document is checked out from the SAP DM server.

5.9.17.2.1 Managing Certificates on BW Connector

To be sent from the SAP Disclosure Management client or server, an SAML RPC request must be signed with a valid certificate with private keys. This certificate must then be imported with public keys on the BW connector. SAP Disclosure Management provides the following two possibilities for managing these certificates:

1. *Locally installed certificates for every client on the computer*
   To implement this scenario, the administrator creates a certificate with private keys and installs it on the certificate store of the computer of every SAP Disclosure Management (SAP DM) client or server. This certificate will be used to sign the SAML request sent to the BW connector. The user who connects to the BW connector using SAML must have access rights to use this certificate with private keys from the local computer key store. This certificate must then be imported with public keys to the BW connector.
2. *Centralized certificates on the SAP DM server for all clients*

To implement this scenario, the administrator must create a certificate with private keys and install it on the certificate store of the computer where the SAP DM server is installed. This scenario only works if every SAP DM client that connects to the BW connector first establishes a server-side connection to the SAP DM server to connect and get all the data sources from the SAP DM server. In this case the *config20.xml* file from the server is used. Normally, the client then connects to any BW data source from the list using SAML. The certificate used for signing the SAML token is provided by the SAP DM server upon request by a client.

This procedure works in the background with no local data persistence. The advantage of this scenario is that the administrator needs to create only a single certificate and import it to the BW connector, instead of having to create a certificate for every SAP DM client.

To use this scenario, you must ensure that the following certificate requirements are fulfilled:

1. The certificate must be created or imported on an SAP DM server with private keys.

2. The user running the application pool connected to the SAP DM server must have access rights to use the certificate. You can provide the access rights by using the following procedure:
    1. Make sure the certificate is installed in the local computer store.
    2. Enter `mmc.exe`.
    3. Add the certificates snap-in to the console and choose a computer account on the local computer.
    4. Expand the certificates by choosing *Personal* > *Certificates* and locate the certificate for which you want to grant read permissions for private keys.
    5. Right-click the certificate, then choose *All Tasks* > *Manage Private Keys*, which starts a standard Windows ACL editor. Unless changed by admin, the application pools run the SAP DM server with network service account privileges by default. You have to grant network service read rights. If you are running your application pool under another identity or performing impersonation, you need to adapt the rights accordingly.
3. The certificate must be marked as exportable. This setting can be made during creation of the certificate or while exporting, by selecting *Mark key as exportable*.

5.9.17.3 Configuring SAML Authentication Using SAP IAS Tenant

Prerequisites

The SAP Cloud Identity Services - Identity Authentication (IAS) tenant must be available.

Scenario and Abbreviations

- SAP Disclosure Management (DM) acts as a Service Provider (SP) in the SAML scenario.
- SAP Cloud Identity Services - Identity Authentication (IAS) acts as an Identity Provider (IDP) in the SAML scenario.

SAML Signing Certificate Creation

On the Disclosure Management Application Server (Service Provider), a certificate is required to sign authentication requests for the IDP.

A self-signed certificate can be generated with a PowerShell script:

Sample Code

```
Generate Cert
 $makecert = @{ Subject = 'CN=DisclosureManagementSAMLTestCert';
```

```
KeyLength = 2048;
HashAlgorithm = 'SHA256';
KeyUsage = 'DigitalSignature';
KeyExportPolicy = 'Exportable';
KeySpec = 'Signature';
NotAfter = (Get-Date).AddYears(2) ;
TextExtension = '2.5.29.37={text}1.3.6.1.5.5.7.3.2'; }
New-SelfSignedCertificate @makecert
```

⚠ Caution

Do not use the same certificate as the one used for HTTPS.

IAS Tenant Configuration

Connect to the IAS tenant admin console via the link provided during the tenant creation.

User Management

IAS has its own user storage and management. You can also connect other IDPs or user storages. Please see the documentation available on SAP Cloud Identity Services - Identity Authentication.

Navigate to *Applications & Resources* > *Applications*. To add SAP Disclosure Management as a new application, click *Create* and provide a unique description.

Select the newly created application and click *SAML 2.0 Configuration*. Enter the following information:

Setting	Value	Details
Name	Host name of the DM application	This setting must match the DM `web.config` setting `SAMLIssuer`.
Assertion Consumer Service Endpoint	`https://hostname:port/Account/GetSAMLResponse`	After user authentication, the IDP will redirect to this URL.
Single Logout Endpoint		
URL	(HTTP-POST) `https://hostname:port/Account/Logout`	The URLs of the service provider single log-out endpoints that receive logout messages.
Response URL	`https://hostname:port/Account/SAMLLoggedOut`	-
Signing certificate	File or text	Upload the service provider's public certificate. You can get it by exporting the certificate as a base64 in CER format from the certificate store. The certificate is used by the IDP to validate requests from the service provider.
Signing options		

Setting	Value	Details
Signing algorithm	SHA-256	Match the certificate creation hash algorithm.
Sign assertions	ON (recommended)	SAML assertions are signed with the IDP certificate.
Sign authentication responses	ON (recommended)	SAML authentication responses are signed with the IDP certificate.
Require signed auth requests	ON (recommended)	SAML authentication requests from the service provider are required to be signed with the service provider certificate.

