



Universal Controller 6.8.x

Security

© 2020 by Stonebranch, Inc. All Rights Reserved.

1. Security .....	3
1.1 Security Overview .....	4
1.2 Users and Groups .....	5
1.3 Roles and Permissions .....	17
1.4 Credentials .....	50
1.5 Business Services .....	59
1.6 Audits .....	64

# Security



## Setting Up Security



## Audit Records

[Overview](#)

[Adding Users](#)

[Adding Groups](#)

[Assigning Roles to Users or Groups](#)

[Assigning Permissions to Users or Groups](#)

[Login Credentials](#)

[Business Services](#)

[Viewing Audit Records](#)



The information on these pages also is located in the [Universal Controller 6.7.x Security.pdf](#).

# Security Overview

## Universal Controller Security

Setting up Universal Controller security involves the following steps:

- Creating [users](#) and assigning them passwords.
- Creating [groups](#) of users.
- Assigning [permissions](#) (access to Controller records) to users and groups.
- Assigning [roles](#) (permission to perform administrative functions) to users and groups.
- Creating [credentials](#) that allow the Controller to log in to remote machines and execute jobs.

See [LDAP Settings](#) for information on how to set up Universal Controller to use LDAP authentication for:

- [Credentials for running tasks](#)
- [User logins](#)

See [Single Sign-On Settings](#) for information on how to set up Universal Controller to use SAML authentication.

# Users and Groups

- [Overview](#)
- [Default Users and Groups](#)
- [Adding a User](#)
  - [User Details](#)
  - [User Details Field Descriptions](#)
- [Adding a Group](#)
  - [Group Details](#)
  - [Group Details Field Descriptions](#)
- [Additional Details](#)
- [Assigning Users to Groups](#)
- [Navigation Visibility for Users and Groups](#)
- [Deleting a User](#)

## Overview

You can create any number of users and user groups for Universal Controller, and you can assign any user to any user group.

The [roles and permissions](#) that you assign each user and group determines the level of access to Universal Controller functions.

You can assign any role and permission to any user or any user group. If you assign a user to a group, the user inherits all roles and permissions assigned to that group.

See [LDAP Settings](#) for information on how to set up Universal Controller to use LDAP authentication for:

- [Credentials for running tasks](#)
- [User logins](#)

## Default Users and Groups

### Default User

The default Universal Controller user is **ops.admin**. It is assigned to one of the default Universal Controller groups, [#Administrator Group](#).

### Default Groups

There are two default groups:

- **Administrator Group** has access to all Controller functions; by default, it is assigned the [ops.admin](#) role, which has permissions on all Controller functions.
- **Everything Group** has access to all functions that do not require the [ops.admin](#) role.

## Adding a User

Note



You must have administrative permissions to add users.

By default, a new user has no permissions. Until permissions are granted, a user can log into the Universal Controller user interface and view options in the [Navigator](#), but cannot perform any tasks.

**Step 1** From the [Administration](#) navigation pane, select **Security > Users**. The Users list displays a list of all currently defined users.

Below the list, User Details for a new user displays.

The screenshot shows the 'Users' list and the 'User Details' form. The 'Users' list displays a table with columns: User Id, Name, Locked Out, Active, Updated By, and Updated. The 'User Details' form is open, showing fields for User Id, Password, First Name, Middle Name, Last Name, Email, Time Zone, Title, Department, Manager, Business Phone, Mobile Phone, Web Browser Access, Command Line Access, Web Service Access, and Active. The 'Login Method' is set to 'Standard'.

User Id	Name	Locked Out	Active	Updated By	Updated
stonebranch-user-01	stonebranch 01	No	Yes	ops.admin	2018-07-20 16:40:00 -0400
stonebranch-user-0	stonebranch 02	No	Yes	ops.admin	2018-07-20 16:40:59 -0400
stonebranch-user-03	stonebranch 03	No	Yes	ops.admin	2018-07-20 16:41:22 -0400
stonebranch-user-04	stonebranch 04	No	Yes	ops.admin	2018-07-20 16:41:56 -0400
stonebranch-user-05	stonebranch 05	No	Yes	ops.admin	2018-07-20 16:42:19 -0400

The 'User Details' form includes the following fields:

- User Id: [Text Field]
- Password: [Text Field]
- First Name: [Text Field]
- Middle Name: [Text Field]
- Last Name: [Text Field]
- Email: [Text Field]
- Time Zone: [Dropdown Menu: Server (America/New\_York)]
- Title: [Text Field]
- Department: [Text Field]
- Manager: [Text Field]
- Business Phone: [Text Field]
- Mobile Phone: [Text Field]
- Web Browser Access: [Dropdown Menu: System Default]
- Command Line Access: [Dropdown Menu: System Default]
- Web Service Access: [Dropdown Menu: System Default]
- Active: [Checkbox]
- Login Method: [Dropdown Menu: Standard, Single Sign-On]
- Locked Out: [Checkbox]
- Password Requires Reset: [Checkbox]

**Step 2** Enter/select Details for a new user, using the [field descriptions](#) below as a guide.

- Required fields display in **boldface**.
- Default values for fields, if available, display automatically.

To display more of the Details fields on the screen, you can either:

- Use the scroll bar.
- Temporarily [hide the list](#) above the Details.
- Click the **New** button above the list to display a pop-up version of the Details.

**Step 3** Optionally, assign one or more roles to the user, assign the user to a group, or assign permissions to this user.

**Step 4** Click a **Save** button. The user is added to the database, and all buttons and tabs in the User Details are enabled.

Note



To **open** an existing record on the list, either:

- Click a record in the list to display its record Details below the list. (To clear record Details below the list, click the **New** button that displays above and below the Details.)
- Clicking the **Details** icon next to a record name in the list, or right-click a record in the list and then click **Open** in the **Action menu** that displays, to display a pop-up version of the record Details.
- Right-click a record in the a list, or open a record and right-click in the record Details, and then click **Open In Tab** in the **Action menu** that displays, to display the record Details under a new tab on the record list page (see [Record Details as Tabs](#)).

User Details

The following User Details is for an existing user. See the [field descriptions](#), below, for a description of all fields that display in the User Details.

User Details: IT

UpdateDeleteRefreshClose

UserUser RolesMember of GroupsPermissions

Details

User Id : stonebranch-user-01

Time Zone : Server (America/New\_York)

Password : .....

Title : IT Technician

First Name : stonebranch

Department :

Middle Name :

Manager :

Last Name :

Business Phone :

Email :

Mobile Phone :

Web Browser Access : -- System Default --

Command Line Access : -- System Default --

Web Service Access : -- System Default --

Active : ☒

Password Requires Reset : ☐

Locked Out : ☐

Login Method : StandardSingle Sign-On

UpdateDeleteRefreshClose

User Details Field Descriptions

The following table describes the fields, buttons, and tabs that display in the User Details.

Field Name	Description
Details	This section contains detailed information about the user.
User ID	Log in ID for this user.
Password	Password of this user. <div>Note<div>The hint for this field, as well as the information icon, will display any current characteristics and restrictions for Passwords as defined in <a href="#">Password Settings</a>.</div></div>

First Name	First name of this user.
Middle Name	Middle name of this user.
Last Name	Last name of this user.
Name	Automatically generated from the <a href="#">#First Name</a> and <a href="#">#Last Name</a> of this user.
Email	Email address of this user.
Password Requires Reset	If enabled, the user will be prompted to reset the password at next login.
Locked Out	If enabled, locks out the user. This field is enabled automatically if the maximum number of successive failed login attempts has been reached by the user.
Login Method	<p>Login method(s) that the user can authenticate with. (You can use the Ctrl key to select both methods.)</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Single Sign-On</li> </ul>
Time Zone	Time zone of this user. When this user logs in, all scheduling times will be shown in the user's time zone, unless the trigger specifies a different time zone.
Title	Business title of this user.
Department	Business department of this user.
Manager	Business manager of this user.
Business Phone	Business phone number of this user.
Mobile Phone	Mobile phone number of this user.
Web Browser Access	<p>Specifies whether or not the user can log in to the user interface.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• System Default - User restriction for logging in to the user interface is based on the current system default value of the <a href="#">System Default Web Browser Access</a> Universal Controller system property.</li> <li>• Yes - User is not restricted from logging in to the user interface.</li> <li>• No - User is restricted from logging in to the user interface.</li> </ul>
Command Line Access	<p>Specifies whether or not the user can log in to the Universal Controller <a href="#">Command Line Interface (CLI)</a>.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• System Default - User restriction for logging in to the CLI is based on the current system default value of the <a href="#">System Default Command Line Access</a> Universal Controller system property.</li> <li>• Yes - User is not restricted from logging in to the CLI.</li> <li>• No - User is restricted from logging in to the CLI.</li> </ul>



Web Service Access	Specifies whether or not the user can log in to the Universal Controller <a href="#">RESTful Web Services API</a> .  Options: <ul style="list-style-type: none"> <li>System Default - User restriction for logging in to the Universal Controller Web Services is based on the current system default value of the <a href="#">System Default Web Service Access</a> Universal Controller system property.</li> <li>Yes - User is not restricted from logging in to the Universal Controller Web Services.</li> <li>No - User is restricted from logging in to the Universal Controller Web Services.</li> </ul>
Active	If enabled, the user ID is active and the user can log in. If disabled, the user is deactivated; the user will not appear in user lists and cannot be used for access to the Controller.
<b>Metadata</b>	This section contains <a href="#">Metadata</a> information about this record.
UUID	Universally Unique Identifier of this record.
Updated By	Name of the user that last updated this record.
Updated	Date and time that this record was last updated.
Created By	Name of the user that created this record.
Created	Date and time that this record was created.
<b>Buttons</b>	This section identifies the buttons displayed above and below the User Details that let you perform various actions.
<b>Save</b>	Saves a new user record in the Controller database.
<b>Save &amp; New</b>	Saves a new record in the Controller database and redisplay empty Details so that you can create another new record.
<b>Save &amp; View</b>	Saves a new record in the Controller database and continues to display that record.
<b>New</b>	Displays empty (except for default values) Details for creating a new record.
<b>Update</b>	Saves updates to the record.
<b>Delete</b>	Deletes the current record.
<b>Refresh</b>	Refreshes any dynamic data displayed in the Details.
<b>Close</b>	For pop-up view only; closes the pop-up view of this user.
<b>Tabs</b>	This section identifies the tabs across the top of the User Details that provide access to additional information about the user.
<b>User Roles</b>	Allows you to assign <a href="#">roles</a> to this user.
<b>Member of Groups</b>	Allows you to assign this user to one or more <a href="#">groups</a> .
<b>Permissions</b>	Allows you to assign <a href="#">permissions</a> to this user.

## Adding a Group

Note



You must have administrative privileges to add groups.

A group is a collection of users. You can assign privileges and roles to groups or users. You can also assign groups to other groups.

Any user assigned to a group inherits all roles and permissions assigned to that group.

Step 1

From the [Administration](#) navigation pane, select **Security > Groups**. The Groups list displays a list of all currently defined groups.

Below the list, Group Details for a new group displays.

Dashboards Groups

5 Groups

Custom Filter -- Unsaved 1 -- Filter... Go To... New

Name	Description	Parent	Updated By	Updated	Navigation Visibility
stonebranch-group-1			ops.admin	2018-01-12 15:19:05 -0500	Activity, Task Instances, H
stonebranch-group-2			ops.admin	2018-01-12 16:00:14 -0500	Activity, Task Instances, H
stonebranch-group-3			ops.admin	2018-01-12 15:59:44 -0500	
stonebranch-group-4			ops.admin	2018-01-12 15:59:50 -0500	
stonebranch-group-5			ops.admin	2018-01-12 15:59:54 -0500	

Group Details Save Save & New New

Group Group Roles Group Members Child Groups Permissions

Details

Name

Description

Email

Control Navigation Visibility

Parent

Manager

Save Save & New New

Step 2

Enter/select Details for a new group, using the [field descriptions](#) below as a guide.

- Required fields display in **boldface**.
- Default values for fields, if available, display automatically.

To display more of the Details fields on the screen, you can either:

- Use the scroll bar.
- Temporarily [hide the list](#) above the Details.
- Click the **New** button above the list to display a pop-up version of the Details.

Step 3

Optionally, assign one or more roles to the group, assign members (users) to the group, assign other groups to this group, or assign permissions to this group.

Step 4

Click a **Save** button. The group is added to the database, and all buttons and tabs in the Group Details are enabled.

Note

To [open](#) an existing record on the list, either:

- Click a record in the list to display its record Details below the list. (To clear record Details below the list, click the **New** button that displays above and below the Details.)
- Clicking the [Details icon](#) next to a record name in the list, or right-click a record in the list and then click **Open** in the [Action menu](#) that displays, to display a pop-up version of the record Details.
- Right-click a record in the a list, or open a record and right-click in the record Details, and then click **Open In Tab** in the [Action menu](#) that displays, to display the record Details under a new tab on the record list page (see [Record Details as Tabs](#)).

