software AG

Managing Users with Common Directory Services

Version 10.15

October 2022

WEBMETHODS

This document applies to Common Directory Services 10.15 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: CDS-AG-1015-20221015

Table of Contents

About This Guide

This help explains how to configure Common Directory Services (CDS) and how to use the CDS user interfaces in Integration Server to manage users, groups, roles and access permissions in a webMethods installation.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Narrowfont	Identifies service names and locations in the format *folder.subfolder.service*, APIs, Java classes, methods, properties.
Italic	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Product Documentation

You can find the product documentation on our documentation website at https://documentation.softwareag.com.

In addition, you can also access the cloud product documentation via https://www.softwareag.cloud. Navigate to the desired product and then, depending on your solution, go to “Developer Center”, “User Center” or “Documentation”.

Product Training

You can find helpful product training material on our Learning Portal at https://knowledge.softwareag.com.

Tech Community

You can collaborate with Software AG experts on our Tech Community website at https://techcommunity.softwareag.com. From here you can, for example:

- Browse through our vast knowledge base.
- Ask questions and find answers in our discussion forums.
- Get the latest Software AG news and announcements.
- Explore our communities.
- Go to our public GitHub and Docker repositories at https://github.com/softwareag and https://hub.docker.com/publishers/softwareag and discover additional Software AG resources.

Product Support

Support for Software AG products is provided to licensed customers via our Empower Portal at https://empower.softwareag.com. Many services on this portal require that you have an account. If you do not yet have one, you can request it at https://empower.softwareag.com/register. Once you have an account, you can, for example:

- Download products, updates and fixes.
- Search the Knowledge Center for technical information and tips.
- Subscribe to early warnings and critical alerts.
- Open and update support incidents.
- Add product feature requests.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

1 Accessing Common Directory Services

To use and configure Common Directory Services, you log on to the Integration Server administration interface as the default Administrator user and the password, specified during installation, or another user that has administrative privileges. For more information about adding an administrator user in Integration Server, see *webMethods Integration Server Administrator's Guide*.

To access Common Directory Services

1. Go to the Integration Server administration interface available at http://localhost:5555/WmAdmin/.

2. Log on as an administrator.

3. Click **Common Directory Services**.

2 Configuring Directory Services

About Common Directory Services

A user directory is a collection of user records, each of which has a set of attributes, such as names, email addresses, and so forth. A directory service provides a mechanism for delivering information about the records in the directory.

Common Directory Services (CDS) provides a unified mechanism to connect to different user directories and manage users, groups, and roles, together with the access of users to webMethods resources.

Common Directory Services includes an internal directory service. However, if you are using an external directory (for example, Lightweight Directory Access Protocol (LDAP), you can configure Common Directory Services to also access user and group information from the external directory service.

About the Internal Directory Service

The internal directory service that is provided by default with your Common Directory Services installation is called the *system* directory service. Common Directory Services stores information about users, groups, and roles that you define in the system directory service to the Common Directory Services/Integration Server database. Use the system directory service if you need to maintain only a moderate number of users and groups.

For security reasons, you must change the default passwords of the system users. For information about how to change passwords for these users, see "Editing Information for a User" on page 27.

The following table lists the users defined by default in the system directory service:

First Name	Description
My webMethods Administrator	The default administrator account for Common Directory Services. This user can perform user management functions and manage external directory services. As installed, the user ID is "administrator" and the password is "manage".
Sys Admin	The system administrator account for Common Directory Services. This user can configure Common Directory Services and manage users, groups, roles, and permissions. As installed, the user ID is "sysadmin" and the password is "manage".
Deleted Items	A user account that is used internally by Common Directory Services to store work done by a user with administrative privileges when that user is deleted from the system. As installed, the user account is "deleteditems" and the password is "manage".
Designer	The user that connects to Common Directory Services/Integration Server from Software AG Designer. This user has privileges similar to those of the system administrator. As installed, the user ID is "designer" and the password is "manage".

First Name	Description
Guest	An anonymous user. This user can read pages that allow anonymous access, such as the login page. Otherwise, this user cannot read, modify, or delete content unless permission is explicitly granted by an administrator. As installed, the user ID for this user is “guest”.
webMethods System	A user account that is used internally by Common Directory Services to invoke web services. Common Directory Services uses this account for web service authentication from one server to another. As installed, the user account is “webm_sysuser” and the password is “manage”. **Important:** Do not delete this user account. Changes to the password for this account must be provided to administrators for custom applications that use it when communicating with Common Directory Services/Integration Server.
webMethods Cluster	A user account that is used internally by Common Directory Services for authentication among servers in a cluster. As installed, the user account is “webm_clusteruser” and the password is “manage”. **Important:** Do not delete this user account. Change the password for this user on one node of the cluster and then restart all nodes for the password to take effect.

No set up is required for the internal system directory service beyond configuring the Common Directory Services database. Configuring the database was required during the installation of Common Directory Services, as described in *Installing Software AG Products*.

About External Directory Services

In addition to the system directory service, Common Directory Services can support multiple external directory services, allowing you to manage a much larger and diverse group of users. If your company has one or more user directories, Common Directory Services can connect to those directories. In addition, you can use a database directory service, or create custom services to connect a directory provider to an external directory service.

Note:
During login, conditions in which the role cache or group cache calculation involves user or group searches that take a long time can result in poor performance in Common Directory Services and in LDAP servers to which it is connected.

Managing External Directory Services

Allowing Externally Defined Users to Perform Actions

By configuring an external directory service, you provide Common Directory Services with the information it needs to connect to and retrieve information from the external directory service. After configuring the external directory service, users defined in the external directory service will be able to log into Integration Server *but will not have permission to do anything else*. You need to take the following additional steps to allow users to perform actions:

- Create one or more LDAP query roles or database roles to identify the users who should be granted access to Integration Server. For more information about how to create roles for external directory services, see “Creating Roles” on page 42.
- Provide the roles the appropriate permissions.

Configuring an External LDAP, ADSI, or ADAM Directory Service

Use the following procedure to create an external directory service and connect Common Directory Services to an external LDAP, ADSI, or ADAM user directory.

To configure an external LDAP, ADSI, or ADAM directory service

1. In **Common Directory Services**, click **Directory Services**.

2. Click ⊕ and select the directory service type from the following options.

   - **LDAP** - Lightweight Directory Access Protocol.
   - **ADSI** - Active Directory Service Interfaces.
   - **ADAM** - Active Directory Application Mode.
   - **Database**
   - **External**

3. Click **Next**.

4. Fill in the form to configure the new directory service.

   For more information about the available configuration properties, see “LDAP, ADSI, and ADAM Directory Service Properties” on page 15.

5. Click **Save**.

6. (Optional) Test your configuration by searching for users or groups that are defined in the external directory service.

   For information, see "Searching for Existing Users, Groups, or Roles" on page 52.

LDAP, ADSI, and ADAM Directory Service Properties

When configuring an external directory service of type LDAP, ADAM, or ADSI, you can configure the following properties.

In the **General Information** section:

The following table lists the directory service properties you configure in the **General Information** section:

Property	Description
Directory Service Name	Required. The name to identify the external directory service. Common Directory Services uses this name to display the external directory service in the user interface.
Description	A descriptive comment about the external directory service.
Keywords	One or more keywords to use when searching for external directory services.

In the **Cache** section:

The following table lists the directory service properties you configure in the **Cache** section:

Property	Description
Cache Capacity	Required. The number of database queries to cache. The default is `1000`. Common Directory Services deletes the cache entries when the number of cached queries reaches the specified capacity, starting from the oldest entries.
Cache Timeout	The period of time for which queries remain in the cache unless the cache capacity is exceeded. The default is `1 day`. Common Directory Services deletes cache entries when the cache timeout expires, even if the specified cache capacity is not reached.

Common Directory Services saves all cache in memory and clears all cache entries when restarted.

In the **General Information** section:

The following table lists the directory service properties you configure in the **Connection Information** section:

Property	Description
Service Enabled	Enables or disables the directory service. The default is `Yes. Service is Enabled.`
Connection Error Threshold	Required. The maximum number of connection errors to occur before disabling the service. The default is `10`.
Auto Reconnect	Attempt to reconnect to the directory server if the service is disabled after reaching the connection error threshold or if the connection to the server is lost due to a network outage or planned maintenance. Enabled by default.
Auto Reconnect Interval	The period of time (in seconds) to wait between subsequent attempts to reconnect. The default is `6`.

Provider URL	Required. The URL for the external directory server using the following syntax:
	`ldap://host_name:port_number`
	or
	`ldaps://domain_name:port_number`

Base DN	Required. The root distinguished name to use when querying the directory server. For example, `ou=Portal,o=webmethods.com`
User DN	The additional user distinguished name to use when searching and loading users.
Groups DN	The additional group distinguished name to use when searching and loading groups.
Security Principal	Required. The distinguished name required to log in to the external directory server.
Security Credentials	Required. The password required to log in to the external directory server.
Failover URLs	The URL to another LDAP server that Common Directory Services uses for failover if the primary LDAP server, specified in the **Provider URL**, fails. Separate multiple values with spaces.
Search Timeout	Required. The maximum amount of time (in seconds) that an LDAP search query can run before it expires. The default is `0` - the query does not expire.