Select the newly created application and click *Subject Name Identifier*. In most cases you must select the email as the basic attribute.

Tenant Settings

1. Navigate to *Applications & Resources* > *Tenant Settings* > *SAML 2.0 Configuration*.
2. Under *Signing Certificates*, click the *Display* action on the main certificate.
3. Copy the certificate information value (base64) and paste it into a new file. Rename the file to, for example, "IAS tenant public.cer". This file will be required for the *SAMLIdentityProviderCertificatePath* setting in the SAP Disclosure Management SAML configuration.

DM Application Server Configuration

Create SAML Users for Mapping

SAP Disclosure Management has its own user management independent from any other user store with application-specific authorizations. To map IDP users to SAP Disclosure Management users, you must create users in the application user management as well. For more information, see User Administration [page 21]. To create SAML users, you must enable SAML authentication.

Prepare the default admin (basic authentication) user by filling the `Incoming User Identifier`. The incoming user identifier must match the setting of the `IDP Subject Name Identifier` with the format `SubjectNameIdentifier=Value`.

Example

If you configure the IDP to use the `Mail` property as its user identifier, you must configure for every DM user an incoming user identifier as follows: `mail=user.name@domain.com`.

Additionally, you must edit the `SAMLUserIdentifier` setting in the application `web.config` file as follows:

Sample Code

```
<setting name="SAMLUserIdentifier" serializeAs="String">
        <value>mail</value>
      </setting>
```

Configure SAML

SAP Disclosure Management SAML 2.0 configuration is done by editing the application `web.config` file in the root of the web application folder:

Sample Code

```
<applicationSettings>
    <cundus.enterpriseReporting.Web.Properties.Settings>
      <setting name="SAMLIdentityProviderURL" serializeAs="String">
        <value>https://<tenantsub>.accounts.ondemand.com/saml2/idp/sso/
<tenantsub>.accounts.ondemand.com</value>
      </setting>
      <setting name="SAMLIdentityProviderCertificatePath"
serializeAs="String">
        <value>D:\****\IdentityProviderPublicCertificate.cer</value>
      </setting>
      <setting name="SAMLUserIdentifier" serializeAs="String">
        <value>mail</value>
      </setting>
      <setting name="SAMLAuthenticationEnabled" serializeAs="String">
        <value>true</value>
      </setting>
      <setting name="SAMLIssuer" serializeAs="String">
        <value>yourhostname</value>
      </setting>
      <setting name="SAMLLocalDMCertificateIssuerName" serializeAs="String">
        <value>DisclosureManagementSAMLTestCert</value>
      </setting>
      <setting name="SAMLUseRequestSignature" serializeAs="String">
        <value>True</value>
      </setting>
     <setting name="SAMLParserPreserveWhitespace" serializeAs="String">
       <value>False</value>
     </setting>
    </cundus.enterpriseReporting.Web.Properties.Settings>
  </applicationSettings>
```

Setting	Value	Description
`SAMLAuthenticationEnabled`	**`True`** or **`False`**	Enables or disables the SAML authentication feature of SAP Disclosure Management. If you enable this setting, you will not be able to log in via Active Directory or basic authentication. Make sure to complete the configuration and user creation before enabling this setting.
`SAMLIssuer`	string	Usually the host name of the service provider application. It matches the `Name` setting in the IDP application SAML 2.0 configuration.
`SAMLIdentityProviderURL`	URL	The URL to the IDP log-in endpoint. Check the IDP admin console under *Applications & Resources* > *Tenant Settings* > *SAML 2.0 Configuration* to find the URL for the SSO endpoint.

Setting	Value	Description
`SAMLIdentityProviderCertificatePath`	`local file path, e.g. D:\certificates\certificate.cer`	Path to the IDP public certificate on the application server file system. The web application pool user (usually group "IIS_IUSRS") must have read access to this folder.
`SAMLUserIdentifier`	string	Defines the incoming SAML assertion user identifier name.
`SAMLLocalDMCertificateIssuerName`	string	Name of the certificate in the windows certificate store.
`SAMLUseRequestSignature`	**`True`** or **`False`**	Enables or disables the signing authentication request with the service provider certificate so that the IDP can validate the request.
`SAMLUseResponseValidation`	**`True`** or **`False`**	Enables or disables IDP response validation with the IDP public certificate.
`SAMLUseBasicAuthforBW`	**`True`** or **`False`**	Enables or disables SAML authentication with external BW data sources and uses basic authentication instead.
`SAMLParserPreserveWhitespace`	**`True`** or **`False`**	Enables or disables that SAML Response from IDP is parsed while preserving whitespaces in SAML XML. Changing this setting can help in case of SAML response validation problems for specific IDPs.

5.9.18 Enabling Active Directory Authentication

This section describes how to enable Single Sign-On Active Directory (SSO AD) authentication after the installation of SAP Disclosure Management with basic authentication.