Group Details

10 / uc-68x-sec

The following Group Details is for an existing group. See the [field descriptions](#), below, for a description of all fields that display in the Group Details.

Group Details: stonebranch-group-1

UpdateDeleteRefreshClose

Group

Group Roles

Group Members

Child Groups

Permissions

Details

Name : stonebranch-group-1

Parent :

Description :

Email :

Control Navigation Visibility : ☒

Manager :


Navigation Visibility : Activity, Task Instances, History, All Triggers, Active Triggers,...

UpdateDeleteRefreshClose

### Group Details Field Descriptions

The following table describes the fields, buttons, and tabs that display in the Group Details.

Field Name	Description
Details	This section contains detailed information about the group.
Name	Name of this group.
Parent	Name of this group's parent group, if any.
Description	Description of this group.
Email	Email address for this group.
Manager	Universal Controller user that is the manager of this group.
Control Navigation Visibility	Indication of whether or not to control the visibility of navigation pane entries in the Controller <a href="#">Navigator</a> , via the Navigation Visibility field, for members of this Group. If Control Navigation Visibility is not checked (the default selection), all entries are visible.

Navigation Visibility	<p>If Control Navigation Visibility is enabled; Drop-down list of all Navigator entries.</p> <p>You can manually select and deselect any entry on the list. You also can click <b>Check All</b> above the list to make all Navigator entries visible to users in this Group, or click <b>Uncheck All</b> above the list to hide all Navigator entries from users in this Group.</p> <p><b>Note</b></p> <p> If a new Navigation Visibility entry becomes available (for example, when a new Universal Task type has been created) <i>after</i> an administrator has configured the Navigation Visibility feature for a Group, you must explicitly add that new entry to the configuration.</p> <p>If a newly created Universal Task type does not appear as an entry in the Navigation Visibility drop-down list, confirm that the Universal Template has at least one field defined, perform the <a href="#">Refresh Navigation Tree</a> operation, and <a href="#">refresh</a> the Group Details (or <a href="#">refresh</a> the Groups list).</p> <p>When a Universal Template is deleted, any Navigation Visibility configuration with a reference to its corresponding Universal Task type entry will automatically have that entry removed.</p>
<b>Metadata</b>	This section contains <a href="#">Metadata</a> information about this record.
UUID	Universally Unique Identifier of this record.
Updated By	Name of the user that last updated this record.
Updated	Date and time that this record was last updated.
Created By	Name of the user that created this record.
Created	Date and time that this record was created.
<b>Buttons</b>	This section identifies the buttons displayed above and below the Group Details that let you perform various actions.
<b>Save</b>	Saves a new group record in the Controller database.
<b>Save &amp; New</b>	Saves a new record in the Controller database and redisplay empty Details so that you can create another new record.
<b>Save &amp; View</b>	Saves a new record in the Controller database and continues to display that record.
<b>New</b>	Displays empty (except for default values) Details for creating a new record.
<b>Update</b>	Saves updates to the record.
<b>Delete</b>	Deletes the current record.
<b>Refresh</b>	Refreshes any dynamic data displayed in the Details.
<b>Close</b>	For pop-up view only; closes the pop-up view of this group.
<b>Tabs</b>	This section identifies the tabs across the top of the Group Details that provide access to additional information about the user.
<b>Group Roles</b>	Allows you to assign <a href="#">roles</a> to this group.
<b>Group Members</b>	Allows you to assign <a href="#">users</a> to this group.
<b>Child Groups</b>	Allows you to assign other groups to this group.
<b>Permissions</b>	Allows you to assign <a href="#">permissions</a> to this group.

# Additional Details

For information on how to access additional details - such as [Metadata](#) and complete [database Details](#) - for Users and Groups (or any type of record), see [Records](#).

## Assigning Users to Groups

You can assign users to groups from a User record and from a Group record.

Step 1

Open the User or Group record.

Step 2

Click the **Group Members** tab.

For a User, a list of all groups to which the user is assigned displays:

User Details: stonebranch-user-01

User



User Roles

Member of Groups

Permissions

New

Edit

Group ^	Updated By	Updated
 stonebranch-group-01	stonebranch-user-01	2014-07-08 10:43:39 -0400
 stonebranch-group-02	stonebranch-user-02	2014-07-08 10:43:39 -0400

For a Group, a list of all users assigned to the group displays.

Group Details: stonebranch-group-01

Group

Group Roles


Group Members

Child Groups

Permissions

New

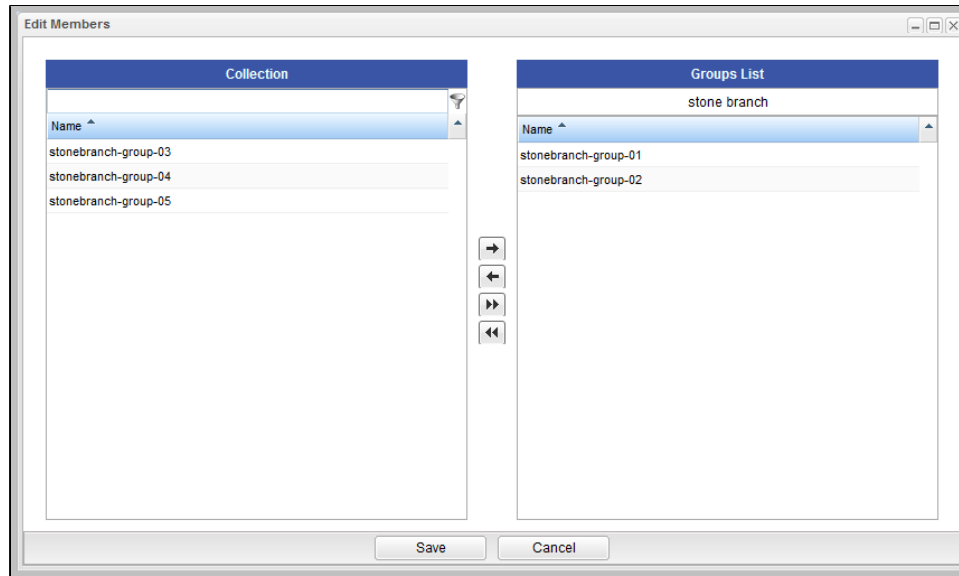
Edit

User ID ^	Name	Updated By	Updated
 stonebranch-user-01	stone a branch	ops.admin	2014-07-08 10:43:39 -0400

Step 3

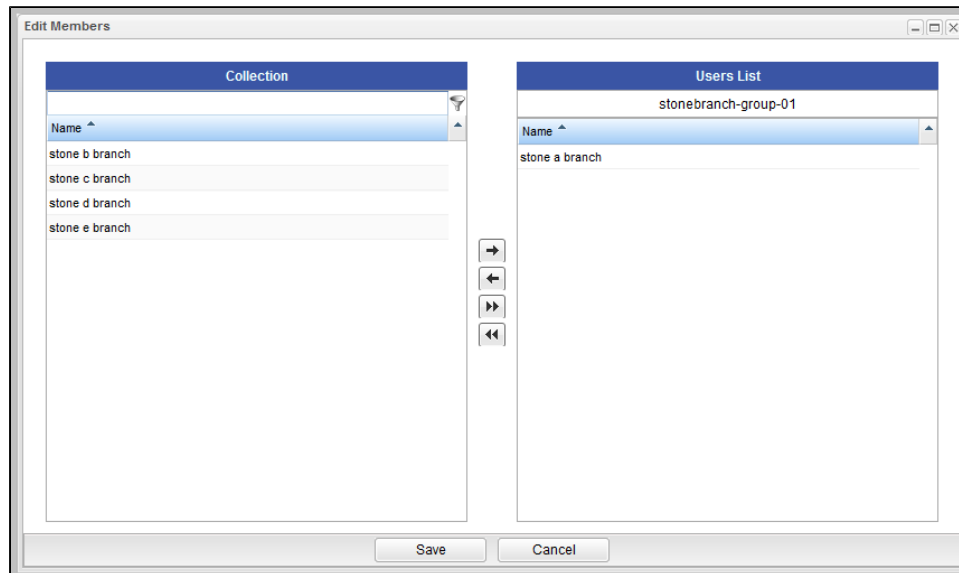
For a User, either:

- Click **New** to [create a Group](#) and automatically assign the User to it.
- Click **Edit** to display an **Edit Members** pop-up that allows you to assign the User to existing Groups.



For a Group, either:

- Click **New** to [create a User](#) and automatically assign it to the Group.
- Click **Edit** to display an **Edit Members** pop-up that allows you to assign existing Users to the Group.



<b>Step 4</b>	To filter the Users/Groups listed in the Collection window, enter characters in the text field above the <b>Name</b> column. Only Users/Groups containing that sequence of characters will display in the list.
<b>Step 5</b>	<p>To assign a User to a Group, move the User/Group from the <b>Collection</b> window to the <b>List</b> window:</p> <ol style="list-style-type: none"> <li>1. To move a single entry, double-click it or click it once and then click the <b>&gt;</b> arrow.</li> <li>2. To move multiple entries, Ctrl-click them and then click the <b>&gt;</b> arrow.</li> <li>3. To move all entries, click the <b>&gt;&gt;</b> arrow.</li> </ol> <p>To unassign the User to a Group, move the User/Group from the <b>List</b> window to the <b>Collection</b> window:</p> <ol style="list-style-type: none"> <li>1. To move a single entry, double-click it or click it once and then click the <b>&lt;</b> arrow.</li> <li>2. To move multiple entries, Ctrl-click them and then click the <b>&lt;</b> arrow.</li> <li>3. To move all entries, click the <b>&lt;&lt;</b> arrow.</li> </ol>
<b>Step 6</b>	Click <b>Save</b> .

## Navigation Visibility for Users and Groups

Users with the [ops.admin](#) role or the [ops\\_user\\_admin](#) role can control, via the [#Control Navigation Visibility](#) and [#Navigation Visibility](#) fields in the [#Group Details](#) for a Group, which entries in the Controller [Navigator](#) are visible to users in that Group.

The following conditions apply to navigation visibility

<b>User in Multiple Groups</b>	If a user belongs to multiple Groups, and for any of those Groups the <a href="#">#Control Navigation Visibility</a> is not enabled, Navigator visibility for that user is not controlled.
<b>User in Multiple Groups</b>	If a user belongs to multiple Groups, and for all of those Groups navigation visibility has been deselected for one or more entries, the visible entries from all Groups will be merged. That is, if an entry is not visible to users in Group A, but the entry is visible to users in Group B, the entry will be visible to any user belonging to both Groups.
<b>Navigation Pane</b>	If all entries in a folder of a navigation pane (for example, the Tasks folder in the Automation Center navigation pane) are not visible to a Group, that folder does not display for any user in that Group.
<b>Navigation Pane</b>	If all entries in a navigation pane are not visible to a Group, that navigation pane does not display for any user in that Group.
<b>Automation Center Navigation Pane</b>	If a Group does not have visibility to one or more entries in the configurable <a href="#">Automation Center</a> navigation pane, those entries are not available for configuration for any user in that Group.
<b>Trigger Types / Task Types</b>	If a Group does not have visibility to a specific Trigger type or Task type, that Trigger type or Task type does not display in the <b>New</b> drop-down menu on the All Triggers list or the All Tasks list for any user in that Group.
<b>Universal Task Types</b>	Dynamically created Universal Task type entries are available for selection / deselection in the <a href="#">#Navigation Visibility</a> field.
<b>User Roles</b>	The <a href="#">role</a> selections for any user override any navigation visibility selections for any Group in which that user is a member.
<b>User Roles</b>	Navigation visibility selections for a Group do not apply to any users in the Group with the <a href="#">ops_admin</a> role.

## Deleting a User

Attempts to delete a user will be prohibited under the following circumstances:

- User is currently assigned as the manager for user(s).
- User is currently assigned as the manager for group(s).
- User currently associated with enabled trigger(s).
- User currently assigned as the execution user for trigger(s).
- User currently assigned as the execution user for active task instance(s).
- User currently assigned as the visible to for bundle(s).

If deletion of a user is allowed, the following information associated with the user record also will be deleted:

- User roles.
- User permissions.
- Group memberships.
- User's filters.
- User's pinned filter preferences.
- User's layout preferences.
- User's navigation preferences.
- User's reports (reports made visible only to that user).
- User's user preferences.
- User's dashboards.