Property	Description
Enable GroupQuickSearch	Required for Active Directory. Indicates whether to determine the group membership of an Active Directory user with one query instead of a recursive search. When you enable this option, the search uses one query, which improves the login performance. Users must belong either to an Active Directory security group, or a regular group. The default is `Disabled`.
Active Directory Domain URLs	Applies only to Active Directory. Specify multiple Active Directory sub-domain URLs, separated by spaces.
Default Wildcard Searches Enabled	Enables or disables the use of wildcard characters in directory searches. The default is `Yes. Enable default wildcard searches.` Disabling wildcard searches might improve performance for large servers. When using wildcards, servers do not use any internal indexes for search performance.
Enable Group Across Directory Service	Indicates whether to query for group membership across all external directory services. When you enable this option, the search queries for group membership across all directory services, which degrades the login performance. The default is `No. Disable Group Across Directory Service.` For more information, see " Group Membership Across Directory Services" on page 20.
Use Kerberos	Enables or disables the use of Kerberos for LDAP authentication. The default is `No. Do not use Kerberos.`

In the **Advanced Object Filters** section:

The following table lists the directory service properties you configure in the **Advanced Object Filters** section:

Property	Description
User Object Filter	The LDAP filter that Common Directory Services applies to all queries when searching for users. Use a technical LDAP query that limits the type of objects exposed in Common Directory Services.
Group Object Filter	The LDAP filter that Common Directory Services applies to all queries when searching for groups. Use a technical LDAP query that limits the type of objects exposed in Common Directory Services.

Property	Description
Use Nested Groups	Enables or disables searches in nested LDAP groups. The default value is `No. Do not use Nested groups`.
Use the Virtual List View Control	Enables or disables the use of the Virtual List View (VLV) control to retrieve a subset of objects for an LDAP query. The default value is `No. Do not use the VLV control`. Applies only when the automatic configuration of LDAP server controls is disabled.
Use Server Side Paging Control	Enables or disables the use of the Server-Side Paging control to page the results of an LDAP query. The default value is `No. Do not use the Paging control`. Applies only when the automatic configuration of LDAP server controls is disabled.
Use Server Side Sorting Control	Enables or disables the use of the Server-Side Sorting control to sort the results of an LDAP query in a particular order. The default value is `No. Do not use the Sorting control`. Applies only when the automatic configuration of LDAP server controls is disabled.
Automatically Configure Server Side Controls	Enables or disables the automatic configuration of LDAP server controls by Integration Server. The default value is `Yes. Autoconfigure the controls`.

In the **User Attributes** section:

The following table lists the directory service properties you configure in the **User Attributes** section:

Property	Descripion
User Object Class	Required. The User Object Class attribute for the external directory service.
First Name	Required. The First Name attribute for the external directory service.
Last Name	Required. The Last Name attribute for the external directory service.
Full Name	Required. The Full Name attribute for the external directory service.
E-mail Address	Required. The Email Address attribute for the external directory service.
User ID	Required. The User ID attribute for the external directory service.

Property	Descripion
User Disabled	The name of an attribute in the external directory service that identifies a user as disabled.
User Disabled Value Regex	The regular expression to use when evaluating the User Disabled attribute for the external directory service.
UUID	The name of the attribute to use as a universally unique identification attribute of a user. Specify a string of maximum 128 characters, for example `cn` or `email`.

In the **Group Attributes** section:

The following table lists the directory service properties you configure in the **Group Attributes** section:

Property	Description
Group Object Class	Required. The Group Object Class attribute for the external directory service. The default is `groupofuniquenames`.
Group ID	Required. The Group ID attribute for the external directory service. The default is `cn`.
Group Name	Required. The Group Name attribute for the external directory service. The default is `cn`.
Group Members	Required. The Group Members attribute for the external directory service. The default is `uniquemember`.
Group E-mail	Required. The Group Email attribute for the external directory service. The default is `mail`.

In the **Connection Pool** section:

The following table lists the directory service properties you configure in the **Connection Pool** section:

Property	Description
Minimum Connections	The minimum number of connections to the external directory server to keep open at all times. The default is `1`.
Maximum Connections	The maximum number of connections to the external directory server to keep open at all times. The default is `20`.
Maximum Connection Time	The maximum amount of time to keep a connection to the external directory server open, before recycling the

Property	Description
	connection. The server resets this value for each LDAP search to ensure that an LDAP connection remains open during the search process. The default is `10minutes`.
Clean Up Interval	The time interval for cleaning up expired LDAP connections. The default is `1minute`.

Note:
In some LDAP implementations, the paging cookie is bound to a specific LDAP connection. Make sure that the value for the **Maximum Connections** property is large enough to handle concurrent LDAP searches and the value fo the **Maximum Connection Time** property is long enough to ensure that searches can finish within the specified time range.

Group Membership Across Directory Services

If you have multiple LDAP, ADSI, or ADAM directory services configured on Common Directory Services, the server can query for group membership across all of the configured directory services. This feature is useful if Users need to be in a branch of the Directory Tree that is distant enough from Groups that it is inefficient to have only one directory service mounted at a root that encompasses both users and groups. Instead, you might configure two directory services. One service points at the root of the User branch while the other points at the root of the Group branch. For example, you might have a directory structure similar to this:

o=MyCompany, ou=Americas, ou=US, ou=Groups
o=MyCompany, ou=Americas, ou=US, ou=Users
o=MyCompany, ou=Americas, ou=Mexico, ou=Groups
o=MyCompany, ou=Americas, ou=Mexico, ou=Users
and so forth....

Common Directory Services would not perform well with a single directory service pointing to o=MyCompany. Instead the administrator might create multiple directory services pointing to ou=Americas and other regional OUs. But suppose that Groups can have members from multiple regions, as might be common in large international organizations. In that case, it is possible for the membership of a Group to span multiple directory services.

To make it possible to query for group membership across all configured directory services, set **Enable Group Across Directory Service** for each directory service to **Yes. Enable Group Across Directory Service**.

Note:
Enabling this feature can noticeably degrade login performance.

Configuring a Database Directory Service

Use the following procedure to configure a database directory service. To use a database directory service, you must first connect to the database as an external data source.

To configure a database directory service

1. In **Common Directory Services**, click **Directory Services**.
2. Click ⊕ and select **Database**.
3. Click **Next**.
4. On the **Create Database Directory Service** page, enter the information for the database directory service.

   In the **General Information** section:

The following table lists the database directory service properties you configure in the **General Information** section:

Property	Description
Name	Required. A name to identify the external database directory service. Common Directory Services uses this name when it needs to identify the external database directory service in the user interface.
Description	A descriptive comment about the external database directory service.
Keywords	One or more keywords to use when searching for external directory services.

   In the **Cache** section:

The following table lists the database directory service properties you configure in the **Cache** section:

Property	Description
Cache Enabled	Determines whether Common Directory Services will attempt to save the load on the database by using cached data whenever possible. The default is `Yes. Enable the cache.`
Cache Capacity	Required. The number of database queries you want to cache. The default is `1000`.
Cache Timeout	The length of time that queries should remain in the cache unless the cache capacity is exceeded. The default is `1 day`.

In the **Attributes** section:

The following table lists the database directory service properties you configure in the **Attributes** section:

User ID	Required. The name of the query field containing the user ID value.
User First Name	Required. The name of the query field containing the user first name.
User Last Name	Required. The name of the query field containing the user last name.
User Full Name	Required. The name of the query field containing the user full name.
User E-mail	Required. The name of the query field containing the user email address.
User Disabled	The name of an attribute in the external directory service that identifies a user as being disabled.
User Disabled Value Regex	A regular expression used to evaluate the **User Disabled** attribute for the external directory service.
Group ID	Required. The name of the query field containing the group ID value.
Group DN	Required. The name of the query field containing the distinguished name value for the user.
Group Name	Required. The name of the query field containing the group name.
Group E-mail	The name of the query field containing the group email address.

In the **Database** section:

The following table lists the database directory service properties you configure in the **Database** section:

Datasource	The database to be used as a data store.