Web.config

In the Web.config, make the following changes:

1. In the section `<system.web>`, change the authentication setting from `<authentication>` to `<authentication mode=”Forms”>`.
2. In the `<forms>` tag of the `<authentication>` setting, change the login URL (loginUrl) from `/Account/LogOn` to `/Account/LogOnAD`.

The result should look like this:

```
<system.web>
```

```
   <!– Enable forms authentication -->
```

```
   <authentication mode="Forms">
```

```
    <forms loginUrl="/Account/LogOnAD" defaultUrl="/Report/Index">
```

```
  </authentication>
```

Windows Server

Open a command line with administrator rights on the Windows Server that hosts the SAP Disclosure Management website and run the following commands:

- **`%windir%\system32\inetsrv\appcmd.exe unlock config /section:anonymousAuthentication`**
- **`%windir%\system32\inetsrv\appcmd.exe unlock config /section:windowsAuthentication`**

This will unlock the config sections of the Internet Information Services (IIS) that are locked by default and that are required to use Active Directory (AD) authentication.

IIS Application Pool

Every SAP Disclosure Management website is assigned to a specific IIS application pool. This application pool runs under a specific identity. In a basic authentication environment, the application pool runs under a built-in account as identity.

In most cases, this account does not have read access to the according AD controller. Therefore, it is necessary to specify a custom account with read access to the AD controller or assign read access to the used built-in account.

To change the application pool identity settings, start the IIS Manager, then navigate to *Application Pools*, and select the relevant application pool of the SAP Disclosure Management website. Select *Advanced Settings...* and define or check the *Identity* in the *Process Model* section.

6 Task Engine

You use this service to perform long-running and resource-consuming tasks in SAP Disclosure Management. The task engine is a Microsoft Windows service that enables you to decouple resource-consuming tasks from the SAP Dislcosure Management server application running on the Microsoft Internet Information Server (IIS), thus avoiding performance impairments when working with SAP Disclosure Management.

Installation

To use the task engine you have to install the task engine. The installation folder for the task engine is:

```
C:\Program Files (x86)\SAP\SAP DisclosureManagement TaskEngine
```

After the installation you have to start the service manually.

Alternatively, you can run the task engine in a Windows console instead of using it as a service. To do this, navigate to the installation folder of the task engine and start

```
SAP.DM.TaskEngine.Console.exe
```

To stop the task engine, activate the console window and press *Enter*.

> **Note**
>
> You need local administrator rights to execute the console application. For Windows Server 2008/2008 R2, start the console application with *Run as administrator*.

Change Web service URL

The task engine provides a Web service, which allows the SAP Disclosure Management server application to create the required task. After installation the Web service is accessible using the URL `http://[ip address or DNS name]:[port]/TaskEngineService` .

> **Example**
>
> The default example is `http://localhost:2605/TaskEngineService`.

If you want to change the URL, follow the steps below:

1. In Windows Explorer, navigate to the task engine installation folder.
2. Open the configuration files *SAP.DM.TaskEngine.WinService.exe.config* and *SAP.DM.TaskEngine.Console.exe.config*.
3. Search for the configuration setting `<baseAddresses><add baseAddress="..."/></baseAddresses>`. Change the value `baseAddress` according to your requirements.
4. Modify the connected setting in Disclosure Management server configuration under *Administration* > *Server configuration* > *Misc* > *TaskEngine Web Service* .
5. Restart the task engine Windows service.

Logging

The task engine writes all detected application errors to a log file. You can configure the directory where the log files are stored by using the file *Log.config*. After installation, the directory for the log files points to `%ALLUSERSPROFILE%\SAP\SAP DM TaskEngine\Logs`.

Troubleshooting

If the task engine Windows service runs, but tasks are not processed, this may result in an error with the polling database being stopped, for example, the MS SQL server can no longer be reached. You then have to investigate the log files as described below:

1. Open the latest task engine log file *[date].log*.
2. Search for the log entry *QueueAgent detected an error!*
3. The related error message is displayed below the entry.
4. Correct the error and restart the task engine.

7 High Availability

To ensure high availability (HA), efficiently manage incoming server requests, and eliminate single points of failure for SAP Disclosure Management, you should consider the following recommendations when you design your configuration:

- Install multiple application servers (that is, create server tiers).
- Use a hardware or software load balancer to manage incoming traffic for the application server.
- Implement the Microsoft SQL Server solutions for high availability and fail-over for your clustered servers.
- Implement the Content Refresh API
  For more information see Calling the Content Refresh API Method [page 97].

For more information about SAP Disclosure Management architecture, see the *Installation and Upgrade Guide* for SAP Disclosure Management. .

Components With Single Point of Failure

Component	Detailed Description	HA Setup Description
SAP Disclosure Management BW connector	Provides financial data from SAP BW.	For more information, see the sections about High Availability (AS ABAP) in the *Technical Operations Guide for SAP NetWeaver* at : http://help.sap.com/netweaver.
SAP Disclosure Management server	Provides the core application for all scenarios.	For more information, see the Microsoft product documentation of the following servers: • Database: Microsoft SQL Server HA concepts • Application: Microsoft Windows Server HA concepts

Each of the components, listed in the table above, can be a single point of failure in this scenario. To achieve HA for the complete scenario, it is necessary that all components with single points of failure are set up with HA.