# Roles and Permissions

- [Overview](#)
- [Assigning Roles to Users or Groups](#)
  - [Description of Roles](#)
- [Assigning Permissions to Users or Groups](#)
  - [General Permissions Field Descriptions](#)
- [Types of Permissions](#)
  - [Agent Permissions](#)
  - [Agent Cluster Permissions](#)
  - [Application Permissions](#)
  - [Bundle Permissions](#)
  - [Calendar Permissions](#)
  - [Credential Permissions](#)
  - [Database Connection Permissions](#)
  - [Email Connection Permissions](#)
  - [Email Template Permissions](#)
  - [OMS Server Permissions](#)
  - [PeopleSoft Connection Permissions](#)
  - [Promotion Target Permissions](#)
  - [SAP Connection Permissions](#)
  - [Script Permissions](#)
  - [SNMP Manager Permissions](#)
  - [Task Permissions](#)
  - [Task Instance Permissions](#)
  - [Trigger Permissions](#)
  - [Variable Permissions](#)
  - [Virtual Resource Permissions](#)
- [Exporting Permissions for a Group](#)

## Overview

[Roles](#) control user and group access to administrative functions within Universal Controller. A user or group that has been assigned a role has permission to perform any function defined for that role.

[Permissions](#) control user and group access to specific functions for specific types of Controller records.

Some roles have permissions for specific functions that can be assigned individually. For example, a user that has been assigned the [ops\\_agent\\_cluster\\_admin](#) role has permission to perform all functions associated with Agent Clusters. A user that has not been assigned the [ops\\_agent\\_cluster\\_admin](#) role still can be given permission to perform individual functions associated with Agent Clusters via the [Agent Cluster Permissions](#).

Conversely, since there is no role associated with Agents, permissions for a user to perform functions associated with Agents must be assigned specific [Agent Permissions](#).

Note



The [#ops\\_admin](#) role assigns a user permission to perform all functions.

## Assigning Roles to Users or Groups

Roles control user access to functions that include:

- Setting up security.
- Creating reports, filters, and gauges.
- Creating Agent Clusters, SNMP Managers.
- Creating Email Connections, Database Connections, PeopleSoft Connections, and SAP Connections.
- Creating and promoting bundles of records.

Each role is a predefined collection of administrative functions (see [Description of Roles](#), below). By assigning a role to a user or group, you automatically give that user or group all functions associated with that role.

#### Note

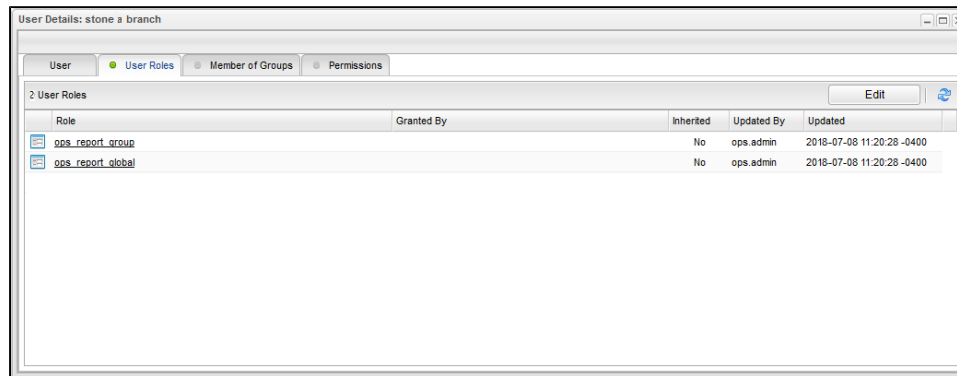


You cannot add new roles to the Controller; you must assign administrative functions to groups or users using the predefined roles.

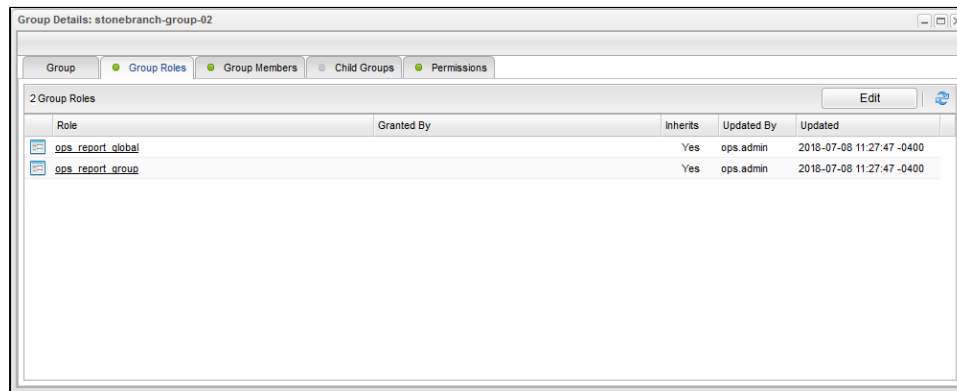
To assign roles to a user or group:

**Step 1** Open a [User](#) or [Group](#) record.

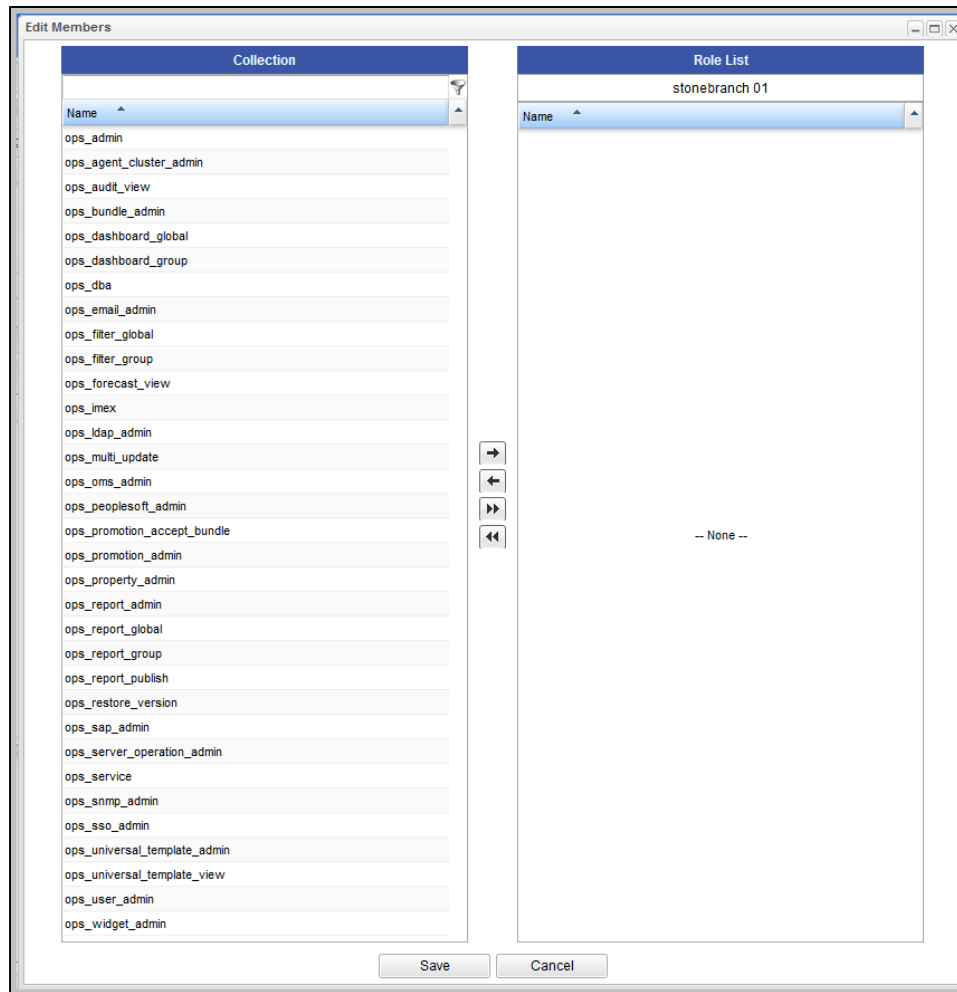
**Step 2** For a User, click the **User Roles** tab. A list of Roles assigned to the User displays.



For a Group, click the **Group Roles** tab. A list of Roles assigned to the Group displays.



**Step 3** Click **Edit**. An **Edit Members** pop-up displays that allows you to assign Roles to the User / Group. For example:



- The Collection window displays all Roles that have not been assigned to this User / Group.
- The Roles List window displays all Roles that have been assigned to this User / Group.


**Step 4** To filter the Users/Groups listed in the Collection window, enter characters in the text field above the **Name** column. Only Users/Groups containing that sequence of characters will display in the list.


Step 5	<p>To assign a Role to the User / Group, move the Role from the <b>Collection</b> window to the <b>Roles</b> window:</p> <ol style="list-style-type: none"><li>1. To move a single Role, double-click it or click it once and then click the &gt; arrow.</li><li>2. To move multiple Roles, Ctrl-click them and then click the &gt; arrow.</li><li>3. To move all Roles, click the &gt;&gt; arrow.</li></ol> <p>To unassign a Role to the User / Group, move the Role from the <b>Roles</b> window to the <b>Collection</b> window:</p> <ol style="list-style-type: none"><li>1. To move a single Role, double-click it or click it once and then click the &lt; arrow.</li><li>2. To move multiple Roles, Ctrl-click them and then click the &lt; arrow.</li><li>3. To move all Roles, click the &lt;&lt; arrow.</li></ol>
Step 6	Click <b>Save</b> .


## Description of Roles

The following table summarizes the roles available in the Controller.

Role Name	Available Functions	Contains Roles
-----------	---------------------	----------------

ops_admin	<p>All functions; this is the Universal Controller administrator role. The easiest way to assign full permissions to a user is to add the user to the Administrator Group, which by default is assigned the ops_admin role.</p> <p><b>Note</b> </p> <p>The ops_admin role contains all other roles. If a user is assigned the ops_admin role, no other roles need to be assigned to that user, and unassigning any other role from the user will not revoke that role.</p>	<ul style="list-style-type: none"> <li>ops_agent_cluster_admin</li> <li>ops_audit_view</li> <li>ops_bundle_admin</li> <li>ops_dba</li> <li>ops_email_admin</li> <li>ops_filter_global</li> <li>ops_filter_group</li> <li>ops_forecast_view</li> <li>ops_imex</li> <li>ops_ldap_admin</li> <li>ops_multi_update</li> <li>ops_oms_admin</li> <li>ops_peoplesoft_admin</li> <li>ops_promotion_admin</li> <li>ops_property_admin</li> <li>ops_report_admin</li> <li>ops_restore_version</li> <li>ops_sap_admin</li> <li>ops_server_operation_admin</li> <li>ops_service</li> <li>ops_snmp_admin</li> <li>ops_sso_admin</li> <li>ops_universal_template_admin</li> <li>ops_user_admin</li> </ul>
ops_agent_cluster_admin	<p>Create, read, update, and delete <a href="#">agent clusters</a>.</p> <p>(Also see <a href="#">Agent Cluster Permissions</a>, below.)</p>	
ops_audit_view	<p>Read <a href="#">Audits</a>.</p>	

ops_bundle_admin	<ul style="list-style-type: none"> <li>• Create, read, update, and delete <a href="#">Bundles</a>.</li> <li>• View <a href="#">Promotion Targets</a>, including <a href="#">agent mappings</a>.</li> <li>• View <a href="#">Promotion History</a>.</li> <li>• View a record's <a href="#">list of bundles</a>.</li> <li>• View <a href="#">Promotion Schedules</a>.</li> <li>• <a href="#">Add a record to a bundle</a>.</li> <li>• <a href="#">Create bundles by date</a>.</li> <li>• Generate a <a href="#">Bundle Report</a>.</li> </ul> <p>(Also see <a href="#">Bundle Permissions</a> and <a href="#">Promotion Target Permissions</a>, below.)</p>	
ops_dashboard_global	Create, update, and delete <a href="#">Dashboards</a> with Everyone visibility; updating includes updating Dashboard visibility.	
ops_dashboard_group	Create, update, and delete <a href="#">Dashboards</a> that are visible for a group in which this user is a member; updating includes updating Dashboard visibility.	
ops_dba	<p>Create, update, delete <a href="#">Database Connections</a>.</p> <p>(Also see <a href="#">Database Connection Permissions</a>, below.)</p>	
ops_email_admin	<p>Create, read, update, delete <a href="#">Email Connections</a>.</p> <p>(Also see <a href="#">Email Connection Permissions</a>, below.)</p>	
ops_filter_global	Create <a href="#">Filters</a> with Everyone visibility.	
ops_filter_group	Create <a href="#">Filters</a> that belong to a group of which this user is a member.	
ops_forecast_view	<p>Read <a href="#">Forecast Calendar</a>, <a href="#">Forecasts List</a>, and <a href="#">Forecast Details</a>.</p> <p>Note  Users also can read forecast information, without being assigned this role, if they have Read permission for the Task specified in the <a href="#">Forecast Details</a>.</p>	
ops_imex	<a href="#">List Import/Export XML</a> .	
ops_ldap_admin	Read and update <a href="#">LDAP Settings</a> .	
ops_multi_update	<a href="#">Update multiple records</a> .	
ops_oms_admin	Create, update, and delete <a href="#">OMS Servers</a> .	
ops_peoplesoft_admin	<p>Create, read, update, and delete <a href="#">PeopleSoft Connections</a>.</p> <p>(Also see <a href="#">PeopleSoft Connection Permissions</a>, below.)</p>	
ops_promotion_accept_bundle	Accept bundles being promoted to a target server. (The <b>Accept Bundle</b> command is executed on the target server automatically as part of the <b>Promote</b> and <b>Promote Bundle</b> commands and does not involve user interaction.)	