Query Lookup User By ID	Required. An SQL query that returns a user record based on the user ID. This query must return all user attributes, as described under **Attributes** in this table.
Query Authenticate	Required. An SQL query that returns persisted user credentials for authentication.
Query Lookup User By DN	An SQL query that returns a user record based on the user distinguished name.
Query Search Users	An SQL query that returns a list of user records by search term.
Query Lookup Group By ID	An SQL query that returns a group record based on the group ID.
Query Lookup Group By DN	An SQL query that returns a group record based on the group distinguished name.
Query Search Groups	An SQL query that returns a list of group records by search term.
Query Group Membership For Group	An SQL query that returns a list of groups that the child group is a member of.
Query User Members	An SQL query that returns a list of users that are members of the parent group.
Query Group Membership For User	An SQL query that returns a list of groups that the user is a member of.
Query Group Members	An SQL query that returns a list of groups that are members of the parent group.

5. Click **Save**.

6. (Optional) Test your configuration by searching for users or groups that are defined in the external directory service.

   For more information, see “Searching for Existing Users, Groups, or Roles” on page 52.

Updating the Configuration for a Directory Service

After you initially configure an external directory service or database directory service, you might need to update the values you specified for one or more of the properties. Use the following procedure to update the values of properties associated with a directory service.

To update the configuration for a directory service

1. In **Common Directory Services**, click **Directory Services**.

2. Click the directory name of the directory service you want to edit, or click ⋮ and then **Delete**.

3. Modify the properties of the directory service as required and click **Save**.

Updating the Search Order for Directory Services

Some user actions can result in Common Directory Services querying multiple directory services. Use the following procedure to control the order in which Common Directory Services searches the available directory services.

Note:
Setting the search order does not affect the order in which Common Directory Services displays directory services in lists throughout the user interface.

To update the order in which Common Directory Services searches external directory services

1. In **Common Directory Services**, click **Directory Services**.

2. Click 12↓.

3. Click and drag ⬍ to move directory services up or down as required.

4. Click **Apply**.

Deleting a Directory Service Configuration

If you no longer want Common Directory Services to have access to users and groups defined in an external directory service, you can delete the configuration information for that external directory service using the following procedure.

To delete the configuration for an external directory service

1. In **Common Directory Services**, click **Directory Services**.

2. Click ⋮, and then click **Delete** for the directory service you want to delete.

3 Managing Users

Users

To authenticate users and provide access to Integration Server or its layered products and packages, the system must have access to a definition for the user. To define users, you can:

- **Add users to the internal system directory service.** You provide all information about the user, for example the user ID the user is to supply to log into the system and the user’s password.
- **Access users already defined in external directory services.** If your users are defined in one or more external directory services, you can configure Common Directory Services to connect to the external directory services. As a result, those users can access and use Integration Server. For more information, see “Managing External Directory Services” on page 14.

With Common Directory Services, you can use a combination of users that are defined in both the internal system directory service and external directory services to access Integration Server and its layered products and packages.

Adding Users

Before a user can access and use Integration Server, you must either add the user to the system directory service or configure Integration Server to use the external directory service where the user is defined. For more information about configuring an external directory service, see “Managing External Directory Services” on page 14. The following procedure describes how to add a user to the system directory service.

To add a user

1. In **Common Directory Services**, click **Users**.

2. Click ⊕ and enter the information for the user you want to add to the system directory service.

The following table lists the fields to configure when adding a new user to the system directory service

Field	Description
User ID	Required. The user ID to assign to the user you are adding. Common Directory Services uses the user ID when forming the distinguished name (DN) for the user. The user ID can be 1 through 225 characters and can contain only alphanumeric ASCII characters with no spaces. The user ID is not case sensitive. Common Directory Services adds the user ID to the system directory service using the case you specify. Common Directory Services typically regards user IDs as case-insensitive, but uses the case you specify for actions that are case-sensitive such as HTTP authentication.

Field	Description
Password	Required. The password for the new user.
Confirm Password	Required. The same password you specified in the **Password** field.
First Name	Required. The first name of the user you are adding. Common Directory Services uses the user's first and last name when displaying the user's name on pages in the user interface.
Last Name	The last name of the user you are adding.
E-mail	The email address for the user you are adding. Common Directory Services uses the email address when it needs to send a notification to the user by means of an email message.

3. Click **Save**.

Editing Information for a User

You can edit the information for a user defined in the system directory service. If a user is defined in an external directory service, you can edit only Common Directory Services-specific information. You must update the external directory to change settings that Common Directory Services obtains from the external directory. For a list of the fields that Common Directory Services maintains for a user, and a description of all user information fields, including whether a field is read-only, see "User Information" on page 27.

To edit a user

1. In **Common Directory Services**, click **Users**.

2. In the **Users** list, click the user ID of the user you want to edit, or click ⋮ and **Edit**.

3. Modify the user information as required and click **Save**.

User Information

Administrative users can edit the information for user accounts defined in the system directory service, and view the information for user accounts, defined in an external directory. User information for externally defined users is read-only.

The following tables list the information that Common Directory Services maintains for a user.

Note:
The **Default** setting for all locale attributes is null value.

User Information

The **User Information** section includes all attributes that you specify when adding a user to the system directory service. You cannot edit the **User Information** attributes for users in an external directory service. This section is part of the user's profile, and administrative users can update some of the fields, for example the password and email address. The following table lists the attributes that the **User Information** section includes:

Field	Description
User ID	Required when adding a new user. The ID that a user supplies to log in to Integration Server. You cannot update this field.
Current Password	Required when adding a new user. The password that a user must supply to log on to Integration Server. Not displayed in the user interface. To change the password for a user, update the **New Password** and **Confirm Password** fields.
New Password	The new password that a user provides to log on to Integration Server.
Confirm Password	Required when adding a new user. The same as the **Password** field.
First Name	Required when adding a new user. The first name of the user, without the following special characters: >, ', ", and &.
Last Name	The last name of the user, without the following special characters: <, >, ', ", and &.
E-mail	The email address that Integration Server uses to send notifications to the user, without the following special characters: <, >, ', ", and &.
Distinguished Name (DN)	The distinguished name for the user. Common Directory Services generates this value using the user information you provide. You cannot update this field.
Login Disabled	Applies only to users in the system directory. Indicates whether the user is allowed to log in to Integration Server.

User Attributes

The **User Profile** tab includes attributes that Common Directory Services maintains regardless of the directory service to which the user belongs. The following table lists the attributes that the **User Profile** tab includes:

Field	Description
First Name	The first name of the user from the **User Information** section. You cannot edit this field on the **User Profile** tab. To change the

Field	Description
	first name, edit the value for **First Name** in the **User Information** section.
Last Name	The last name of the user from the **User Information** section. You cannot edit this field on the **User Profile** tab. To change the last name, edit the value for **First Name** in the **User Information** section.
Middle Name	The middle name of the user.
Title	The title of the user, for example, Mr., Mrs., or Ms. If the title you want to use is not available in the list, select **Other**.
Name Suffix	The suffix that appears after the name of the user, if applicable, for example, Jr., Sr., PhD, III. If the suffix you want to use is not available in the list, select **Other**.
Preferred Language/Locale	The language and locale for the user.
Address 1Address 2	The street address for the user.
Custom Address	Additional information included when more than a postal code is required for the address of the user, for example, special instructions.
City	The city where the user is located.
State/Province	The state or province where the user is located.
Postal Code	The postal code for the user, for example, a ZIP Code if the user is located in the United States.
Country/Region ID	The country where the user is located.
Phone 1 Area Code	The area code for the user.
Phone 1 Number	The phone number for the user.
Phone 1 Extension	The extension at which the user can be reached, if applicable.
Phone 1 Country Code	The country code associated with the phone number of the user.
Default Date Format	The date format to use when displaying dates.
Default Time Format	The time format to use when displaying time.
Default Time Zone	The time zone to use when displaying time.
Default Number Format	The format that to use when displaying numbers.
Default Currency Format	The format to use when displaying currency.

Field	Description
Android Subscription	Displays the Android device subscribed to receive mobile notifications for the user profile, if applicable. You cannot update this field.
iOS Subscription	Displays the iOS device subscribed to receive mobile notifications for the user profile, if applicable. You cannot update this field.
Created Date	Displays the date when the user profile was created. You cannot update this field.
Last Modified Date	Displays the date when the user profile was last modified from the Edit User page. You cannot update this field.

The **Roles** tab displays the roles to which a user is assigned and the attributes associated with each role. For more information about roles and role attributes, see "Creating Roles" on page 42.

Note:
If a user is assigned to dynamic roles, the list of roles might not always be completely accurate. Common Directory Services evaluates attributes and determines the roles to which a user belongs when a user logs in to Integration Server. If a change in user attributes occurs during a user session, and the user is no longer eligible to be a member of a role, Common Directory Services continues to consider the user a member of the role until the next login.

The following table lists the attributes, that the **Roles** tab includes:

Field	Description
Role Precedence	The roles to which a user is assigned, listed in order of precedence. Move roles up or down to reorder.
Role Members	The dynamic attributes associated with the selected role. Dynamic attributes provide more information about a role. For each attribute, the following information is available: ■ **Attribute** - the display name that you specify when adding the attribute to the role. ■ **Data Type** - the data type of the attribute. ■ **Role Value** - the default value for the attribute. All users are assigned this value unless a user-specific value takes precedence. ■ **User Value** - the user-specific value for the attribute. For example, for a "Customer Service" role, you can add a "Location" attribute to identify where the user assigned to the "Customer Service" role is located.