8 Software Change Mangement

8.1 Transport and Change Management

The system administrator can use the Transport function to perform transports between your development, test, and production environments. All systems should have the same stack installed. You can transport files from different stacks but we can't guarantee full compatibility.

For more information about transporting content, see the chapter *Import and Export of Content in SAP Disclosure Management* in the user help.

Business users create periods, reports, chapters, and content in the production system. You can refresh your test system from the production system with backup and restore. Remember that security profiles are transferred as well, so make any necessary changes after the restoration.

> **Note**
>
> If you transport users to another SAP Disclosure Management system where these users do not yet exist, you can define a default initial password:
>
> 1. In SAP DM, choose *Administration* > *System Configuration* > *Transport*.
> 2. The initial password has to be changed when the user logs on for the first time.
>
> > **Note**
> >
> > Importing a user that already exists in the target system does not set the user's password to the initial password, but keeps the existing password. The initial password is only used for users that do not yet exist in the target system.

8.2 Support Packages and Patch Implementation

SAP Disclosure Management support packages are available on the SAP Support Portal (https://support.sap.com/swdc). Each Support Package is linked to an individual SAP Note.

A description of the Support Package and the installation instructions are included in the note. Support Packages are cumulative, meaning that each subsequent Support Package contains fixes from all prior Support Packages since the last major release. For example, SAP Disclosure Management 10.0 SP03 would contain fixes included in SAP Disclosure Management 10.0 SP01 and SP02. You must install the preceding major release (that is, 10.0) before installing a Support Package.

Support Packages are typically installed on the application server.

SAP Disclosure Management 10.0 does not support SAP Solution Manager Maintenance Optimizer or the `Note Assistant` at this time.

8.3 SAP Disclosure Management Installation and Migration Tool

As of SAP Disclosure Management Application Server 10.1 SP06, you can use the installation and migration tool, which is part of the application server software component. This tool takes over several procedures which must be carried out after a new installation or after an installation update of SAP Disclosure Management Application Server.

For example, these procedures migrate datalink metadata from earlier software versions to later versions, creating and expanding database tables and a lot more. The first step to prepare the SAP Disclosure Management installation tool is to create a `dbconnect.temp` file under the `\bin` folder of the installation directory of the SAP Disclosure Management Application Server. The procedure is as follows:

1. Open Windows Explorer and open the `\bin` directory of the SAP Disclosure Management instance.
2. Create a new `dbconnect.temp` text file within the `\bin` directory. The file must contain a valid database connection string for the used SAP Disclosure Management instance database. In order to add the connection string to the `dbconnect.temp` file, you can use the pattern below, where all <...> placeholders must be replaced by valid values:

   {·} Sample Code

   ```
   Data Source=<SQL Server Name>;Initial Catalog=<Database Name>;Integrated
   Security=False; User Id=<Database User Name>; Password=<Database User
   Password>;MultipleActiveResultSets=True
   ```

The `dbconnect.temp` file is required for making changes in the database by executing the installation tool. These changes can only be done by an administrative database user who has sufficient permissions to execute structure-manipulating SQL commands directly on the database level. In the example above, we used user *sa*, because it is a default database administrator user. You can also use a different user as long as they have the required administrative permissions.

8.3.1 Running the Installation Tool

Context

You can use the installation tool in either the installation or update modes. The number of installables, which will be processed by the installation tool differs between the two modes. The affected installables, required for the two modes, are contained in the installation or update batch files so that you do not need to take care of installing the corrrect installables yourself.

To run the installation tool follow the steps below:

Procedure

1. As an administrator, open the command prompt window on the Windows server where the SAP Disclosure Management Application Server instance has been installed. Then, change to `\bin` folder of the installation directory:

   Output Code

   ```
   C:\>cd "\inetpub\wwwroot\SAP\SAP DISCLOSURE MANAGEMENT Instance 2\bin"
   C:\inetpub\wwwroot\SAP\SAP DISCLOSURE MANAGEMENT Instance 2\bin>
   ```

2. To run the migration tool in the installation mode, type in the command **`install.bat`** at the command prompt.
3. Press enter to execute the command.
4. Alternatively, to run the migration tool in the update mode, type in the command **`install_update.bat`** .
5. Press enter to execute the command.

8.3.2 Custom Execution of Installables

A number of installables are provided as a package depending on the software release version of the SAP Disclosure Management. Each installable can be run using the SAP Disclosure Management installation tool with specific parameters at the command line.

The following command line parameters are defined:

Parameter	Description
`/i`	Defines the installable package to be executed, for example, **`DM101SP06PL00`** for SAP Disclosure Management 10.1 SP06 Patch 0.
`/p`	Defines the output directory for log files written during installation tool execution.
`/conStrFileName`	Defines the path to the database connect string file, e.g. `dbconnect.temp` file.
`/update`	Executes the installation tool in update mode.