ops_promotion_admin	<ul style="list-style-type: none"> <li>Create, read, update, and delete <a href="#">Promotion Targets</a>, including agent mappings.</li> <li>View <a href="#">Bundles</a>.</li> <li><a href="#">Refresh Target Agents</a>.</li> <li><a href="#">Promote records</a>.</li> <li><a href="#">Promote</a> or <a href="#">schedule the promotion</a> of a bundle.</li> <li>Reschedule, cancel, and delete <a href="#">Promotion Schedules</a>.</li> <li><a href="#">Generate a Bundle report</a>.</li> <li>Accept bundles being promoted to a target server. (The <b>Accept Bundle</b> command is executed on the target server automatically as part of the <b>Promote</b> and <b>Promote Bundle</b> commands and does not involve user interaction.)</li> </ul> <p>Note </p> <p>By default, the ops_promotion_admin role also grants Read permission for any type of definition that can be added to a Bundle, given the expectation that a promotion administrator would review the content of a Bundle before promoting it. To change this default behaviour, see the <a href="#">Promotion Read Permission Required</a> Universal Controller property.</p> <p>(Also see <a href="#">Bundle Permissions</a> and <a href="#">Promotion Target Permissions</a>, below.)</p>	<ul style="list-style-type: none"> <li>ops_promotion_accept_bundle</li> </ul>
ops_property_admin	Read, update, and delete <a href="#">Universal Controller system properties</a> and <a href="#">Password Settings</a> .	
ops_report_admin	<ul style="list-style-type: none"> <li>Create, read, update, and delete any <a href="#">report</a>, regardless of <a href="#">visibility</a>, in addition to the roles granted by the <a href="#">ops_widget_admin</a> role.</li> <li>Create, update, and delete <a href="#">Dashboards</a> with Everyone visibility and <a href="#">Dashboards</a> that are visible for a group in which this user is a member; updating includes updating Dashboard visibility.</li> </ul> <p>The <a href="#">Strict Report Create Constraints</a> Universal Controller system property specifies whether or not to restrict report creation only to users with the ops_admin, ops_report_admin, ops_report_group, or ops_report_global role.</p> <p>The <a href="#">Strict Dashboard Create Constraints</a> Universal Controller system property specifies whether or not to restrict Dashboard creation only to users with the ops_admin, ops_report_admin, ops_dashboard_group, or ops_dashboard_global role.</p>	<ul style="list-style-type: none"> <li>ops_dashboard_global</li> <li>ops_dashboard_group</li> <li>ops_report_global</li> <li>ops_report_group</li> <li>ops_report_publish</li> <li>ops_widget_admin</li> </ul>
ops_report_global	Create global <a href="#">reports</a> .	
ops_report_group	Create <a href="#">reports</a> that belong to a group to which this user is a member.	
ops_report_publish	Publish <a href="#">reports</a> . (This role was applicable only to the Controller 5.x release.)	
ops_restore_version	<a href="#">Restore</a> old versions of records.	
ops_sap_admin	Create, read, update, and delete <a href="#">SAP Connections</a> .  (Also see <a href="#">SAP Connection Permissions</a> , below.)	
ops_server_operation_admin	Run <a href="#">Server Operations</a> .	

ops_service	<ul style="list-style-type: none"> <li>Log in and view <a href="#">Home Dashboard</a>. The Active Task Instances By Status <a href="#">widget</a> will remain blank unless the user is assigned the <a href="#">Task Instance Read</a> permission, as the ops_service role does not include access to such data.</li> <li>Read <a href="#">Agents</a>.</li> <li>Read <a href="#">Universal Controller system properties</a>.</li> <li>Read <a href="#">Password Settings</a>.</li> <li>Read <a href="#">LDAP Settings</a> (and run the Test Connection command).</li> <li>Read <a href="#">Single Sign-On Settings</a>.</li> <li>Read <a href="#">Universal Templates</a> and related data (Fields and Field Choices).</li> <li>Read <a href="#">Data Backup/Purge</a>. Unless the user also is assigned the <a href="#">ops_audit_view</a> role, the Audit tab on the <a href="#">Data Backup/Purge</a> Details, which allows for conveniently viewing related Audit records, will not be available.</li> <li>Read <a href="#">Users</a> and related data (Roles, Group Membership, and Permissions).</li> <li>Read <a href="#">Groups</a> and related data (Roles, Group Membership, Child Groups, and Permissions).</li> </ul>	
ops_snmp_admin	Create, read, update, and delete <a href="#">SNMP Managers</a> , to which the Controller sends <a href="#">SNMP notifications</a> .  (Also see <a href="#">SNMP Manager Permissions</a> , below.)	
ops_sso_admin	Read and update <a href="#">Single Sign-On Settings</a> .	
ops_universal_template_admin	Create, read, update, and delete <a href="#">Universal Templates</a> .	<ul style="list-style-type: none"> <li>ops_universal_template_view</li> </ul>
ops_universal_template_view	Read <a href="#">Universal Templates</a> .	
ops_user_admin	Create, read, update, and delete <a href="#">users and groups</a> .	
ops_widget_admin	Create, update, and delete <a href="#">Widgets</a> .	

## Assigning Permissions to Users or Groups

Permissions control user access to specific types of Controller records, such as task or trigger, and the types of functions that can be performed for those record types, such as create or delete.

You can further narrow down which records each permission applies to by specifying either name parameters or Business Services. For example, a given permission might apply only to tasks whose name begins with "SF," or a permission might apply only to tasks that have been assigned to a specific [Business Service](#) or to tasks that do not belong to any Business Services. See [General Permissions Field Descriptions](#), below, for more details.

To add permissions to a user or group:

<b>Step 1</b>	Open a <a href="#">User</a> or <a href="#">Group</a> record.
---------------	--



**Step 2** Click the **Permissions** tab. A list of permissions assigned to the User / Group displays.

For Example:

Type	Operations	Commands	Name	Unassigned to Business Service	Business Services	Updated By	Updated
Agent	Read, Update, Execute	*		Yes	stonebranchbusinessservice 01	ops.admin	2016-06-17 13:29:14 -0400
Task	Read, Update	ALL	*	Yes	stonebranchbusinessservice 03	ops.admin	2016-06-17 13:29:02 -0400

#### Note

The **Business Services** column represents a virtual field whose value is determined by data from both the **Member of Business Services** field and the **Member of Any Business Service or Unassigned** field. If you want to apply a sort relating to the data in **Business Services**, you have to add either or both **Member of Business Services** and **Member of Any Business Service or Unassigned** fields as **columns** and apply the desired sort on either or both of them.

**Step 3** Click **New**. The Permissions Details pop-up displays.

Permission Details

Save Save & New Close

Permission

Details

Type :

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : \*

Member of Any Business Service or Unassigned : ☐

Unassigned to Business Service : ☒

Member of Business Services :

Save Save & New Save & View Close

**Step 4**

Select permissions for the selected user or group.

The permissions available differ depending on the **Type** of permission that you select. Available permissions are Create, Read, Update, Delete, and Execute. For some record types, additional Commands are available. If the permission does not apply to the record type in the Type drop-down, the permission does not appear in the display.

These permissions automatically include other permissions:

- **Create** permission includes **Read** and **Update** permissions.
- **Update** permission includes **Read** permission.
- **Delete** permission includes **Read** permission.

## General Permissions Field Descriptions

The following fields of information and buttons display in the Permissions Details for all [Permission types](#):

Field Name	Description
<b>Details</b>	This section contains detailed information about the permission.
Name	Applies this permission to records whose name matches the string specified here. <a href="#">Wildcards</a> are supported.
Member of Any Business Service or Unassigned	Applies this permission both to records that belong to any Business Service and to records that do not belong to any Business Service.
Unassigned to Business Service	Applies this permission to records that do not belong to any Business Service. If this option is enabled, the user / user group will have the defined permissions on all records that do not belong to any Business Service.
Member of Business Services	Applies this permission to records that are members of the selected <a href="#">Business Service(s)</a> . Click the lock icon to unlock the field and <a href="#">select Business Services</a> .
<b>Metadata</b>	This section contains <a href="#">Metadata</a> information about this record.
UUID	Universally Unique Identifier of this record.
Updated By	Name of the user that last updated this record.
Updated	Date and time that this record was last updated.
Created By	Name of the user that created this record.
Created	Date and time that this record was created.
<b>Buttons</b>	This section identifies the buttons displayed above and below the Permissions Details that let you perform various actions.
<b>Save</b>	Saves a new record in the Controller database.
<b>Save &amp; New</b>	Saves a new record in the Controller database and redisplay empty Details so that you can create another new record.
<b>Update</b>	Saves updates to the record.
<b>Delete</b>	Deletes the current record.
<b>Refresh</b>	Refreshes any dynamic data displayed in the Details.
<b>Close</b>	For pop-up view only; closes the pop-up view of this record.

## Types of Permissions

This section identifies the different types of permissions that you can add to a user or group.

### Agent Permissions

The screenshot shows the 'Permission Details' window with the 'Agent' type selected. The 'Name' dropdown menu is open, displaying three options: 'ALL', 'Resume Agent', and 'Suspend Agent'. The 'Unassigned to Business Service' checkbox is checked. The window includes standard save and close buttons at the top and bottom.

Options	Description
Read	Grants permission to read an Agent definition.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an Agent definition. (Only certain fields can be updated.)
Execute	Grants permission to execute a task on an Agent.
Commands	<ul style="list-style-type: none"> <li>• ALL: Grants permission to suspend and resume Agents.</li> <li>• Resume Agent: Grants permission to resume the ability of a suspended Agent to run tasks.</li> <li>• Suspend Agent: Grants permission to suspend the ability of an Agent to run tasks.</li> </ul>

### Agent Cluster Permissions

(You also can assign Agent Cluster Permissions to a user by assigning the [ops\\_agent\\_cluster\\_admin](#) role to the user.)

Permission Details

SaveSave & NewSave & ViewClose

Permission

Details

Type : Agent Cluster

Create : ☐

Read : ☒

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business : Resume Agent Cluster

Service or Unassigned : Suspend Agent Cluster

Member of Business : Resume Agent Cluster Membership

Services : Suspend Agent Cluster Membership

Resolve Agent Cluster

Unassigned to Business : ☒

Service :

SaveSave & NewSave & ViewClose

Options	Description
Create	Grants permission to create a new Agent Cluster.
Read	Grants permission to read an Agent Cluster definition.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an Agent Cluster definition. (Only certain fields can be updated.)
Delete	Grants permission to delete an Agent Cluster.
Commands	<ul style="list-style-type: none"><li>• ALL: Grants permission to issue any command.</li><li>• Resume Agent Cluster: Grants permission to resume the ability of a suspended Agent Cluster to run tasks.</li><li>• Suspend Agent Cluster: Grants permission to suspend the ability of an Agent Cluster to run tasks.</li><li>• Resume Agent Cluster Membership: Grants permission to resume the membership of an Agent in an Agent Cluster.</li><li>• Suspend Agent Cluster Membership: Grants permission to suspend the membership of an Agent from an Agent Cluster.</li><li>• Resolve Agent Cluster: Grants permission to resolve the Network Alias of an Agent Cluster with a Distribution type of Network Alias.</li></ul>

Application Permissions

Permission Details

Save

Save & New

Save & View

Close

Permission

Details

Type : Application

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : Start

Member of Business Services : Stop

Query

Unassigned to Business Service : ☒

Save

Save & New

Save & View

Close

Options	Description
Create	Grants permission to create a new Application.
Read	Grants permission to read an Application.
Update	Grants permission to update an Application.
Delete	Grants permission to delete an Application.
Commands	See <a href="#">Application Control Tasks</a> for details. Options: <ul style="list-style-type: none"><li>• ALL: Grants permission to execute a Start, Stop, and Query from the Application resource screen.</li><li>• Start: Grants permission to execute a Start from the Application resource screen.</li><li>• Stop: Grants permission to execute a Stop from the Application resource screen.</li><li>• Query: Grants permission to execute a Query from the Application resource screen.</li></ul>

Bundle Permissions

(You also can assign Bundle Permissions to a user by assigning the [ops\\_bundle\\_admin](#) role to the user.)