The **Calendar** tab displays information about the user calendars for business or personal use. For information about creating and managing user and business calendars, see "Managing Calendars" on page 56.

The following table lists the attributes that the **Calendar** tab includes:

Field	Description
Business Calendar	The calendar to use as a business calendar.
User Personal Calendar	The calendar to configure and use as a personal calendar.

The **LDAP Attributes** tab - If a user is defined in an external directory service, this tab lists a set of specific attributes from the external directory service. LDAP attributes must be set by a user with administrative privileges.

Database Attributes tab - If the user is defined in an external database directory service, this tab lists a set of specific attributes from the external database directory service. Database attributes must be set by a user with administrative privileges.

The **Groups** tab displays the groups to which the user belongs, and allows modification of the group membership for the user.

The following table lists the attributes that the **Groups** tab includes:

Field	Description
Type	Indicates that the user is a member of a group.
Display Name	The display name of the group.
Principal DN	The distinguished name of the group in which the user is a member.

Exporting User Data

You can export the profile data for a user in .json file format.

To export user data

1. In **Common Directory Services**, click **Users**.
2. In the **Users** list, click the user name for the user for which you want to export profile data.
3. On the **User Profile** tab of the **User Attributes** section, click **Export user data**.

Assigning a User to a Group

You can assign users defined in the system directory service to groups that are also defined in the system directory service. You cannot assign users that are defined in an external directory service to a group defined in the system directory, or assign users defined in the system directory service to an externally-defined group. You can assign both system and external users to a role.

For information about creating groups, see "Adding Groups" on page 36.

To assign a user in the system directory service to a group in the system directory service

1. In **Common Directory Services**, click **Users**.
2. Click the user ID of the user you want to add to a group.
3. In the **User Attributes** section, click the **Groups** tab and click 👤.
4. In the **Select Principlals** window, select a directory service from the **Directory Service** drop-down list, or use the search options to find specific groups.
5. Use the arrow buttons to move the groups you want the user to be a member of from the **Available** to the **Selected** box.
6. Click **Apply**.

Disabling Login for a User

You can deny a user defined in the internal system directory service the ability to log into Integration Server and its layered products. To disable login for users defined in an external directory service, see "Disabling User Accounts" on page 32. All products and packages that use Common Directory Services for authentication are affected by this feature.

To disable log-in for a user

1. In **Common Directory Services**, click **Users**.
2. Click the user ID of the user you want to disable login for.
3. Select the **Login Disabled** option and click **Save**.

Disabling User Accounts

You can prevent users from logging into Integration Server and its layered products, based on the value of a specified attribute in an external directory service. All products and packages that use Common Directory Services for authentication are affected by this feature.

To disable user accounts for an external directory service

1. In **Common Directory Services**, click **Directory Services**.
2. Click the name of the directory service, or click ⋮ and **Edit**.
3. Locate the properties needed to disable user accounts:
   - For an LDAP, ADSI, or ADAM directory service, go to the **User Attributes** section.
   - For a database directory service, go to the **Attributes** section.
4. In the **User Disabled** field, type the name of the attribute in the external directory service that will determine the User Disabled status.

   The exact value depends on the external directory service and the class of users you want to disable.
5. In the **User Disabled Value Regex** field, type a regular expression to match against the value of the **User Disabled** property. When the value matches, the user is disabled
6. Click **Save**.

Deleting Users

You can remove users that you have previously defined in the internal system directory service. To remove externally defined users, you must delete them from the corresponding user directory.

To delete users from the internal system directory service

1. In **Common Directory Services**, click **Users**.
2. Select all users you want to delete.
3. Click ⋮, and then click **Delete Selected**.
4. Click **Delete**.

Generating a Shared Secret

In Common Directory Services you can generate shared secrets for one-time authentication. Common Directory Services sends the shared secret to the email address specified for the user.

To generate a shared secret

1. In **Common Directory Services**, click **Users**.

2. In the **Users** list, click the user ID of the user for whom you want to generate a secret, or click ⋮ and **Edit**.

3. Expand the **User Attributes** section and click **Generate Shared Secret**.

4. Click **Ok**.

4 Managing Groups

Groups

You can logically organize collections of users into groups, which allows you to identify a group of users by a group name rather than identifying each user individually. For example, if you want to assign a group of users to a role, you can simply assign the group containing the users to the role, rather than identifying each user individually.

To define a group, you can do the following:

- **Add groups to the internal system directory service**. You provide information about the group and define its membership. You can assign both individual users or other groups to be a members. The users and groups that you assign to a group that is defined in the internal system directory service must also be defined in the internal system directory service. That is, you cannot assign users or groups that are defined in an external directory service to an internally-defined group.
- **Access groups already defined in external directory services.** If you want to use groups that are defined in one or more external directory services, you can configure Common Directory Services to use the external directory services. For more information, see "Managing External Directory Services" on page 14.

With Common Directory Services, you can use a combination of groups that are defined in both the internal system directory service and external directory services.

Adding Groups

You can define groups of users in the internal system directory service and add members to those groups.

To create a group

1. On the **Common Directory Services** page, click **Groups**.

2. Click ⊕ and enter the following information for the group you want to add to the internal system directory service:

The following table lists the required and optional fields to configure when adding a new group to the system directory service:

Field	Description
Group ID	An ID for the group. Common Directory Services uses this ID in the distinguished name (DN) for the group. The group ID can be 1 through 255 characters and can contain only alphanumeric ASCII characters with no spaces. The group ID is not case sensitive.

Field	Description
Group Name	The name that you want to assign to the group you are adding. The group name can be 1 through 255 characters.
Group E-mail	(Optional) The email address for the group you are adding.

3. Click **Save**.

Editing Group Information

You can edit the information for a group defined in the internal system directory service. If a group is defined in an external directory service, you must update the external directory service directory to change settings that Common Directory Services obtains from the external directory. For a list of the fields that Common Directory Services maintains for a group, and a description of all group information fields, including whether a field is read-only, see "Group Information" on page 37.

To edit a group

1. On the **Common Directory Services** page, click **Groups**.

2. Click the name of the group you want to edit, or click ✏.

3. Modify the group information as required and click **Save**.

Group Information

The following table lists the information that Common Directory Services (CDS) maintains for a group. The Section column of the table lists the section on the **Edit Group** page where the field is located.

<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td><b>Group Information</b></td><td>Attributes that you specify when you add a group.
<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td><b>Group ID</b></td><td>The group ID assigned to a group. The group ID is defined when the group is added and cannot be changed.</td></tr>
<tr><td><b>E-mail</b></td><td>The email address for the group.</td></tr>
<tr><td><b>Distinguished Name (DN)</b></td><td>The distinguished name for the group. You cannot update this field. Common Directory Services forms this field using information defined for the group.</td></tr>
</table>
</td></tr>
</table>

Section	Description
Group Attributes	Group attributes you configure after the creation of a group. This panel is comprised of two tabs: - **Groups** - shows which groups this group is a member of. For more information about how to make a group a member of another group, see “Making a Group a Member of Another Group” on page 39. - **Group Members** - lists the members of the group. For more information about how to add members to a group, see “Managing Members of a Group” on page 38.

Managing Members of a Group

Members of a group can be users or other groups. You can add members to a group defined in the internal system directory service if they are defined in the system directory service.

To work with users and groups defined in external directory services, use the mechanisms provided by the external directory services.

To manage members of a group defined in the internal system service directory

1. On the **Common Directory Services** page, click **Groups**.

2. Click on the name of the group you want to modify, or click ✎.

3. Click on the **Group Members** tab, and then click 👤.

4. In the **Select Principlals** window, select a directory service from the **Directory Service** drop-down list, or use the search options to find specific users or groups.

5. Use the arrow buttons to manage the members of the group:

   - To add users (in the system directory service) to the group, select the **Users** option, and move the users from the **Available** to the **Selected** box. For more information about adding users to a group, see “ Assigning a User to a Group” on page 32.

   - To add groups (in the system directory service) to the group, select the **Groups** option, and move them to the **Selected** box. For more information about making a group a member of another group, see “Making a Group a Member of Another Group” on page 39.

   - To remove users or groups of users from the group, move them from the **Selected** to the **Available** box.

6. Click **Apply**.

Making a Group a Member of Another Group

You can make a group a member of another group as long as both groups are defined in the internal system directory service. When one group becomes a member of a second group, all members of the first group also become members of the second group.

> **Note:**
> You cannot assign groups that are defined in an external directory service to a group defined in the system directory, or assign groups defined in the system directory to an externally-defined group. You can assign both internal and external groups to a role.