Example

To run the SAP Disclosure Management installation tool for installation of 10.1 SP06 Patch 1 installable, use the command prompt: `install.exe /i:DM101SP06PL01 /p:"..\Logs\Install Log" /conStrFileName:"..\bin\dbconnect.temp"`

The 10.1 SP06 Patch 1 installable package will be executed and a log file will be written to the current execution path under the `\Logs\Install Log\` folder. The database connect string file used is `dbconnect.temp` under the current execution path and `\bin` folder.

9 Troubleshooting

Issue	Solution
If you have made any changes to a Microsoft Office Excel document tagged with the Report Builder and click  *Apply Changes* or  *Discard Changes*, a dialog box asks you whether you want to save.	Click *OK*. If you do not want the dialog box to appear, you can save the file using the standard *Save* function in Microsoft Office Excel.
In Microsoft Office Word or Microsoft Office Excel, a Microsoft Office Excel object is embedded, but it cannot be opened. An error message is received from the host, but otherwise nothing happens.	This issue can occur when third-party COM add-ins are installed. We recommend you to temporarily disable the COM add-in in Microsoft Office Excel.
In Microsoft Office PowerPoint, the refresh of datalinked objects does not work properly.	This issue can occur if you use the Report Builder or the SAP EPM solutions, add-in for Microsoft Office (EPM add-in) in combination with Microsoft Office PowerPoint. Before refreshing data in Microsoft Office PowerPoint, do one of the following, depending on which application is installed: • Deinstall the Report Builder from your client. • Deactivate the EPM add-in.
The insertion of a new Microsoft Office Excel object in a Microsoft Office PowerPoint presentation does not work properly.	This issue can occur if you use the Report Builder in combination with Microsoft Office PowerPoint. Deinstall the Report Builder from your client.
You have checked out a Microsoft Office document and closed the document, but you want to continue working on the document. In the first dialog box, you have clicked *Cancel*. In the next dialog box, you have clicked *No*. The document is closed, not saved, and still checked out.	You cannot undo this action. To prevent data loss, do the following: 1. In the first dialog box, click *Cancel*. 2. In the next dialog box, click *Cancel*.
You have added extra columns to the write back preview window and used the *Expand all* or *Collapse all* options. The following issues can occur: • The top of the report tree is no longer displayed. • The vertical scroll bar is no longer displayed.	Resize the preview window.

10 Support Desk Management

Support Desk Management enables you to set up an efficient internal support desk for your support organization that seamlessly integrates your end users, internal support employees, partners, and SAP Active Global Support specialists with an efficient problem resolution procedure.

For support desk management, you need the methodology, management procedures, and tools infrastructure to run your internal support organization efficiently.

10.1 Problem Message Handover

Problem messages can be logged at the SAP Support Portal, located on *SAP Service Marketplace* at the following site:http://service.sap.com.

You can use component strings to efficiently direct your support message related to SAP Disclosure Management.

The table below shows the relevant component strings.

Component Strings for Support Messages

Component	Area	Additional Information to Be Delivered
EPM-DSM	SAP Disclosure Management	Not applicable
EPM-DSM-ADM	Administration	Not applicable
EPM-DSM-AUT	Authorization	Not applicable
EPM-DSM-BWC	BW Connector	Which SAP BW version is being used?
EPM-DSM-DOC	Documentation	Not applicable
EPM-DSM-DSC	Data sources	Which data source is being used?
EPM-DSM-INF	Infrastructure	Which Microsoft platform in which version is being used: • Microsoft Windows Server • Microsoft SQL Server
EPM-DSM-INS	Installation	Which SAP Disclosure Management version shall be installed? Is this an upgrade installation? If yes, from which version?

Component	Area	Additional Information to Be Delivered
EPM-DSM-PPT	Microsoft Office PowerPoint	Which Microsoft Office PowerPoint version is being used?
EPM-DSM-WEB	Web	Which Web Browser is being used?
EPM-DSM-WFL	Workflow	Not applicable
EPM-DSM-WRD	Microsoft Office Word	Which Microsoft Office Word version is being used?
EPM-DSM-XBF	XBRL Factory	Not applicable
EPM-DSM-XRB	Report Builder	Which Microsoft Office Excel version is being used?
EPM-DSM-XTD	Taxonomy Designer	Not applicable
EPM-DSM-XLS	Microsoft Office Excel	Which Microsoft Office Excel version is being used?

11 Appendix

11.1 Service Interfaces for SAP Disclosure Management

You can implement RESTful APIs to create client applications that use SAP Disclosure Management functionality. Currently, the APIs are intended to work only with the authorization concepts in SAP Disclosure Management, and can be used for the following tasks:

- Retrieve and set user information and also create new users in the SAP Disclosure Management system
- Retrieve a list of entities from the SAP Disclosure Management system
- Retrieve a list of the roles available in the SAP Disclosure Management system
- Retrieve a list of the periods available in the SAP Disclosure Management system
- Retrieve a list of the reports available in a period
- Retrieve a list of the chapters available in a report
- Retrieve a list of a user's global permissions and also assign new global permissions or delete existing global permissions
- Retrieve a list of a user's local permissions and also assign new local permissions or delete existing local permissions at report or chapter level

> **Note**
>
> The Disclosure Management APIs are described in the SAP Disclosure Management RESTful APIs Swagger documentation. You can find the Swagger documentation in `<Installation Root of SAP Disclosure Management>/Content/Webapi`.
>
> To display the Swagger Files, you must install Swagger UI. For more information, visit https://swagger.io/ .