Permission Details

Save Save & New Save & View Close

Permission

Details

Type: Bundle

Create: ☐

Read: ☐

Update: ☐

Delete: ☐

Commands: -- None --

Name: -- None --

Member of Any Business Service or Unassigned: Promote Bundle

Unassigned to Business Service: ☒

Member of Business Services:

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a Bundle matching both the specified name wildcard and business service membership, including the use of the Create Bundle By Date and Create Bundle By Business Service commands.
Read	Grants permission to read a Bundle matching both the specified name wildcard and business service membership. <ul style="list-style-type: none"> <li>User can run a Bundle Report for a Bundle matching both the specified name wildcard and business service membership.</li> <li>User can Read a Promotion Schedule associated with a Bundle matching both the specified name wildcard and business service membership.</li> </ul>
Update	Grants permission to update a Bundle matching both the specified name wildcard and business service membership, including the use of the Add To Bundle command.
Delete	Grants permission to delete a Bundle matching both the specified name wildcard and business service membership.
Commands	<ul style="list-style-type: none"> <li>ALL: Grants permission to issue any command.</li> <li>Promote Bundle: Grants permission to promote a Bundle.</li> </ul> <p>For the ALL or Promote Bundle command:</p> <ul style="list-style-type: none"> <li>User can promote a Bundle matching both the specified name wildcard and business service membership, assuming the user has Read permission for the Bundle.</li> <li>User can Cancel, Reschedule, or Delete a Promotion Schedule associated with a Bundle matching both the specified name wildcard and business service membership, assuming the user has Read permission for the Bundle.</li> </ul>

## Calendar Permissions

Permission Details

Save Save & New Close

Permission

Details

Type: Calendar

Create: ☐

Read: ☒

Update: ☐

Delete: ☐

Commands: -- None --

Name: -- None --

Member of Any Business Service or Unassigned: ALL

Member of Business Services: Copy Calendar

Unassigned to Business Service: ☒

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a new Calendar.
Read	Grants permission to read a Calendar.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update a Calendar.
Delete	Grants permission to delete a Calendar.
Commands	<ul style="list-style-type: none"> <li>ALL: Grants permission to issue any command.</li> <li>Copy Calendar: Grants permission to copy a Calendar.</li> </ul>

## Credential Permissions

Permission Details

SaveSave & NewClose

Permission

Details

Type :Credential

Create :☐

Read :☒

Update :☐

Delete :☐

Execute :☐

Commands :-- None --

Name :-- None --

Member of Any Business Service or Unassigned :☐

Unassigned to Business Service :☒

Member of Business Services :

SaveSave & NewSave & ViewClose

Options	Description
Create	Grants permission to create a new Credential.
Read	Grants permission to read a Credential.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update a Credential.
Delete	Grants permission to delete a Credential.
Execute	Grants permission to execute a task that requires a Credential.
Commands	N/A

### Database Connection Permissions

(You also can assign Database Connection Permissions to a user by assigning the [ops\\_dba](#) role to the user.)



Permission Details

SaveSave & NewSave & ViewClose

Permission

Details

Type : Database Connection

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : Copy Database Connection

Member of Business Services : Test Connection

Unassigned to Business Service : ☒

SaveSave & NewSave & ViewClose

Options	Description
Create	Grants permission to create a new Database Connection.
Read	Grants permission to read a Database Connection.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update a Database Connection.
Delete	Grants permission to delete a Database Connection.
Execute	Grants permission to execute a task that requires a Database Connection. (Displays only if the <a href="#">Strict Connection Execute Constraints</a> Universal Controller system property is true.)
Commands	<ul style="list-style-type: none"><li>• ALL: Grants permission to issue any command.</li><li>• Copy Database Connection: Grants permissions to copy a Database Connection.</li><li>• Test Connection: Grants permission to test a Database Connection.</li></ul>

### Email Connection Permissions

(You also can assign Email Connection Permissions to a user by assigning the [ops\\_email\\_admin](#) role to the user.)

33 / uc-68x-sec

**Permission Details**

Save Save & New Save & View Close

**Permission**

**Details**

Type : Email Connection

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : ALL

Member of Business Services : Copy Email Connection

Unassigned to Business Service : ☒

Test Connection

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a new Email Connection.
Read	Grants permission to read an Email Connection.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an Email Connection.
Delete	Grants permission to delete an Email Connection.
Execute	Grants permission to execute a task that requires an Email Connection. (Displays only if the <a href="#">Strict Connection Execute Constraints</a> Universal Controller system property is true.)
Commands	<ul style="list-style-type: none"> <li>• ALL: Grants permission to issue any command.</li> <li>• Copy Email Connection: Grants permissions to copy an Email Connection.</li> <li>• Test Connection: Grants permission to test an Email Connection.</li> </ul>

## Email Template Permissions

Permission Details

SaveSave & NewSave & ViewClose

Permission

Details

Type : Email Template

Create : ☐

Read : ☒

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

ALL

Copy Email Template

Member of Any Business Service or Unassigned : 

Unassigned to Business Service : ☒

Member of Business Services :

SaveSave & NewSave & ViewClose

Options	Description
Create	Grants permission to create a new Email Template.
Read	Grants permission to read an Email Template.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an Email Template.
Delete	Grants permission to delete an Email Template.
Commands	<ul style="list-style-type: none"><li>• ALL: Grants permission to issue any command.</li><li>• Copy Email Template: Grants permission to copy an Email Template.</li></ul>

OMS Server Permissions

(You also can assign OMS Server Permissions to a user by assigning the [ops\\_peoplesoft\\_admin](#) role to the user.)

Permission Details

SaveSave & NewSave & ViewClose

Permission

Details

Type : OMS Server

Create : ☐

Read : ☒

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : ☐

Unassigned to Business Service : ☒

Member of Business Services :

SaveSave & NewSave & ViewClose

Options	Description
Create	Grants permission to create a new OMS Server.
Read	Grants permission to read an OMS Server. The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an OMS Server.
Delete	Grants permission to delete an OMS Server.
Commands	N/A

## PeopleSoft Connection Permissions

(You also can assign PeopleSoft Connection Permissions to a user by assigning the [ops\\_peoplesoft\\_admin](#) role to the user.)

Options	Description
Create	Grants permission to create a new PeopleSoft Connection.
Read	Grants permission to read a PeopleSoft Connection.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update a PeopleSoft Connection.
Delete	Grants permission to delete a PeopleSoft Connection.
Execute	Grants permission to execute a task that requires a PeopleSoft Connection. (Displays only if the <a href="#">Strict Connection Execute Constraints</a> Universal Controller system property is true.)
Commands	<ul style="list-style-type: none"> <li>• ALL: Grants permission to issue any command.</li> <li>• Copy PeopleSoft Connection: Grants permission to copy a PeopleSoft Connection.</li> </ul>

## Promotion Target Permissions

(You also can assign Promotion Target Permissions to a user by assigning the [ops\\_promotion\\_admin](#) role to the user.)

**Permission Details**

Permission

Details

Type : Promotion Target

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Execute : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : ALL

Member of Business Services : Refresh Target Agents

Unassigned to Business Service : ☒

Save Save & New Save & View Close

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a Promotion Target matching both the specified name wildcard and business service membership.
Read	Grants permission to read a Promotion Target matching both the specified name wildcard and business service membership. User can View Target Server Info for Promotion Target matching both the specified name wildcard and business service membership.
Update	Grants permission to update a Promotion Target matching both the specified name wildcard and business service membership.
Delete	Grants permission to delete a Promotion Target matching both the specified name wildcard and business service membership
Execute	Grants permission to promote a Bundle using a Promotion Target matching both the specified name wildcard and business service membership, assuming the user has both Read permission and Promote Bundle command permission for the Bundle.
Commands	<ul style="list-style-type: none"> <li>ALL: Grants permission to issue any command.</li> <li>Refresh Target Agents: Grants permission to refresh Target Agents.</li> </ul>

## SAP Connection Permissions

(You also can assign SAP Connection Permissions to a user by assigning the [ops\\_sap\\_admin](#) role to the user.)

Permission Details

Save Save & New Save & View Close

Permission

Details

Type: SAP Connection

Create: ☐

Read: ☐

Update: ☐

Delete: ☐

Commands: -- None --

Name: -- None --  
ALL  
Copy SAP Connection

Member of Any Business Service or Unassigned:

Unassigned to Business Service: ☒

Member of Business Services:

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a new SAP Connection.
Read	Grants permission to read an SAP Connection.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an SAP Connection.
Delete	Grants permission to delete an SAP Connection.
Execute	Grants permission to execute a task that requires an SAP Connection. (Displays only if the <a href="#">Strict Connection Execute Constraints</a> Universal Controller system property is true.)
Commands	<ul style="list-style-type: none"> <li>• ALL: Grants permission to issue any command.</li> <li>• Copy SAP Connection: Grants permissions to copy an SAP Connection.</li> </ul>

## Script Permissions

Options	Description
Create	Grants permission to create a new Script.
Read	Grants permission to read a Script.
Update	Grants permission to update a Script.
Delete	Grants permission to delete a Script.
Execute	Grants permission to execute a Script contained by a task.
Commands	<ul style="list-style-type: none"> <li>• ALL: Grants permission to issue any command.</li> <li>• Copy Script: Grants permission to copy a Script.</li> </ul>

## SNMP Manager Permissions

(You also can assign SNMP Manager Permissions to a user by assigning the [ops\\_snmp\\_admin](#) role to the user.)



Permission Details

Save Save & New Save & View Close

Permission

Details

Type : SNMP Manager

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : ☐

Unassigned to Business Service : ☒

Member of Business Services :

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a new SNMP Manager.
Read	Grants permission to read an SNMP Manager. The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update an SNMP Manager.
Delete	Grants permission to delete an SNMP Manager.
Execute	Grants permission to execute a task that requires an SNMP Manager. (Displays only if the <a href="#">Strict Connection Execute Constraints</a> Universal Controller system property is true.)
Commands	<ul style="list-style-type: none"> <li>ALL: Grants permission to issue any command.</li> <li>Copy SNMP Manager: Grants permissions to copy an SNMP Manager.</li> </ul>

## Task Permissions

Permission Details

SaveSave & NewSave & ViewClose

Permission

Details

Type : Task

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : Copy Task

Member of Business Services : Launch

Recalculate Forecast

Reset Statistics

Reset z/OS Override Statistics

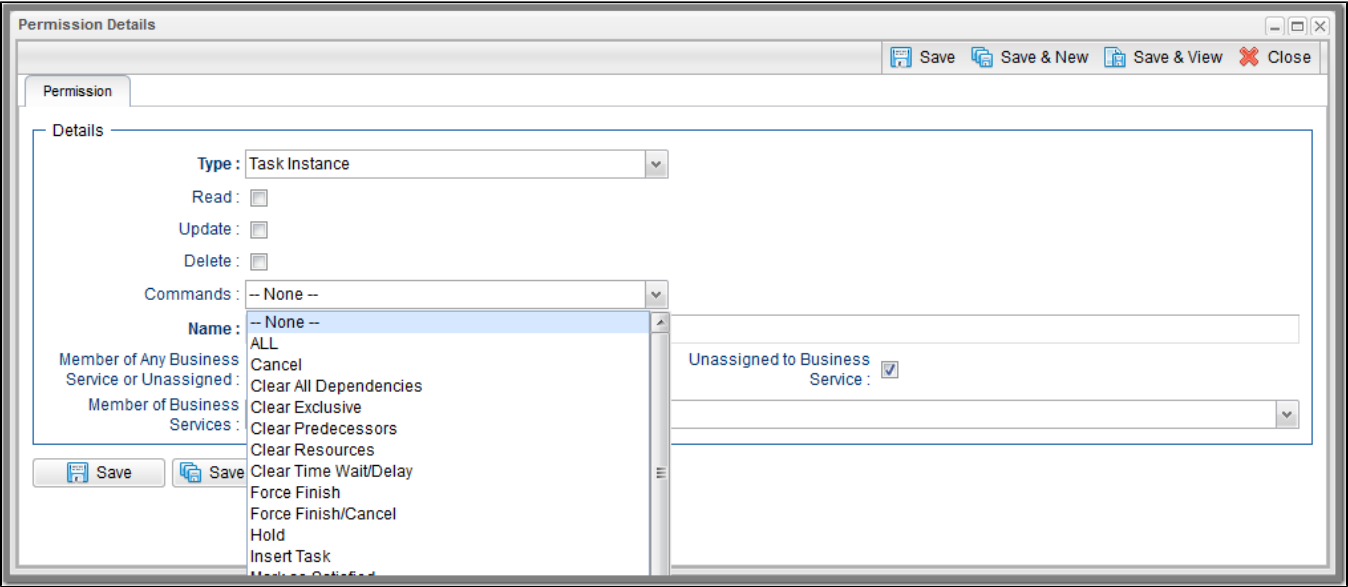
Set Execution Restriction

Unassigned to Business Service : ☒


SaveSave

Options	Description
Create	Grants permission to create a new Task.
Read	Grants permission to read a Task.
Update	Grants permission to update a Task.
Delete	Grants permission to delete a Task.
Commands	<div><ul style="list-style-type: none"><li>• ALL: Grants permission to issue any command.</li><li>• Copy Task: Grants permission to copy a Task.</li><li>• Launch: Grants permission to launch a Task.</li><li>• Recalculate Forecast: Grants permission to recalculate a forecast.</li><li>• Reset Statistics: Grants permission to reset statistics, including statistics being tracked by each parent Workflow of a Task.</li><li>• Reset z/OS Override Statistics: Grants permission to reset z/OS override statistics.</li><li>• Set Execution Restriction: Grants permission to set an execution restriction for a task in a workflow.</li></ul></div>

Task Instance Permissions



Options	Description
Create	Task instances are created automatically when the task launches, so the <b>Create</b> permission does not appear.
Read	Grants permission to read a Task Instance
Update	Grants permission to update certain fields on a Task Instance.
Delete	Grants permission to delete a Task Instance.