To make a group a member of another group

1. On the **Common Directory Services** page, click **Groups**.
2. Click the name of the group you want to edit, or click ✎.
3. On the **Groups** tab, click 👤.
4. In the **Select Principlals** window, select a directory service from the **Directory Service** drop-down list, or use the search options to find specific groups.
5. Use the arrow button to manage the membership of the group in other groups:
   - To make the current group a member of other groups from the system directory service, move the parent groups from the **Available** to the **Selected** box.
   - To remove the current group as a member of other groups, move the parent groups from the **Selected** to the **Available** box.
6. Click **Apply**.

Deleting Groups

You can remove groups that you have previously defined in the internal system directory service.

> **Note:**
> When you delete a group, the definition for the group is removed, but the individual members of the deleted group (users and/or other groups) are not deleted.

To delete groups from the internal system directory service

1. On the **Common Directory Services** page, click **Groups**.
2. Select all groups you want to delete.

3. Click ⋮, and then click **Delete Selected**.

4. Click **Delete**.

5 Managing Roles

Roles

A *role* is a collection of users, groups, or other roles. A set of default roles is installed with Common Directory Services. You can add users, groups, and other roles to this initial set.

The following table lists the default roles, available in Common Directory Services and the resources these roles can access:

Default role	Description
Admin Role	Provides access to all resources. By default, the Sys Admin and Designer users are members of this role.
My webMethods Administrators	Provides access to user management and other functions needed by the Administrator user, who is a default member of this role.
My webMethods Users	Provides access to the My webMethods user interface for all users of My webMethods applications. By default, the Administrator is a member of this role, but you must add all other users to it.

The members assigned to a role can span across multiple directory services. That is, their membership can include users, groups, and roles defined in the internal directory service, as well as, users and groups defined in external directory services. The membership of a role can be static, like groups where each member is specifically assigned. However, you can also make the membership of a role dynamic. It is valid for roles to be recursive, making it possible for roles to be members of each other.

The following table lists the different ways you can define the membership of a role, whether the membership is static or dynamic, and where to find more information about how to define membership for each type of role:

Defining Membership	Static or Dynamic	Additional Information
Specify the users, groups, and other roles you want to be members of the role	Static	"Adding a Static Role" on page 43
Specify an LDAP query that queries an external directory service to determine the users or groups assigned to the role	Dynamic	"Adding an LDAP Query Role" on page 44
Specify a database query that queries a database directory service to determine the users or groups assigned to the role	Dynamic	"Adding a Database Role" on page 48

Creating Roles

Administrators can create different types of user roles. Common Directory Services uses all roles, regardless of type, in the same manner, but role membership is identified differently for each type.

The following table describes the types of roles you can create and how to identify role membership for each role type:

Role	Identifying Membership
Static Role	Specify a collection of users, groups, and roles that are members of the role you are creating. The membership of the role does not change unless you manually edit the role and change its membership. For more information, see "Adding a Static Role" on page 43. **Note:** This is similar to a group except that role membership can span multiple directory services.
LDAP Query Role	Specify an LDAP query. The users, groups, and roles that match the query become members of the role. The membership of the role is dynamic based on the outcome of the query at run time. For more information, see "Adding an LDAP Query Role" on page 44.
Database Role	Specify a query for a database directory service. The users, groups, and roles that match the query become members of the role. The membership of the role is dynamic based on the outcome of the query at run time. For more information, see "Adding a Database Role" on page 48.

Adding a Static Role

A static role is a simple collection of users, groups, and other roles.

To create a static role

1. On the **Common Directory Services** page, click **Roles.**
2. Click ⊕.
3. In the **Role Name** field, type the name that you want to assign to the new role.

   Valid role names can contain only letters, numbers, underscores, or space characters.
4. From the **Role Provider** drop-down list, select **Static Role Provider**.
5. Click **Apply**.

Editing Members of a Static Role

Use the following procedure to edit the members of a static role.

To edit members of a static role

1. On the **Common Directory Services** page, click **Roles**.

2. Click the name of the role you want to edit, or click ⋮ and then click **Edit**.

3. In the **Role Attributes** section, click the **Members** tab and then click ✎.

4. In the **Select Principals** window select a directory service from the **Directory Service** drop-down list, or use the search options to find specific users, groups, or roles.

5. Use the arrow buttons to manage the membership of the role:

   - To add a user, role, or group to the role, move them from the **Available** to the **Selected** box.

   - To remove a user, role, or group from the role, move them from the **Selected** to the **Available** box.

6. Click **Apply**.

Adding an LDAP Query Role

An LDAP query role is based on an LDAP query to an external directory service. Any user or group that meets the requirements of the query is a member of the role.

To create an LDAP query role

1. On the **Common Directory Services** page, click **Roles.**

2. Click ⊕.

3. In the **Role Name** field, type the name that you want to assign to the new role.

   Valid role names can contain only letters, numbers, underscores, or space characters.

4. From the **Role Provider** drop-down list, select **LDAP Query Role Provider**.

5. Click **Apply**.

6. On the **Roles** page, click the name of the newly created role, or click ⋮ and then click **Edit**.

7. In the **Role Membership** section:

   a. In the **LDAP Query** field type a valid LDAP query.

b. Select the **Simple Query** option if the query in the **LDAP Query** field contains simplified LDAP query syntax.

> **Note:**
> Unless you are creating a complex LDAP query, the query syntax can be cumbersome to use. With the **Simple Query** option, the syntax is filled in for you. For example, to find all persons whose manager has the user ID `abrown`, the simple query syntax is `manager=abrown`.

c. Select a directory service from the **Directory Service** drop-down list.

d. In the **Principal Type** list, choose whether the query searches for **Users** or **Groups**.

8. Click **Save**.

Adding a Rule-Based Role

A rule-based role is based on a server rule. Any user, group, or role that matches the rule is a member of the role.

To create a rule-based role

1. On the **Common Directory Services** page, click **Roles**.

2. Click ⊕.

3. In the **Role Name** field, type the name you want to assign to the new role.

   Valid role names can contain only letters, numbers, underscores, or space characters.

4. From the **Role Provider** drop-down list, select the **Rule Based Role Provider**.

5. Click **Apply**.

6. On the **Roles** page, click the name of the newly created role, or click ⋮ and then click **Edit**.

7. Under the **Match Criteria** heading, select one of the following as the criteria for the rule-based role.

   - **Match All Criteria Below** - each regular expression must match some part of the corresponding attribute value for the current user.

   - **Match Any Criteria Below** - any regular expression in the list can match some part of the corresponding attribute value for the current user.

8. Fill in the appropriate match criteria for the rule-based role using the following guidelines:

Match Criteria	Description
User DN Value(s):	A regular expression that matches any part of the current user's directory distinguished name (DN). In the field, type the portions of the DN to which you want a match. For example, `ou=Engineering.*ou=US` matches a user with the following DN: `uid=joe,ou=Development,ou=Engineering,ou=Midwest,ou=US,o=webMethods`
Domain Name Expression:	A regular expression that matches any part of the name of the current user's directory service as registered in Common Directory Services. In the field, type the directory service name to which you want a match. For example, `US` (without quotes) matches a user from the US Corporate directory service. This is a very effective way to govern the look and feel for users that may be in different user directories, such as partners.
Group DN and Role DN Expression:	A regular expression that matches any part of any group or role of which the current user is a member. In the field, type the portions of the DN to which you want a match. For example, `ou=Engineering` matches a user belonging to a group with the following DN: `cn=portal,ou=Engineering,ou=Midwest,ou=US,o=webMethods.`
Parent Resource	A resource that matches the current resource or a parent of the current resource.
Resource Type	A resource type that matches the current resource type.
User Attributes	One or more pairs of user attributes and their values from the user’s record. To create an attribute-value pair, click ⊕ and enter a **Key** and a **Value**. If you have more than one user attribute, the value set in **Match Criteria** determines how attributes are matched: ■ **Match All Criteria Below** - each regular expression must match some part of the corresponding attribute value for the current user. ■ **Match Any Criteria Below** - any regular expression in the list can match some part of the corresponding attribute value for the current user. For example, if the rule is configured to match all criteria, and the configured user attribute pairs are listed with their name and value in the following table:

<table>
<tr><th>Match Criteria</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Name</th><th>Value</th></tr>
<tr><td><code>office</code></td><td>Bellevue</td></tr>
<tr><td><code>telephonenumber</code></td><td>(425) 564-0000</td></tr>
</table>
<p>and the current user's attribute values are listed with their name and value in the following table:</p>
<table>
<tr><th>Name</th><th>Value (current user)</th></tr>
<tr><td><code>office</code></td><td>Bellevue</td></tr>
<tr><td><code>telephonenumber</code></td><td>(206) 123-4567</td></tr>
</table>
<p>the rule does not match the current user because it matches the <code>office</code> attribute value but not the <code>telephonenumber</code> attribute value. If, however, the rule is configured to match any criteria, the preceding example rule does match the current user.</p>
</td></tr>
<tr><td><b>Request Headers</b></td><td>
<p>One or more pairs of HTTP header attributes and values. You can match anything that appears within an HTTP header, such as the browser agent string or the kinds of MIME types the user will accept. The rule can be a regular expression, or a simple text string.</p>
<p>To create an attribute-value pair, click ⊕ and enter a <b>Key</b> and a <b>Value</b>.</p>
<p>If you have more than one attribute-value pairs, the value set in <b>Match Criteria</b> determines how attributes are matched:</p>
<ul>
<li><b>Match All Criteria Below</b> - Each regular expression must match some part of the corresponding attribute value for the request header.</li>
<li><b>Match Any Criteria Below</b> - Any regular expression in the list must match some part of the corresponding attribute value for the request header.</li>
</ul>
<p>For example, if the rule is configured to match all criteria, and the configured request header pairs are listed in the following table:</p>
<table>
<tr><th>Name</th><th>Value</th></tr>
<tr><td><code>Accept-Charset</code></td><td>utf-8</td></tr>
<tr><td><code>Accept-Language</code></td><td>ja</td></tr>
</table>
<p>and the request header values for the current user are listed in the following table:</p>
</td></tr>
</table>

<table>
<tr><th>Match Criteria</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Name</th><th>Value (current user)</th></tr>
<tr><td><code>Accept-Charset</code></td><td>ISO-8859-1,utf-8;q=0.7</td></tr>
<tr><td><code>Accept-Language</code></td><td>en-us,en;q=0.5</td></tr>
</table>
the rule does not match the current user because it matches the Accept-Charset header value but not the Accept-Language header value. If, however, the rule was configured to match any criteria, the rule does match the current user.
</td></tr>
<tr><td><b>Parent Property</b></td><td>One or more pairs of resource properties and values. If you know the internal name of a property associated with a resource, you can match it.
To create an property-value pair, click ⊕ and enter a <b>Key</b> and a <b>Value</b>.
If you have more than one property-value pair, the value set in <b>Match Criteria</b> determines how properties are matched:
■ <b>Match All Criteria Below</b> - Each regular expression must match some part of the corresponding attribute value for the request header.
■ <b>Match Any Criteria Below</b> - Any regular expression in the list must match some part of the corresponding attribute value for the request header.
For example, if you want to match files that are PDFs, the property-attribute pair is <code>mimeType=pdf</code>.</td></tr>
</table>

9. Click **Apply**.

Adding a Database Role

A database role is based on a query to a database directory service. Any user, group, or role that matches the rule is a member of the role.

Note:
To create a database role, you must first connect to the database as an external data source.

To create a database role

1. On the **Common Directory Services** page, click **Roles**.

2. Click ⊕.

3. In the **Role Name** field, type the name that you want to assign to the new role.

   Valid role names can contain only letters, numbers, underscores, or space characters.

4. From the **Role Provider** drop-down list, select **Database Role Provider**.

5. Click **Apply**.

6. On the **Roles** page, click the name of the newly created role, or click ⋮ and then click **Edit**.

7. From the **Datasource** drop-down list, select the database to be used as a data source.

8. If the role can include users, in the **Query User** field, type an SQL query that returns a record for a given user in the database who should be a member of the role.

   The parameters to the query are:

   - {uid}—Principal unique ID
   - {dn}—Principal distinguished name

   An example of a valid query is:

   ```
   select * from user-roles where roleID=‘Admin’ and userid=‘{uid}’
   ```

9. If the role can include groups, in the **Query Group** field, type a SQL query that returns a record for a given group in the database that should be a member of the role.

10. Click **Save**.

Deleting Roles

If you no longer need a role, you can delete it.

Note:
When you delete a role, the members of the role (users, groups, and/or other roles) are not deleted.

To delete a role

1. On the **Common Directory Services** page, click **Roles**.

2. Optional. Search for the roles you want to delete. For more information, see “Searching for Existing Users, Groups, or Roles” on page 52.

3. Select the check boxes beside the roles you want to delete, click ⋮, and then click **Delete Selected**.

6 Searching for Users, Groups, and Roles

Searching for Existing Users, Groups, or Roles

When using basic searches, you can search for the following:

- Users and groups defined in the internal system directory service
- Users and groups defined in external directory services
- Roles

To search for users, groups, or roles

1. On the **Common Directory Services** page, click **Users**, **Groups**, or **Roles**.
2. Click **Basic**.
3. In the **Basic Keyword Search** field, specify the search criteria, as follows:
   - To search for users, enter the first name, last name, e-mail address, or user ID.
   - To search for groups, enter the group name, group ID, or group e-mail address.
   - To search for roles, enter the role name or the role ID.

   The search is *not* case sensitive. If you do not specify a keyword, Common Directory Services returns information for all entries in the selected directory service.
4. For users and groups, from the **Directory Service** list select the directory service where the users or groups are defined.

   If you select **Any Directory**, Common Directory Services searches all available directory services.
5. Click **Apply**.

Common Directory Services displays the search results in a table. For information about how to export search results, see "Exporting Search Results to a .xslx File" on page 53.

Performing Advanced Searches

You can perform an advanced search for users or groups, based on user or group information and extended attributes. You cannot perform an advanced search for roles.

To perform an advanced search for users or groups

1. On the **Common Directory Services** page, click **Groups** or **Users**.
2. Cick **Advanced**.

3. In the **Core Attributes** section, fill in the attribute values you want to search for and select the directory service where the users or groups are defined from the **Directory Service** list.

   If you select **Any Directory**, Common Directory Services searches all available directory services.

4. Click **Apply**.

Common Directory Services displays the search results in a table. For information about how to export search results, see “Exporting Search Results to a .xslx File” on page 53.

Exporting Search Results to a .xslx File

You can export search results to a .xslx file and then import the .xslx file into Microsoft Excel, or any other application that accepts the .xslx file format.

To export search results

1. In Common Directory Services, pefrom a search as explained in “Searching for Existing Users, Groups, or Roles” on page 52.

2. Click ⋮ and then click **Export as *.xslx**

3. Use the file-download mechanism in your browser to browse to the location where you want to save the .xslx file.

7 Configuring Calendars

Managing Calendars

Common Directory Services supports the use of business calendars and user calendars to assist with task definition, assignment, and behavior. Both business and user calendars are set up and configured in Common Directory Services. Each type of calendar is configured separately, and you can define business calendars only, user calendars only, or both.

Business Calendars

Software AG Designer and Integration Server support the use of business calendars and user calendars to assist with task definition and behavior. Both business and user calendars are set up and configured in Common Directory Services. Each type of calendar is configured separately, and you can define business calendars only, user calendars only, or both.

Business calendars define standard business days and hours for your business organization, including holidays, weekends, or any other times when your organization is not conducting business. For example, you might define your business calendar for normal business hours of Monday through Friday, 8:00 A.M. to 5:00 P.M. Eastern Standard time. You can define multiple business calendars.

These business calendars are defined in Common Directory Services and can be specified when you define a task date/time event type, for example. This ensures that when counting days, only business days will be considered and that non-business days such as weekends and holidays are not included.

A business calendar can also be associated with a process. In this case, the business calendar is used only to determine process time outs and joins and does not apply to any tasks in the process.

Creating Business Calendars

You can create multiple business calendars, enabling you to accommodate operations that may span different locations. For example, you may have an office in one location that works 8 A.M. to 4:30 P.M Monday through Friday, and another office that works 8 A.M. to 6:30 P.M Tuesday through Friday

Note:
Calendars are not limited to the current year, but continue automatically into following years. However, holidays are not carried forward from year to year, and must be manually defined for each calendar year.

To create a business calendar

1. In Common Directory Services, navigate to **Calendars** > **Business Calendars**.

2. Click ⊕.

3. On the Create Business Calendar page, specify the details for the calendar you want to add.

The following table lists the fields to configure when creating a business calendar and the field descriptions.

Property	Description
Name	A unique name for the calendar.
LookUp Name	An internal unique name (or alias) used to identify the calendar. **Note:** Changing the **LookUp Name** of a calendar will break anny associations made to the calendar. In this case, the task or process will revert to calculating time intervals using every day of the week (including weekends and holidays).
Time Zone	The time zone for the calendar. Default is system time zone.

4. In **Workdays**, click ⊕ to add the workdays of the week.

5. In the **Create Workday** dialog, select the day of the week, specify the hours of the day, and click **Save**.

6. In **Holidays**, click ⊕ to add any holidays you want to include in the calendar.

7. In the **Create Holiday** dialog, specify the **Start Date**, **Name**, and the **Duration in day(s)** of the holiday you want to add.