11.1.1 Code Samples

The SAP Disclosure Management RESTful APIs use OAuth to authenticate users. Users must have an access token to make calls to the APIs. The timeout for the access token one day.

> **Note**
>
> Please make sure to remove any cookies when making API calls. Cookies indicate an UI interaction and require additional security measures, for example, to prevent Cross-Site Request Forgery (CSRF).

C# Code Snippet for Authenticating Users and Getting Bearer Access Token

The sample below shows how to get the access token, followed by an example of a GET call to retrieve a list of users from the SAP Disclosure Management system.

Code Sample for Reuse

Sample Code

```
using System.Net.Http;
using System.Text;
using System.Text.Json;
using System.Threading.Tasks;
public static async Task<string> AuthenticateAsync(string apiBaseUri, string
username, string password)
{
    var tokenEndpoint = new Uri(new Uri(apiBaseUri), "api/Authenticate");
    var jsonBody = new { Username = username, Password = password }; //
Define an anonymous object for the request payload
    var content = new StringContent(
        JsonSerializer.Serialize(jsonBody),
        Encoding.UTF8,
        "application/json"
    );
    using (var client = new HttpClient())
    {
        HttpResponseMessage response = await client.PostAsync(tokenEndpoint,
content);
        if (!response.IsSuccessStatusCode)
        {
            // Get the error message
            var errorContent = await response.Content.ReadAsStringAsync();
            throw new Exception($"Error {response.StatusCode}:
{errorContent}");
        }
        // Try to retrieve the access token from headers
        if (response.Headers.TryGetValues("access_token", out var values))
        {
            return values.FirstOrDefault();
        }
        throw new Exception("Access token not found in response headers.");
    }
}
```

Once an access token is obtained, future calls to any of the RESTful APIs can use this access token for authentication.

C# Code Snippet for getting User Information from the System with Authentication Using Bearer Access Token

Note

You should delete the bearer token on the client after use. This prevents misuse of the token.

Code Sample for Reuse

Sample Code

```
/* Snippet: /api/Users - Get all user information from Disclosure Management
System */
using (var client = new HttpClient())
{
    client.BaseAddress = new Uri(apiBaseUri);
    client.DefaultRequestHeaders.Accept.Clear();
    client.DefaultRequestHeaders.Accept.Add(new
System.Net.Http.Headers.MediaTypeWithQualityHeaderValue("application/json"));
    // Add the access_token in the header of the request
    client.DefaultRequestHeaders.Add("access_token", accessToken);
    try
```

```
    {
        // Use async/await pattern for proper asynchronous operations
        HttpResponseMessage response = await client.GetAsync("api/Users");
        if (!response.IsSuccessStatusCode)
        {
            string errorContent = await response.Content.ReadAsStringAsync();
            throw new Exception($"Error: {errorContent}");
        }
        // Read the response content and process it if the call is successful
        string responseContent = await response.Content.ReadAsStringAsync();
        // Task(s) to perform when the call is successful
        // Example: Logging, parsing JSON, etc.
        // ...
    }
    catch (Exception ex)
    {
        // Handle exceptions (e.g., logging)
        Console.WriteLine($"An error occurred: {ex.Message}");
        throw;
    }
    finally
    {
        // Recommended: Cleanup sensitive data to prevent memory leak attacks
        accessToken = null;
    }
}
```

Powershell Script for Deleting User Information from the System with Authentication Using Bearer Access Token

Code Sample for Reuse

Sample Code

```
# API Server details
$baseUrl = 'http://servername:8080/'
$apiAuthenticate = "${baseUrl}api/Authenticate"
$apiDeleteData = "${baseUrl}api/DeletePersonalData"
# Admin credentials
$user = 'AdminLogin'
$pw = 'Password'
# Authenticate and get access token
try {
    $authParams = @{username = $user; password = $pw} | ConvertTo-Json -Depth
2
    $authResponse = Invoke-WebRequest -Uri $apiAuthenticate -Method Post
-Body $authParams -ContentType 'application/json'
    if ($authResponse.StatusCode -eq 200) {
        $accessToken = $authResponse.Headers['access_token']
        Write-Host "Authorization token obtained."
    } else {
        Write-Host "Error during authentication: HTTP $
($authResponse.StatusCode)"
        exit 1
    }
} catch {
    Write-Host "Exception during authentication: $_"
    exit 1
}
# Prepare headers and body for DeletePersonalData API
$headers = @{
    Authorization  = "Bearer $accessToken"
    "Content-Type" = "application/json"
    "Accept-Language" = "en-EN"
}
$deleteBody = @{UserLogin = 'user1'} | ConvertTo-Json -Depth 2
```

```
# Perform personal data deletion
try {
    $deleteResponse = Invoke-WebRequest -Uri $apiDeleteData -Method Post
-Headers $headers -Body $deleteBody -ContentType 'application/json'
    if ($deleteResponse.StatusCode -eq 200) {
        Write-Host "Deletion of personal data done."
    } else {
        Write-Host "Error during deletion: HTTP $($deleteResponse.StatusCode)"
        exit 1
    }
} catch {
    Write-Host "Exception during deletion: $_"
    exit 1
}
```