Commands	<p>For command descriptions, see <a href="#">Manually Running and Controlling Tasks</a>.</p> <ul style="list-style-type: none"> <li>• ALL: Grants permission to issue any command.</li> <li>• Cancel: Grants permission to cancel a Task Instance.</li> <li>• Clear All Dependencies: Grants permission to clear all dependencies on a Task Instance.</li> <li>• Clear Predecessors: Grants permission to clear all predecessors on a Task Instance.</li> <li>• Clear Exclusive: Grants permission to clear all mutual exclusive dependencies from a Task Instance.</li> <li>• Clear Resources: Grants permission to clear all resource dependencies of a Task Instance.</li> <li>• Clear Time Wait/Delay: Grants permission to clear all Wait To Start and Delay On Start specifications for a Task Instance.</li> <li>• Force Finish: Grants permission to force finish a Task Instance.</li> <li>• Force Finish/Cancel: Grants permission to force finish/cancel a Task Instance.</li> <li>• Hold: Grants permission to put a Task Instance on hold.</li> <li>• Insert Task: Grants permission to insert a task on the workflow monitor of a workflow Task Instance.</li> <li>• Mark as Satisfied: Can mark a dependency as satisfied.</li> <li>• Re-run: Grants permission to re-run a Task Instance.</li> <li>• Release: Grants permission to release a Task Instance from hold.</li> <li>• Release Recursive: Grants permission to release a workflow and all its tasks from hold.</li> <li>• Retrieve Output: Grants permission to execute the Retrieve Output button.</li> <li>• Set Priority Low: Grants permission to change the priority of a task to Low.</li> <li>• Set Priority Medium: Grants permission to change the priority of a task to Medium.</li> <li>• Set Priority High: Grants permission to change the priority of a task to High.</li> <li>• Set Completed: Grants permission to set a Manual Task Instance status to completed.</li> <li>• Set Started: Grants permission to set a Manual Task Instance status to a new started time.</li> <li>• Skip: Grants permission to skip a Task Instance.</li> <li>• Unskip: Grants permission to unskip a Task Instance selected to be skipped.</li> </ul> <p>Note </p> <p>Universal Controller will initially check for command permission specifically for the task instance.</p> <p>If no command permission is granted for the task instance, Universal Controller will check if command permission is granted for the parent workflow task instance, and then continue to check for command permission up the workflow task instance hierarchy.</p>
----------	---

## Trigger Permissions

Permission Details

SaveSave & NewSave & ViewClose

Permission

Details

Type : Trigger

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : -- None --

Member of Any Business Service or Unassigned : Assign Execution User

Member of Business Services : Copy Trigger

Disable Trigger

Enable Trigger

Recalculate Forecast

Trigger Now

Unassigned to Business Service : ☒

SaveSave

Options	Description
Create	Grants permission to create a Trigger.
Read	Grants permission to read a Trigger.
Update	Grants permission to update a Trigger.
Delete	Grants permission to delete a Trigger.
Commands	<ul style="list-style-type: none"><li>• ALL: Grants permission to issue any command.</li><li>• Assign Execution User: Grants permission to override the execution user of task instances launched by a Trigger.</li><li>• Copy Trigger: Grants permission to copy a Trigger.</li><li>• Disable Trigger: Grants permission to disable a Trigger.</li><li>• Enable Trigger: Grants permission to enable a Trigger.</li><li>• Recalculate Forecast: Grants permission to recalculate a forecast.</li><li>• Trigger Now: Grants permission to Trigger (launch) a task.</li></ul>

Variable Permissions

Permission Details

SaveClose

Permission

Details

Type : Variable

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Commands : -- None --

Name : \*

Member of Any Business Service or Unassigned : ☐

Unassigned to Business Service : ☒

Member of Business Services :

Save

Save & New

Save & View

Close

Options	Description
Create	Grants permission to create a Variable.
Read	Grants permission to read a Variable.
Update	Grants permission to update a Variable.
Delete	Grants permission to delete a Variable.
Commands	N/A

Enabling / Disabling Enhanced Variable Security

Important

If you have upgraded from a Controller release that did not previously support the Variable permission type, it is important that you review and assign global variable permissions to all appropriate users/groups to avoid impacting existing workload that requires the use of global variables to execute.

By default, enhanced global variable security is enabled; the [Variable Security Enabled](#) Universal Controller system property is set to true.

This controls global variable access the following ways:

- Users with the [ops\\_admin](#) role have full access to all global variables.
- Users with the [ops\\_promotion\\_admin](#) role have **Read** access to all global variables.
- **Create**, **Read**, **Update**, and **Delete** permissions must be assigned to users explicitly if those permissions are not granted through the [ops\\_admin](#) or [ops\\_promotion\\_admin](#) role.
- Only those global variables for which a user has **Read** permission will be visible from the [Variables list](#).
- Only those global variables for which the **Execution User** of a task instance has **Read** permission will be available within the variable scope of a task instance.

- A [Set Variable action](#) for a global variable will require appropriate global variable **Create** or **Update** permission.
- CLI and Web Services APIs will require appropriate global variable permissions depending on whether the command will **Read**, **Create**, or **Update** a global variable.
- [Create Bundle By Date](#) command will only add a global variable to the bundle if the:
  - Global variable qualifies for the specified date.
  - User invoking the command has **Read** permission for that global variable.

All defined Variable permissions will be enforced unless enhanced global variable security has been disabled by setting [Variable Security Enabled](#) to false. This allows all global variables to be managed and used by any valid Universal Controller user.

## Virtual Resource Permissions

Permission Details

Save Save & New Save & View Close

Permission

Details

Type : Virtual Resource

Create : ☐

Read : ☐

Update : ☐

Delete : ☐

Execute : ☐

Commands : -- None --

Name : -- None --

ALL

Copy Virtual Resource

Member of Any Business Service or Unassigned :

Unassigned to Business Service : ☒

Member of Business Services :

Save Save & New Save & View Close

Options	Description
Create	Grants permission to create a virtual resource.
Read	Grants permission to read a virtual resource.  The <b>Read</b> check box will be checked automatically if the <a href="#">Strict Business Service Membership Read Constraints</a> Universal Controller system property is false.
Update	Grants permission to update a virtual resource.
Delete	Grants permission to delete a virtual resource.
Execute	Grants permission to execute a virtual resource.
Commands	<ul style="list-style-type: none"> <li>• ALL: Grants permission to issue any command.</li> <li>• Copy Virtual Resource: Grants permission to copy a Virtual Resource.</li> </ul>

## Enabling Enhanced Virtual Resource Security

Important



If you have upgraded from a Controller release that did not previously support the Virtual Resource permission type, it is important that you review and assign virtual resource permissions to all appropriate users /groups to avoid impacting existing workload that requires the use of virtual resources to execute.

By default, enhanced virtual resource security is enabled; the [Virtual Resource Security Enabled](#) Universal Controller system property is set to true.

This controls virtual resource access the following ways:

- All users will have **Read** access to virtual resources.
- Users with the [ops\\_admin](#) role will have full access to all virtual resources.
- **Create, Update, Delete,** and **Execution** permissions must be explicitly assigned to users if those permissions are not granted through the [ops\\_promotion\\_admin](#) role.
- Only those virtual resources for which the **Execution User** of the task instance has **Execute** permission can be requested by the task instance. Any virtual resource requested by task instances with an **Execution User** that does not have **Execute** permission for that virtual resource will result in the task instance going into [Start Failure](#) status, with status description **Execution for virtual resource "resource-name" prohibited due to security constraints**.
- Set Virtual Resource Limit [System Operation action](#) will require appropriate virtual resource **Update** permission.
- CLI and Web Services APIs will require appropriate virtual resource permissions: Updating a virtual resource limit through the CLI and Web Services APIs will require virtual resource **Update** permission.

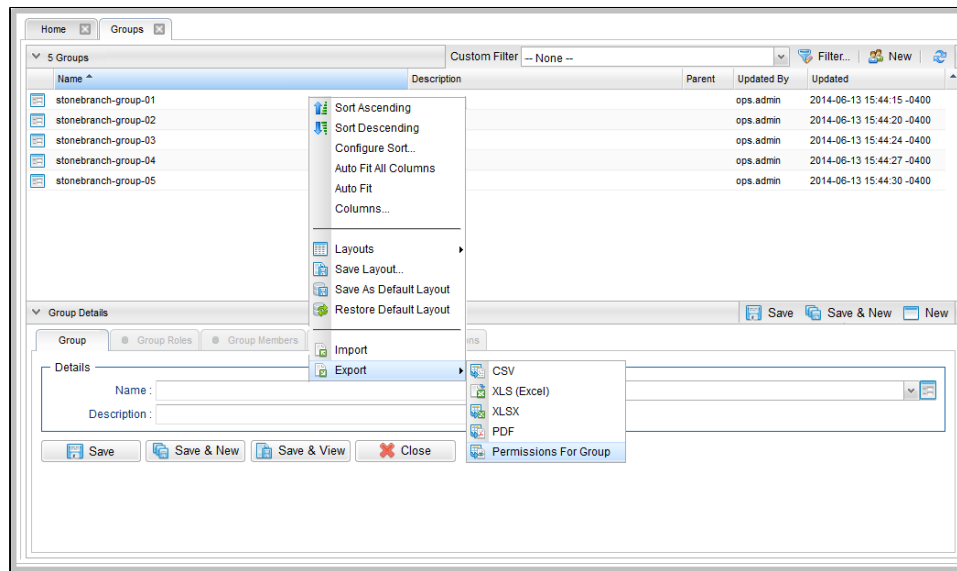
All defined Virtual Resource permissions will be enforced unless enhanced virtual resource security has been disabled by setting [Virtual Resource Security Enabled](#) to false. This allows all virtual resources to be managed and used by any valid Universal Controller user.

## Exporting Permissions for a Group

The Controller lets you export user groups and their permissions, which then can be imported into another Controller system. Only the permissions listed under the Permissions tab for each group will be exported.

Step 1	From the <a href="#">Administration</a> navigation pane, select <b>Security &gt; Groups</b> . The Groups list displays.
Step 2	As desired, <a href="#">filter</a> the list to select the group(s) whose permissions you want to export. When you perform the export, all groups matching the filter will be exported.



**Step 3** Access the [Action menu](#) and select **Export > Permissions For Group**.

To export or import the **Permissions For Group** XML, you must have both the [ops\\_imex](#) and [ops\\_admin](#) roles.

If the groups do not exist on the import system, they (and their Permissions) will be created there.

If the groups do exist on the import system, only the description of the groups and the permissions under their **Permissions** tab will be replaced with those from the imported XML.

# Credentials

- [Overview](#)
- [Types of Credentials](#)
- [Converting Credential Types](#)
- [Credentials Compatibility](#)
- [Resolvable Credentials](#)
  - [Using Resolvable Credentials in a Script](#)
  - [Using Resolvable Credentials in a Task](#)
- [Embedding Resolvable Credentials](#)
  - [Restrictions on Embedding Resolvable Credentials](#)
- [Other Credentials](#)
- [Defining a Credential](#)
  - [Credential Details](#)
  - [Credential Details Field Descriptions](#)
- [Deleting a Credential](#)

## Overview

Credentials are the user ID and password under which an [Agent](#) runs [tasks](#) on the machine where the Agent resides.