8. Click **Save**.

Deleting a Business Calendar

You the following procedure to delete a business calendar in Common Directory Services

To delete a business calendar

1. In Common Directory Services, navigate to **Calendars** > **Business Calendars**.

2. Click ⋮, and then click **Delete** for the business calendar want to delete.

User Calendars

Personal user calendars are maintained in a third-party application such as Microsoft Outlook or Lotus Notes, where the user maintains daily calendar events that define the user's availability. webMethods applications can check the user's personal calendar to determine if the user is available on this working day, taking into consideration only Out of the Office and Busy types of calendar events that are *scheduled for the entire day*.

You can configure Common Directory Services to provide access to user calendars, enabling you to view individual user calendars. You can also view the user's calendar on the **Calendar** tab of the **Edit User** page.

Configuring Microsoft Exchange User Calendars

To configure user calendars for Microsoft Exchange

1. In Common Directory Services, navigate to **Calendars** > **User Calendars**.
2. From the **External User Calendar** drop-down menu select **Microsoft Exchange**.
3. Specify values for the Exchange connection properties as described in the following table.

The following table lists the fields to configure when configuring a user calendar for Microsoft Exchange and the field descriptions.

Property	Description
Exchange hostname or IP	The URL for the Exchange e-mail server, for example, `main.mail.server.com`. To use a secure connection to the server, you must specify a server URL starting with https://. Otherwise, the http protocol is used by default.
Email User Attribute	The attribute from User attribute page that is used to pass the e-mail account name to the server to identify the correct user calendar on the Exchange server. Default value is `email` which passes the e-mail address entered on the Edit User page. In most cases, this is the information required by the server. If this value does not work, consult with your mail server administrator to determine the required value. In this case, you must define a new dynamic attribute at the role level and configure it to pass the required information.

Property	Description
Calendar Data Caching	How often the user calendar information is retrieved from the mail server. The information is cached in Integration Server until the next refresh time. Select **No Cache** to retrieve the calendar information from the mail server with each request.
Time Window	The calendar time period that is retrieved from the mail server, beginning with today's date.
Time Slot	The time divisions displayed in the user calendar. Events that are of a shorter duration than the selected value are "rounded up" to the selected value.
Exchange User	The user name for connecting to the Exchange server.
Exchange User Password	Password for the Exchange user.

4. Click **Save**.

Configuring IBM Lotus Notes User Calendars

To configure user calendars for IBM Lotus Notes

1. In Common Directory Services, navigate to **Calendars** > **User Calendars**.

2. From the **External User Calendar** drop-down menu select **IBM Lotus Notes**.

3. Specify values for the connection properties as described in the following table.

The following table lists the fields to configure when configuring a user calendar for IBM Lotus Notes and the field descriptions.

Property	Description
Calendar hostname or IP	The URL for the Lotus Domino e-mail server containing the calendar, for example, `main.mail.server.com`.
Calendar Server Port	The port number for the Lotus Domino e-mail server containing the calendar.
Email User Attribute	The attribute from User attribute page that is used to pass the e-mail account name to the

Property	Description
	server to identify the correct user calendar on the Lotus Domino server. Default value is `email` which passes the e-mail address entered on the Edit User page. In most cases, this is the information required by the server. If this value does not work, consult with your mail server administrator to determine the required value. In this case, you must define a new dynamic attribute at the role level and configure it to pass the required information
Calendar Data Caching	How often the user calendar information is retrieved from the mail server. The information is cached in Integration Server until the next refresh time. Select **No Cache** to retrieve the calendar information from the mail server with each request.
Time Window	The calendar time period that is retrieved from the mail server, beginning with today's date.
Time Slot	The time divisions displayed in the user calendar. Events that are of a shorter duration than the selected value are "rounded up" to the selected value.
Notes Admin User Id	Administrator user name for connecting to the Lotus Domino server.
Notes Admin Password	The password for the administrator user.

4. Click **Save**.

8 Configuring E-mail

Managing Email Settings

Configure an SMTP server to ensure that Common Directory Services sends emails successfully. You can use the existing Integration Server email server configuration, or configure an email server which specifically sends out Common Directory Services notifications.

To configure an email server to send Common Directory Services notifications

1. On the **Common Directory Services** page, click **Settings > E-Mail Configuration**.

2. Specify values for the properties as described in the following table.

Property	Description
SMTP Protocol	Identifies the email protocol to be used. The default and only valid value is `smtp`.
SMTP Host	Identifies the SMTP server. Specify the server's host name. For example: `smtp.server.com`. If you specify two or more hosts, type one address per line.
SMTP Port	Identifies the port number. Specify the SMTP server's port number. For example, `25`.
SMTP Username	Optional. Identifies the user name that Common Directory Services is to supply for authentication. If the SMTP server requires authentication, specify the user name to supply to satisfy the authentication challenge.
SMTP Password	Optional. Identifies the password associated with the **SMTP Username**. If the SMTP server requires authentication, specify the appropriate password.
SMTP Timeout	Defines the maximum period of time to wait for a response from the server, specified in milliseconds. Default value is 60000.
SMTP Connection Timeout	Defines the maximum period of time for a given SMTP session, specified in milliseconds. Default value is 60000.
From Name	Defines the default "From" name. Specify the default name to use in the "From" field of the email messages that Common Directory Services sends using the SMTP server. **Note:** Text in this field is subject to the requirements of the RFC822 Internet Text Message standard. For example, text in parentheses, as in "(Important)", is treated as a comment and is removed when the message is created, and bracketed text, such as "[Status]", is treated as an optional element and is also removed.

Property	Description
From E-Mail Address	Defines the default "From" email address. Specify the default email address to use in the "From" field of the email messages that Common Directory Services sends using the SMTP server.
Admin E-mail Address	Defines the email address of the Common Directory Services administrator. This is used as the 'from' address for administrative email messages sent on behalf of the server.

3. Optionally, click **Test** and specify a recipient email to confirm your configuration works as intended.

4. Click **Save**.

9 Managing Certificates

Managing Authentication Certificates

Administrators can manage authentication certificates for users who connect to Integration Server or other webMethods applications. Authentication certificates do not govern a connection between a user and Integration Server. To be assigned a certificate, the user must be a member of the system directory service or an external directory service connected to Common Directory Services. For more information about working with directory services, see "About Common Directory Services" on page 12.

The assignment of users to authenticate follows these rules:

- A user can be assigned to multiple certificates.
- An instance of a certificate can have only one user assigned to it, but you can add multiple instances of a certificate, each with a different certificate type, and assign a different user to each instance.

Adding an Authentication Certificate

You can use certificates that authenticate the users who connect to Integration Server. Use the following procedure to add a certificate.

To add an authentication certificate

1. On the **Common Directory Services** page, click **Certificates**.
2. Click ⊕.
3. Click **Browse**, navigate to the location of the certificate file you want to add, and click **Open**.
4. From the **Type** drop-down list, choose the type of authentication certificate to be used by a client connecting to Integration Server or other layered products.

The following table lists the available certificate types and their purpose:

Certificate Type	Purpose
SSL (default)	Authenticates the message sender. The credentials are supplied in the protocol header.
Verify	Verifies the digital signature on incoming messages to Integration Server.
Encrypt	Encrypts outgoing messages from Integration Server.
Verify and Encrypt	Both verifies the digital signature on incoming messages and encrypts outgoing messages. Used if a user has the same certificate for sending and receiving messages.

Certificate Type	Purpose
Message Authentication	Authenticates the message sender. The message header contains the credentials of the sender.

5. Click **Upload**.

Searching for Authentication Certificates

You can search for authentication certificates based on a number of criteria.

To search for authentication certificates

1. On the **Common Directory Services** page, click **Certificates**.
2. Click **Advanced**.
3. In each section, specify the criteria to apply when searching for certificates for each sect.

   In the **Certificate Info** section:

The following tables lists the available search criteria in the Certificate Info section and their descriptions

Field	Description
Type	Choose the certificate type assigned to the certificate. For more information about valid types, see “ Adding an Authentication Certificate” on page 66. The default is **Any**.
Issuer Common Name	Type the common name of the certificate issuer. This field is not used if you leave it blank.
Serial Number	Type the serial number assigned to the certificate. This field is not used if you leave it blank.
Subject Common Name	Type the common name of the subject. This field is not used if you leave it blank.

In the **Valid Not Before** section:

The following tables lists the available search criteria in the Valid Not Before section and their descriptions

Field	Description
Range	Choose a range of dates from the selection provided. The default is **All**.

Field	Description
Start Date	Type a start date using the format DD/MM/YYYY.
End Date	Type an end date using the format DD/MM/YYYY.

In the **Valid Not After** section:

The following tables lists the available search criteria in the Valid Not After section and their descriptions

Field	Description
Range	Choose a range of dates from the selection provided. The default is **All**.
Start Date	Type a start date using the format DD/MM/YYYY.
End Date	Type an end date using the format DD/MM/YYYY.

4. Click **Apply**.

Viewing Details of an Authentication Certificate

You can view the details associated with an authentication certificate.