Powershell Script for Content Refresh of a Report with Authentication Using Bearer Access Token

Code Sample für Reuse

Sample Code

```
$SystemEndpoint = 'http://servername:8080'
$Username = 'AdminLogin'
$Password = '*****'
$OutputFile = "C:\temp\DMRefreshProtocol3.txt"
# Log start of the script
"Running PowerShell script: refresh_chapters" | Set-Content -Path $OutputFile
"Check file 'c:\temp\DMRefreshProtocol3.txt'" | Add-Content -Path $OutputFile
# Authenticate to the system
try {
    $AuthPayload = @{ username = $Username; password = $Password } |
ConvertTo-Json
    $AuthResponse = Invoke-WebRequest -Uri "$SystemEndpoint/api/Authenticate"
-Method Post -Body $AuthPayload
    if ($AuthResponse.StatusCode -ne 200) {
        throw "Authentication failed with status code: $
($AuthResponse.StatusCode)"
    }
    $AccessToken = $AuthResponse.Headers.access_token
    "Authorization token obtained" | Add-Content -Path $OutputFile
} catch {
    "Error during authentication: $_" | Add-Content -Path $OutputFile
    exit 1
}
# Start refreshing content
try {
    "Starting content refresh..." | Add-Content -Path $OutputFile
    $Headers = @{
        access_token    = $AccessToken
        "Content-Type"  = "application/json"
        "Accept-Language" = "en-EN"
    }
    $RefreshPayload = @{
        ReportName  = 'report1'
        PeriodName  = 'period1'
        Datasources = 'DM server Stack 1100 (basic),ct,ct|P28 NW
7.31,erp,erp1234'
    } | ConvertTo-Json
    $RefreshResponse = Invoke-WebRequest -Uri "$SystemEndpoint/api/
ContentRefresh" -Headers $Headers -Method Post -Body $RefreshPayload
    if ($RefreshResponse.StatusCode -ne 200) {
        throw "Content refresh failed with status code: $
($RefreshResponse.StatusCode)"
    }
    "Content refresh successful" | Add-Content -Path $OutputFile
    $RefreshResponse.RawContent | Add-Content -Path $OutputFile
```

```
} catch {
    "Error during content refresh: $_" | Add-Content -Path $OutputFile
    exit 1
}
```

11.1.2 Calling the Content Refresh API Method

Context

Procedure

1. Run the PoweShell script Microsoft PowerShell. For more information, see Code Samples [page 93]. The script first authenticates the user. Then, the access token is used to call the refresh method with its parameters `Chaptername` (optionally) , `ReportName`, and `PeriodName`. Two data sources are used by the report chapters.
2. Large reports containing many chapters or a significant amount of data can block the system or the task engines. This is why you can run the content refresh function for multiple reports at night. The Microsoft Windows task scheduler calls the Microsoft PowerShell script after the working hours. Please note that the Internet Identification Service (IIS) must run when the API is called.
3. The system runs the general refresh asynchronously.

11.1.3 API Responses for Content Refresh

The following table contains HTTP API response codes for content refresh:

HTTP Response Code	HTTP Response Description	Possible reason of the response on:		
		Other level	Report	Chapter
200	OK	Content refresh successful		
400	Bad Request	Period not found.	Report not found.	Chapter not found. Workflow of chapter is not status to edit chapter.

HTTP Response Code	HTTP Response Description	Possible reason of the response on:		
403	Forbidden	Connection to data source failed.	Missing permission of 'Content Refresh'.	Missing permission 'Edit chapter'. Missing edit permission in a chapter according to its current workflow step and possible condition.
409	Conflict	/	Report is locked.	Chapter is already checked out.

11.1.4 Values Supported for the TimeZone Field When Creating New Users

Name of Time Zone	Time
Dateline Standard Time	(GMT-12:00) International Date Line West
Samoa Standard Time	(GMT-11:00) Midway Island, Samoa
Hawaiian Standard Time	(GMT-10:00) Hawaii
Alaskan Standard Time	(GMT-09:00) Alaska
Pacific Standard Time	(GMT-08:00) Pacific Time (US and Canada); Tijuana
Mountain Standard Time	(GMT-07:00) Mountain Time (US and Canada)
Mexico Standard Time 2	(GMT-07:00) Chihuahua, La Paz, Mazatlan
U.S. Mountain Standard Time	(GMT-07:00) Arizona
Central Standard Time	(GMT-06:00) Central Time (US and Canada
Canada Central Standard Time	(GMT-06:00) Saskatchewan
Mexico Standard Time	(GMT-06:00) Guadalajara, Mexico City, Monterrey
Central America Standard Time	(GMT-06:00) Central America
Eastern Standard Time	(GMT-05:00) Eastern Time (US and Canada)
U.S. Eastern Standard Time	(GMT-05:00) Indiana (East)
S.A. Pacific Standard Time	(GMT-05:00) Bogota, Lima, Quito