By default, an Agent will run tasks under the same Credentials used to install the Agent. However, via the Controller user interface, you also can define Credentials and assign them to any task or Agent.


When prompted for Credentials, the Agent looks in the following locations, in this order, for a user ID and password:

1. If the task specifies Credentials, the Agent uses those Credentials.
2. If the task does not specify Credentials, the Agent uses the Credentials specified in its [Agent Details](#) record.
3. If the Agent Details does not specify Credentials, the Agent uses the Credentials used to install the Agent.

## Types of Credentials

There are four types of Credentials:

Standard	Runtime user name and runtime password of a user.
Resolvable	Runtime user name and runtime password of a user that you can <a href="#">embed</a> into a task or script without exposing the password in clear text.
Web Service	Runtime user name and runtime password of a user running a Web Service task.
Email	Runtime user name and runtime password of a user connecting to an incoming mail server (IMAP).

 **Note**  
Unless Credentials must be [embedded](#), we recommend defining Standard Credentials. If required, you can always [convert](#) a Standard Credential to a Resolvable Credential at a future time.

## Converting Credential Types

You can convert a Credential from any [type](#) to any type.

To convert a Credential type from Standard to Resolvable, Web Service, or Email, the [Resolvable Credentials Permitted](#), [Web Service Credentials Permitted](#), or [Email Credentials Permitted](#) Universal Controller system property, respectively, must be set to true.

To convert a Credential, either:

- Click the **Convert...** button in the [Credential Details](#).
- Select **Convert...** in the Credentials Details [action menu](#).
- Select **Convert...** for a specific Credential in the Credentials List [action menu](#).

When you convert a Credential, you must provide a new password. The Controller will not convert an encrypted password of one Credential type to an encrypted password of a different Credential type.

#### Note



Converting a Credential type does not create a new version of the Credential. Also, you cannot [restore](#) a Credential to an older version if the Credential type of the current version is not the same Credential type as the older version.

## Credentials Compatibility

As of Universal Controller 6.4.x, the Credential Runtime Passwords, along with the [LDAP Settings Bind Password](#), [Email Connection Passwords](#), [Promotion Target Passwords](#), and [Promotion Schedule Promotion Passwords](#), now are encrypted using AES with 128-bit keys.

Additionally, Standard and Resolvable Credentials are encrypted using separate keys; therefore, an encrypted password for a Standard Credential cannot be decrypted by the Resolvable Credential framework.

Under the following circumstances, conversion from the old encryption to the new encryption will be automatic. Furthermore, all pre-6.4.x credentials will be recognized as Standard credentials.

- Apply maintenance to a pre-6.4.x release of Universal Controller to increase it to a 6.7.x release.
- Perform a bulk import or list import from a pre-6.4.x release of Universal Controller to a 6.7.x release.
- Promote from a pre-6.4.x release of Universal Controller to a 6.7.x release.

Under the following circumstance, conversion from the new encryption to the old encryption will be automatic.

- Promote from a 6.7.x release of Universal Controller to a compatible pre-6.4.x release. However, any attempt to promote a Resolvable Credential from a 6.7.x release of Universal Controller to a compatible pre-6.4.x release will fail.

Pre-6.4.0.0 releases cannot decrypt anything encrypted by a 6.7.x release, with the exception of promotion (noted above), which is fully backwards compatible.

Please note the following backwards compatibility constraints with respect to [List Import](#), [Bulk Import](#), and the [Universal Controller Start-up Properties \(opswise.properties\)](#).

- Any attempt to List Import or Bulk Import XML (containing a password encrypted by a 6.7.x release) into a pre-6.4.0.0 release will result in an encrypted value that cannot be decrypted by the pre-6.4.0.0 release.
- Any encrypted passwords within the Universal Controller Start-up Properties will be re-encrypted using the new algorithm when the 6.7.x Controller initializes at start-up. Once converted, that Universal Controller Start-up Properties will no longer be compatible with a pre-6.4.0.0 release.

## Resolvable Credentials

Resolvable Credentials are meant to be used with [scripts](#) and commands specified in [tasks](#), and resolved when the script or command is executed. They provide the script or command with access to Credentials (user name and password) without having to hard-code the Credentials in the script, command, or parameters itself.

In order to enable the use of Resolvable Credentials, the [Resolvable Credentials Permitted](#) Universal Controller system property must be set to true (default is false).

If the [Resolvable Credentials Permitted](#) property is set to false, the following restrictions on Resolvable Credentials apply:

- You cannot create a Resolvable Credential.
- You cannot convert a Standard Credential to a Resolvable Credential.
- Any attempt to launch a task with an embedded Resolvable Credential will result in a Start Failure status.

## Using Resolvable Credentials in a Script

To use Resolvable Credentials with a script, embed the Resolvable Credentials in any of the following:

- [Content](#) of a Script specified in the Script field in a [Linux/Unix](#) or [Windows](#) task
- [Content](#) of a Data Script
- [Universal Template](#) Script (Script, Linux/Unix Script, or Windows Script field)

## Using Resolvable Credentials in a Task

To use Resolvable Credentials with a task, embed the Resolvable Credentials in any of the following:

- Command field in a [Linux/Unix](#) or [Windows](#) task
- Parameters field in a [Linux/Unix](#) or [Windows](#) task

## Embedding Resolvable Credentials

Four Controller [Credentials Functions](#) are available for embedding Resolvable Credentials:

Name	Description	Syntax
<a href="#">Return Key Location of a Credential</a>	Used for embedding the Key Location in a script.	<code>\${_credentialKeyLoc(' &lt;credential_name&gt;')}</code>
<a href="#">Return Passphrase of a Credential</a>	Used for embedding the Passphrase in a script.	<code>\${_credentialPassphrase(' &lt;credential_name&gt;')}</code>
<a href="#">Return User Name of a Credential</a>	Used for embedding the Runtime User in a script.	<code>\${_credentialUser(' &lt;credential_name&gt;')}</code>
<a href="#">Return User Password of a Credential</a>	Used for embedding the Runtime Password in a script.	<code>\${_credentialPwd(' &lt;credential_name&gt;')}</code>

Variables are supported for these Functions.

For example:

- `${_credentialKeyLoc('${my_credential}')}`
- `${_credentialPassphrase('${my_credential}')}`
- `${_credentialUser('${my_credential}')}`
- `${_credentialPwd('${my_credential}')}`

In the resolved script, these Functions are resolved to (for example):

- `$(ops_unv_cred_key_loc_08236da16c3944899aae5a874da077bb)`
- `$(ops_unv_cred_passphrase_08236da16c3944899aae5a874da077bb)`
- `$(ops_unv_cred_user_08236da16c3944899aae5a874da077bb)`
- `$(ops_unv_cred_pwd_08236da16c3944899aae5a874da077bb)`

Additionally, for a [Universal Template](#), you can create a [Field](#) of Type = Credential, which lets you select or create Resolvable Credentials. The Controller will create a variable for the Resolvable Credential Field, which you can embed in the Universal Template script using the Credentials Functions. This also lets you change Credentials when you run a [Universal Task](#) based on the Universal Template.

#### Note



When you embed Resolvable Credentials in a script, the password is exposed in the temporary script on the Agent while the task instance is running.

Resolvable Credentials embedded in a command or parameters field of a Linux/Unix or Windows task are not exposed on the Agent system.

By default, occurrences of Resolvable Credential passwords are scrubbed from the output, reducing (but not eliminating) the risk of passwords echoed directly to the task instance output, which can be retrieved and viewed within the Universal Controller. Please note, however, you still could echo the password to a file on the Agent server.

## Restrictions on Embedding Resolvable Credentials

If an embedded Credential is not a Resolvable Credential, the task instance will transition into the Start Failure status with one of the following status descriptions:

Execution with credentials "credential-name", contained within the Universal Template Script, prohibited due to credential type constraint; only Resolvable credential type permitted.

Execution with credentials "credential-name", contained within the command field or parameters field prohibited due to credential type constraint; only Resolvable credential type permitted.

Execution with credentials "credential-name", contained within the script "script-name", prohibited due to credential type constraint; only Resolvable credential type permitted.

If the [Execution User](#) for a task instance does not have [Execute permission](#) for an embedded Resolvable Credential, the task instance will transition to the Start Failure status with one of the following status descriptions:

Execution with credentials "credential-name", contained within the Universal Template Script, prohibited due to security constraints.

Execution with credentials "credential-name", contained within the command field or parameters field, prohibited due to security constraints.

Execution with credentials "credential-name", contained within the script "script-name", prohibited due to security constraints.

Execution with credentials "credential-name", contained within a script, prohibited due to security constraints.

If the [Resolvable Credentials Permitted](#) Universal Controller system property is set to false, any task instance with an embedded Resolvable Credential will result in a Start Failure status with the following status description:

Execution with resolvable credentials not permitted; Universal Controller property "Resolvable Credentials Permitted" is not enabled.

If an embedded Resolvable Credential cannot be decrypted, the task instance will transition into the Start Failure status with the following status description:

Unable to decrypt password for "credential-name" credentials.

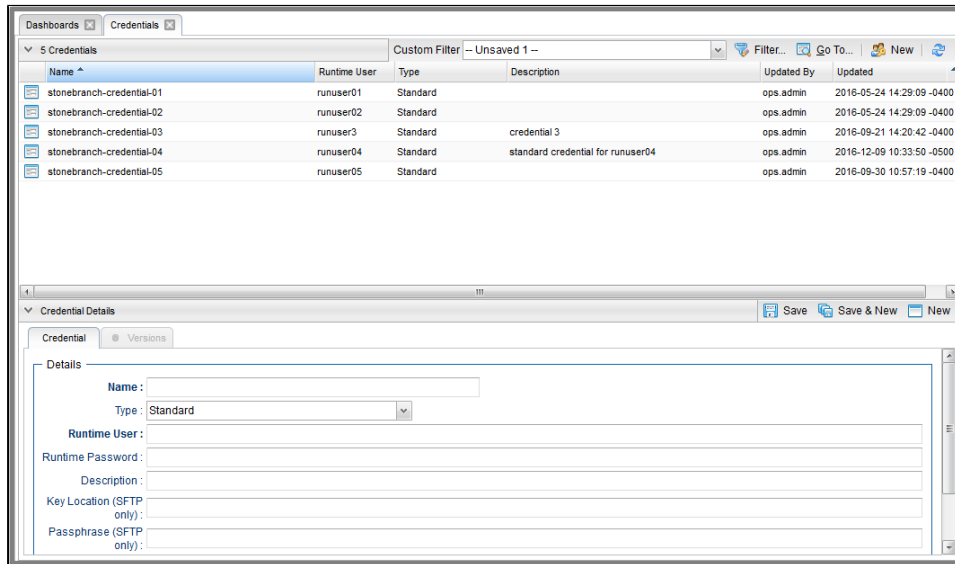
## Other Credentials

You can embed source and destination Credentials in a UDM script using [File Transfer Task Instance built-in variables](#).

For [File Transfer tasks](#), the Agent may need additional credentials for logging on to the FTP server.

## Defining a Credential

- Step 1** From the [Automation Center](#) navigation pane, select **Other > Credentials**. The Credentials list displays a list of all currently defined Credentials. Below the list, Credential Details for a new Credential displays.



- Step 2** Enter/select Details for a new Credential, using the [field descriptions](#) below as a guide. As a best practice, use an alias in the **Name** field, as you may have several identical user names for different systems all having different passwords.

- Required fields display in **boldface**.
- Default values for fields, if available, display automatically.

To display more of the Details fields on the screen, you can either:

- Use the scroll bar.
- Temporarily [hide the list](#) above the Details.
- Click the **New** button above the list to display a pop-up version of the Details.

- Step 3** Click a **Save** button. The Credential is added to the database, and all buttons and tabs in the Credential Details are enabled.

Note



To **open** an existing record on the list, either:

- Click a record in the list to display its record Details below the list. (To clear record Details below the list, click the **New** button that displays above and below the Details.)
- Clicking the **Details icon** next to a record name in the list, or right-click a record in the list and then click **Open** in the **Action menu** that displays, to display a pop-up version of the record Details.
- Right-click a record in the a list, or open a record and right-click in the record Details, and then click **Open In Tab** in the **Action menu** that displays, to display the record Details under a new tab on the record list page (see **Record Details as Tabs**).

Credential Details

The following Credential Details is for an existing credential. See the [field descriptions](#), below, for a description of all fields that display in the Credential Details.

Credential Details: stonebranch-credential-01

Update

Convert...