To view the details of an authentication certificate

1. On the **Common Directory Services** page, click **Certificates**.

2. Click on the Subject DN for the certificate, or click ⋮ and then click **Edit**.

   The following table lists the details, available for each authentication certificate:

Certificate Detail	Description
Certificate User	The name of the user assigned to the certificate.
Certificate Type	The certificate type assigned when the certificate was added.
Version	The version of the certificate.
Serial Number	The serial number assigned to the certificate.
Issuer Common Name	The common name of the issuer.
Issuer DN	The distinguished name of the certificate issuer.

Certificate Detail	Description
Subject Common Name	The common name of the host being authenticated.
Subject DN	The distinguished name of the being authenticated.
Valid Not Before	The date before which the certificate is not valid.
Valid Not After	The date after which the certificate is not valid.
Alg Name	The name of the algorithm used in the certificate.

3. Click **Cancel** to return to the list of certificates.

Assigning a User to an Authentication Certificate

You can assign only one user to an instance of an authentication certificate. To assign the same certificate to multiple users, add a separate instance of the certificate for each user. For more information on how to add a certificate, see“ Adding an Authentication Certificate” on page 66.

To assign a user to an authentication certificate

1. On the **Common Directory Services** page, click **Certificates**.
2. Click the Subject DN for the certificate, or click ⋮ and then click **Edit**.
3. In the **User Mapping** section, click **Set**.
4. In the **Select Principlals** window, select a directory service from the **Directory Service** drop-down list, or use the search options to find a specific user.
5. Use the arrow buttons to move the user from the **Available** to the **Selected** box.
6. Click **Apply**.

Changing Users for an Authentication Certificate

You can exchange one user for another in an existing authentication certificate.

To change users for an authentication certificate

1. On the **Common Directory Services** page, click **Certificates**.
2. Click on the Subject DN for the certificate, or click ⋮ and then click **Edit**.

3. In the **User Mapping** section, click **Set**.

4. In the **Select Principlals** window, select a directory service from the **Directory Service** drop-down list, or use the search options to find a specific user.

5. Use the arrow buttons to exchange the users so that the original certificate user is in the **Available** box, and the user to assign the certificate to is in the **Selected** box.

6. Click **Apply**.

Removing a User from an Authentication Certificate

You can remove a user who is assigned to an existing authentication certificate.

To remove a user from an authentication certificate

1. On the **Common Directory Services** page, click **Certificates**.

2. Click the Subject DN for the certificate, or click ⋮ and then click **Edit**.

3. In the **User Mapping** section, click **Remove**.

4. Click **Cancel**.

Deleting Authentication Certificates

You can remove authentication certificates that you have previously defined in the system directory service.

To delete authentication certificates

1. On the **Common Directory Services** page, click **Certificates**.

2. Select all certificate instances you want to delete.

3. Click ⋮, and then click **Delete Selected**.

4. Click **Delete**.

10 Managing GDPR Options

Managing User Data

Data protection laws and regulations, such as the GDPR (General Data Protection Regulation) might require specific handling of user data, even after a user profile is removed.

To ensure user data integrity, Common Directory Services stores timestamps for the initial registration of a of a user profile in Common Directory Services, and the latest modification that occurred before the current login session. Both timestamps are available for users and administrators to view as part of the user information for the profile. Users can review profile timestamps to ensure that they are aware of all profile modifications.

When an administrator deletes a profile using the user interface, or when users delete their own profiles, Common Directory Services clears all information about the user from the database and cache. However, since deleting a user account does not remove user identifying data that appear in log files, administrators can use the timestamps as a reference when cleaning up Common Directory Services log data.

Additionally, administrators can configure Common Directory Services to send e-mail notifications to users when their profile was modified, either by the users or by an administrator, and determine the level of detail that notification e-mails include.

For more information about GDPR and data protection configurations, see:

- "Configuring GDPR Settings" on page 72
- "User Information" on page 27
- "Exporting User Data" on page 31
- "Deleting Users" on page 33

Configuring GDPR Settings

You can enable and disable GDPR-compliant user data protection options from the **GDPR Configuration** page in the Integration Server administration interface. You configure notification settings and message texts separately for each notification type.

1. On the **Common Directory Services** page, click **Configurations > GDPR Configuration**.

2. From the **Service Enabled** drop-down list select **Yes. Service is Enabled** to enable GDPR options.

3. Optionally, configure e-mail notifications by performing the following steps:

    a. From the **Select Notification Type** drop-down list, select the user profile event for which you want to configure e-mail notifications.

    Available notification types are **Update notification** and **Delete notification**

    b. Select the **Notification Enabled** to enable e-mail notifications for the event.

c. In the **Notification Subject** field, enter a custom subject.

d. In the **Notification Content** field, specify the body of the message.

   Strings enclosed in double braces are variables that Integration Server uses to include the user names of Integration Server users in the message. The `{{user}}` variable denotes the user that receives the message, the `{{actor}}` variable - the user that makes modifications to the profile, and the `{{changes}}` variable - details about the profile modifications, if configured. You can move the variables through the text, as in the following example:

   Default message:

   ```
   Dear {{user}},
   Your personal data has been modified.
   {{changes}}
   The account was updated by user logged-in as {{actor}}.
   ```

   Modified message:

   ```
   Hello {{user}},
   You are receiving this message because
   {{actor}} has modified your profile data.
   Modifications:
   {{changes}}
   ```

4. Optionally, in **Content Detail**, choose what information to include about the modified profile attributes. Details replace the `{{changes}}` variable in the notification message. The options are:

   - **No details** - Default. Do not include detailed information about modified attributes.
   - **Include changed attribute names** - Include only the names of modified attributes in the notification message.
   - **Include changed attribute with values** - Include the names and values of modified attributes in the notification message.

5. Click **Save**.

11 Configuring Permissions

Managing Permissions

Administrators manage permissions for accessing and working with Integration Server and other webMethods applications.

Administrators can manage permissions for users, groups, and roles in any required combination.

> **Note:**
> Do not modify permissions for the built-in roles from the Permissions Management page. Fixes you install to Integration Server subsequently might remove you changes.

Adding Permissions

The basic workflow in assigning permissions is to search for the resources on which to assign permissions.

To assign permissions

1. In **Common Directory Services**, click **Permissions Management**.
2. On the **Permissions Management** page, select **My webMethods Applications**, and click the right arrow.
3. Click **Next**.
4. On the **Manage Permissions** page, click ☰ for the principal whose permissions you want to edit.
5. Click the **Grant All** or **Deny All** option for the settings, and click **Save**.

   If neither option is selected, permissions for a setting will be determined from another source.

Editing the Access Control List

You can add or delete users, groups, and roles from the list of principals with managed priviledges.

To modify the access control list

1. In **Common Directory Services**, click **Permissions Management**.
2. On the **Permissions Management** page, select **My webMethods Applications**, and click the right arrow.
3. Click **Next**.

4. On the **Manage Permissions** page, click 👤.

5. In the **Select Principlals** window, select a directory service from the **Directory Service** drop-down list, or use the search options to find specific princpals.

6. Use the arrow buttons to modify the list of principals on the access control list:

   - To add a principal to the access control list, move the principal from the **Available** to the **Selected** box.

   - To remove a principal from the access control list, move the principal from the **Selected** to the **Available** box and click **Delete**.

7. Click **Apply**.

12 TOTP Configuration

Configuring Time-based One-time Password Settings

Time-based one-time password (TOTP) is an algorithm for generating passwords which uses current time to ensure the uniqueness of passwords. In the case of TOTP, the server and the client requesting authentication must be synchronized to generate one-time passwords. Use the following procedure to configure one-time passwords for multi-level authentication of users in Common Directory Services.

To configure TOTP settings

1. In **Common Directory Services**, click **Configurations > TOTP Configuration**.

2. Specify values for the properties as described in the following table.

Property	Description
Name	The name of the TOTP configuration.
Service Enabled	Whether the service is active. Select **Yes. Service is Enabled** from the drop-down menu to activate the service.
Time-step windows	The number of time-step windows to check during password validation.
One-time password role name	The name of the role for one-time password management.
One-time passwords service name	The name of the service for one-time password management

3. Click **Save**.

13 JMS Configuration

Configuring JMS Provider Settings

When the system load requires using several Common Directory Services nodes in a cluster, you must configure Common Directory Services to use a JMS provider for communication between the cluster nodes. Common Directory Services can use either the Integration Server database for JMS communication, or Universal Messaging as an external JMS provider.

To configure a JMS provider

1. On the **Common Directory Services** page, click **Configurations > JMS Configuration**.

2. Select one of the following from the **JMS Provider** drop-down menu:

   - **DB JMS**

   - **Universal Messaging** - this option requires that you also specify the URL to the Universal Messaging server for your installation in the **Universal Messaging URL**.

3. Click **Save**.