Name of Time Zone	Time
Atlantic Standard Time	(GMT-04:00) Atlantic Time (Canada)
S.A. Western Standard Time	(GMT-04:00) Caracas, La Paz
Pacific S.A. Standard Time	(GMT-04:00) Santiago
Newfoundland and Labrador Standard Time	(GMT-03:30) Newfoundland and Labrador
E. South America Standard Time	(GMT-03:00) Brasilia
S.A. Eastern Standard Time	(GMT-03:00) Buenos Aires, Georgetown
Greenland Standard Time	(GMT-03:00) Greenland
Mid-Atlantic Standard Time	(GMT-02:00) Mid-Atlantic
Azores Standard Time	(GMT-01:00) Azores
Cape Verde Standard Time	(GMT-01:00) Cape Verde Islands
GMT Standard Time	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Greenwich Standard Time	(GMT) Casablanca, Monrovia
Central Europe Standard Time	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Central European Standard Time	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
Romance Standard Time	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
W. Europe Standard Time	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
W. Central Africa Standard Time	(GMT+01:00) West Central Africa
E. Europe Standard Time	(GMT+02:00) Bucharest
Egypt Standard Time	(GMT+02:00) Cairo
FLE Standard Time	(GMT+02:00) Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius
GTB Standard Time	(GMT+02:00) Athens, Istanbul, Minsk
Israel Standard Time	(GMT+02:00) Jerusalem
South Africa Standard Time	(GMT+02:00) Harare, Pretoria
Russian Standard Time	(GMT+03:00) Moscow, St. Petersburg, Volgograd

Name of Time Zone	Time
Arab Standard Time	(GMT+03:00) Kuwait, Riyadh
E. Africa Standard Time	(GMT+03:00) Nairobi
Arabic Standard Time	(GMT+03:00) Baghdad
Iran Standard Time	(GMT+03:30) Tehran
Arabian Standard Time	(GMT+04:00) Abu Dhabi, Muscat
Caucasus Standard Time	(GMT+04:00) Baku, Tbilisi, Yerevan
Transitional Islamic State of Afghanistan Standard Time	(GMT+04:30) Kabul
Ekaterinburg Standard Time	(GMT+05:00) Ekaterinburg
West Asia Standard Time	(GMT+05:00) Islamabad, Karachi, Tashkent
India Standard Time	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
Nepal Standard Time	(GMT+05:45) Kathmandu
Central Asia Standard Time	(GMT+06:00) Astana, Dhaka
Sri Lanka Standard Time	(GMT+06:00) Sri Jayawardenepura
N. Central Asia Standard Time	(GMT+06:00) Almaty, Novosibirsk
Myanmar Standard Time	(GMT+06:30) Yangon Rangoon
S.E. Asia Standard Time	(GMT+07:00) Bangkok, Hanoi, Jakarta
North Asia Standard Time	(GMT+07:00) Krasnoyarsk
China Standard Time	(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi
Singapore Standard Time	(GMT+08:00) Kuala Lumpur, Singapore
Taipei Standard Time	(GMT+08:00) Taipei
W. Australia Standard Time	(GMT+08:00) Perth
North Asia East Standard Time	(GMT+08:00) Irkutsk, Ulaanbaatar
Korea Standard Time	(GMT+09:00) Seoul
Tokyo Standard Time	(GMT+09:00) Osaka, Sapporo, Tokyo
Yakutsk Standard Time	(GMT+09:00) Yakutsk
A.U.S. Central Standard Time	(GMT+09:30) Darwin

Name of Time Zone	Time
Cen. Australia Standard Time	(GMT+09:30) Adelaide
A.U.S. Eastern Standard Time	(GMT+10:00) Canberra, Melbourne, Sydney
E. Australia Standard Time	(GMT+10:00) Brisbane
Tasmania Standard Time	(GMT+10:00) Hobart
Vladivostok Standard Time	(GMT+10:00) Vladivostok
West Pacific Standard Time	(GMT+10:00) Guam, Port Moresby
Central Pacific Standard Time	(GMT+11:00) Magadan, Solomon Islands, New Caledonia
Fiji Islands Standard Time	(GMT+12:00) Fiji Islands, Kamchatka, Marshall Islands
New Zealand Standard Time	(GMT+12:00) Auckland, Wellington
Tonga Standard Time	(GMT+13:00) Nuku'alofa

11.2 Related Information

The following table contains links to information relating to the Administrator's Guide.

Related Information

Content	Resources
Master Guide, Installation Guide, and Upgrade Guide	SAP Help Portal (http://help.sap.com)
Related SAP Notes	SAP Support Portal (https://support.sap.com/notes)
Released Platforms	SAP Support Portal (https://support.sap.com/en/release-upgrade-maintenance.html)
Network Security	SAP Help Portal (http://help.sap.com)
Technical Infrastructure	SAP Help Portal (http://help.sap.com)
SAP Solution Manager	SAP Solution Manager (https://support.sap.com/en/solution-manager.html)

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.