Delete

Refresh

Close

Credential

Versions

Details

Name :

stonebranch-credential-01

Version :

1

Type :

Standard

Runtime User :

runuser01

Runtime Password :

Description :

Key Location (SFTP only) :

Passphrase (SFTP only) :

Member of Business Services :

Update

Convert...

Delete

Refresh

Close

For information on how to access additional details - such as [Metadata](#) and complete [database Details](#) - for Credentials (or any type of record), see [Records](#).

Credential Details Field Descriptions

The following table describes the fields, buttons, and tabs that display in the Credential Details.

Field Name	Description
Details	This section contains detailed information about the credential.
Name	Required. Name for this credential.
Version	System-supplied; version number of the current record, which is incremented by Universal Controller every time a user updates a record. Click on the <a href="#">#Versions</a> tab to view previous versions. For details, see <a href="#">Record Versioning</a> .

Type	<p>Type of Credential.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• Standard (default)</li> <li>• Resolvable</li> <li>• Web Service</li> <li>• Email</li> </ul> <p>Note</p> <p>Only Resolvable Credentials can be embedded in a <a href="#">Universal Template</a> script.</p>
Runtime User	<p>Runtime user ID, including an LDAP- or AD-formatted user ID, under which the job will be run.</p> <p>If the user does not have a login shell, add a - character in front of the ID. The Controller will provide a shell for that user and strip the - character from the username.</p> <p>When specifying a Windows account, be aware that the user must have the following privileges based upon the Universal Agent's configuration for the UAG <a href="#">logon</a> option:</p> <ul style="list-style-type: none"> <li>• logon = Interactive (default) <ul style="list-style-type: none"> <li>• Not be in "Deny log on locally."</li> <li>• Be a member of "Allow log on locally."</li> </ul> </li> <li>• logon = Batch <ul style="list-style-type: none"> <li>• Not be in "Deny log on as a batch job"</li> <li>• Be a member of "Allow log on as a batch job"</li> </ul> </li> </ul> <p>When specifying a <b>local</b> Windows account that may be used by an Agent running inside a Windows domain environment, be sure to use "." as a placeholder for the domain name (for example, ".\&lt;localuser&gt;").</p> <p>This qualifies the account name and ensures that Windows will authenticate it against the local – and not the active directory – account database. If the "." placeholder is missing, the account may be interpreted as a domain account in a domain environment, and a task using that credential may fail.</p> <p>If none of your Agents execute on a Windows domain member or domain controller, the placeholder is optional.</p> <p>If a domain account must be used, you may specify the account name using the user principal name (UPN) format (that is, "&lt;domainuser&gt;@&lt;domainname&gt;") or the down-level logon name format (that is, "&lt;domainname&gt;\&lt;domainuser&gt;").</p>
Runtime Password	<p>Runtime user's password. Maximum is 512 characters.</p> <p>Note</p> <p>As of Universal Controller release 6.4.4.0, a credential with a password greater than 40 characters can now be used for an agent-based task instance that uses Universal Agent 6.4.2.0 or greater. If the Universal Agent release is earlier than 6.4.2.0, the agent-based task instance will continue to go Start Failure with the expected Status Description. Credentials with a password greater than 40 characters are supported only on Universal Agent 6.4.2.0 or higher.</p>
Description	<p>Description of this record. (Maximum = 200 characters.)</p>
Key Location (SFTP only)	<p>Using SFTP requires that you supply a valid credential that specifies the location of the SSL Private key on your Agent. This field provides the location, which must exist on the Agent where you intend to run the SFTP task. Currently, the Controller does not support password authentication for SFTP Transfer.</p> <p>For File Transfer over SSL, make sure you have your private/public keys properly set up and working before you configure the Controller to use it. For example, to validate the keys, log into your destination server from your agent server using ssl.</p>



Pass Phrase (SFTP only)	Pass phrase for the Runtime User's SSL Private key file.
Member of Business Services	User-defined; allows you to select one or more <a href="#">Business Services</a> that this record belongs to.  If the <a href="#">Business Service Visibility Restricted</a> Universal Controller system property is set to true, depending on your assigned (or inherited) <a href="#">Permissions</a> or <a href="#">Roles</a> , Business Services available for selection may be restricted.
<b>Metadata</b>	This section contains <a href="#">Metadata</a> information about this record.
UUID	Universally Unique Identifier of this record.
Updated By	Name of the user that last updated this record.
Updated	Date and time that this record was last updated.
Created By	Name of the user that created this record.
Created	Date and time that this record was created.
<b>Buttons</b>	This section identifies the buttons displayed above and below the Credential Details that let you perform various actions.
<b>Save</b>	Saves a new Credential record in the Controller database.
<b>Save &amp; New</b>	Saves a new record in the Controller database and redisplay empty Details so that you can create another new record.
<b>Save &amp; View</b>	Saves a new record in the Controller database and continues to display that record.
<b>New</b>	Displays empty (except for default values) Details for creating a new record.
<b>Update</b>	Saves updates to the record.
<b>Convert...</b>	Allows you to convert the current Credential <a href="#">#Type</a> to a new type and define a new password for the Credential (see <a href="#">#Converting Credential Types</a> ).
<b>Delete</b>	Deletes the current record.
<b>Refresh</b>	Refreshes any dynamic data displayed in the Details.
<b>Close</b>	For pop-up view only; closes the pop-up view of this credential.
<b>Tabs</b>	This section identifies the tabs across the top of the Credential Details that provide access to additional information about the credential.
<b>Versions</b>	Stores copies of all previous versions of the current record. See <a href="#">Record Versioning</a> .

## Deleting a Credential

You cannot delete a Credential if any references exist for the Credential.

References will be checked according to the Credential type, as shown in the following table:

Credential Type	Record Type
Resolvable	<ul style="list-style-type: none"> <li>• Universal Task (Credentials Fields 1-4)</li> <li>• Universal Template Field (Default Value)</li> </ul>
Email	<ul style="list-style-type: none"> <li>• Email Monitor (Credentials)</li> </ul>
Web Service	<ul style="list-style-type: none"> <li>• Web Service Task (Credentials)</li> </ul>
Standard	<ul style="list-style-type: none"> <li>• Windows Agent (Credentials)</li> <li>• Linux/Unix Agent (Credentials)</li> <li>• Application (Credentials)</li> <li>• Database Connection (Credentials)</li> <li>• PeopleSoft Connection (Credentials)</li> <li>• Windows Task (Credentials)</li> <li>• Linux/Unix Task (Credentials)</li> <li>• z/OS Task (Credentials)</li> <li>• Universal Command Task (Utility Credentials, UCMD Credentials)</li> <li>• SAP Task (Utility Credentials, SAP Credentials)</li> <li>• PeopleSoft Task (Utility Credentials, PeopleSoft Credentials)</li> <li>• File Transfer Task (Credentials, FTP Credentials, Source Credentials, Destination Credentials)</li> <li>• SQL Task (Credentials)</li> <li>• Stored Procedure Task (Credentials)</li> <li>• File Monitor Task (Credentials)</li> <li>• FTP File Monitor Task (Credentials, FTP Credentials)</li> <li>• System Monitor (Credentials)</li> <li>• Universal Task (Credentials)</li> <li>• Universal Template (Credentials)</li> </ul>

## Note



Resolvable, Email, and Web Service Credentials can be used anywhere that a Standard Credential can be specified.

# Business Services

- [Overview](#)
  - [Record Types for Business Services](#)
- [Creating Business Services](#)
  - [Business Service Details](#)
  - [Business Service Details Field Descriptions](#)
- [Business Service Membership Considerations for Create, Read, Update, Delete, and Execute](#)

## Overview

The Universal Controller Business Services feature allows you to organize your data into groups of related information.

You can create Business Services that represent your organization and [assign individual records](#) of different [record types](#) to each Business Service. You can then sort and filter the lists of these record types based on the Business Services, as well as generate reports.

For example, you may want to place all records of different record types related to accounting in a Business Service named Accounting.

You also can take advantage of Business Services when you set up security by [assigning permissions](#) to users and groups for records that are members of specific Business Services.

You also can [promote Bundles](#) that include records from one or more specific Business Services.

## Record Types for Business Services

You can assign any record of the following record types to one or more Business Services:

- Agent
- Agent Cluster
- Application
- Calendar
- Credential
- Database Connection
- Email Connection
- Email Template
- PeopleSoft Connection
- SAP Connection
- Script
- SNMP Manager
- Task
- Task Instance
- Trigger
- Variable
- Virtual Resource

## Creating Business Services

Note



You must be assigned the `ops_admin` role in order to perform this procedure.

Step 1

From the [Administration](#) navigation pane, select **Security > Business Services**. The Business Services list displays.

Below the list, Business Service Details for a new Business Service displays.

Business Services

5 Business Services

Custom Filter: -- None --

Filter...

Go To...

New

Name	Description	Updated By	Updated
stonebranchbusinessservice 01		stonebranch-user-01	2014-06-13 15:19:37 -0400
stonebranchbusinessservice 02		stonebranch-user-02	2014-06-13 15:19:47 -0400
stonebranchbusinessservice 03		stonebranch-user-03	2014-06-13 15:19:51 -0400
stonebranchbusinessservice 04		stonebranch-user-04	2014-06-13 15:19:56 -0400
stonebranchbusinessservice 05		stonebranch-user-05	2014-06-13 15:20:00 -0400

Business Service Details

Save Save & New New

Business Service

Versions

Details

Name

Description

Save Save & New New

Step 2

Enter/select Details for a new Business Service, using the [field descriptions](#) below as a guide.

- Required fields display in **boldface**.
- Default values for fields, if available, display automatically.

To display more of the Details fields on the screen, you can either:

- Use the scroll bar.
- Temporarily [hide the list](#) above the Details.
- Click the **New** button above the list to display a pop-up version of the Details.

Step 3

Click a **Save** button. The Business Service is added to the database, and all buttons and tabs in the Business Service Details are enabled.

Note

To [open](#) an existing record on the list, either:

- Click a record in the list to display its record Details below the list. (To clear record Details below the list, click the **New** button that displays above and below the Details.)
- Clicking the [Details icon](#) next to a record name in the list, or right-click a record in the list and then click **Open** in the [Action menu](#) that displays, to display a pop-up version of the record Details.
- Right-click a record in the a list, or open a record and right-click in the record Details, and then click **Open In Tab** in the [Action menu](#) that displays, to display the record Details under a new tab on the record list page (see [Record Details as Tabs](#)).

60 / uc-68x-sec

## Business Service Details

The following Business Service Details is for an existing Business Service. See the [field descriptions](#) below for a description of the fields that display in the Business Service Details.

Business Service Details: stonebranchbusinessservice 01

UpdateDeleteRefreshClose

Business ServiceVersions

Details

Name : stonebranchbusinessservice 01Version : 1

Description :


UpdateDeleteRefreshClose

For information on how to access additional details - such as [Metadata](#) and complete [database Details](#) - for Business Services (or any type of record), see [Records](#).

## Business Service Details Field Descriptions

The following table describes the fields, buttons, and tabs that display in the Business Service Details.

Field Name	Description
Details	This section contains detailed information about the Business Service.
Name	Name used within the Controller to identify this Business Service. It can contain a maximum of 40 alphanumeric.
Version	System-supplied; version number of the current record, which is incremented by the Controller every time a user updates a record. Click the <a href="#">#Versions tab</a> to view previous versions. For details, see <a href="#">Record Versioning</a> .
Description	User-defined: description of this record.
Metadata	This section contains <a href="#">Metadata</a> information about this record.
UUID	Universally Unique Identifier of this record.
Updated By	Name of the user that last updated this record.
Updated	Date and time that this record was last updated.
Created By	Name of the user that created this record.
Created	Date and time that this record was created.

<b>Buttons</b>	This section identifies the buttons displayed above and below the Task Details that let you perform various actions.
<b>Save</b>	Saves a new task record in the Controller database.
<b>Save &amp; New</b>	Saves a new record in the Controller database and redisplay empty Details so that you can create another new record.
<b>Save &amp; View</b>	Saves a record in the Controller database and continues to display that record.
<b>New</b>	Displays empty (except for default values) Details for creating a new record.
<b>Update</b>	Saves updates to the record.
<b>Delete</b>	<p>Deletes the current record.</p> <p>Note </p> <p>You cannot delete a Business Service if it has been assigned to one or more <a href="#">records</a>.</p>
<b>Refresh</b>	Refreshes any dynamic data displayed in the Details.
<b>Close</b>	For pop-up view only; closes the pop-up view of this task.
<b>Tabs</b>	This section identifies the tabs across the top of the Task Details that provide access to additional information about the task.
<b>Versions</b>	Stores copies of all previous versions of the current record. See <a href="#">Record Versioning</a> .

## Business Service Membership Considerations for Create, Read, Update, Delete, and Execute

When creating or updating a record, use the **Member of Business Services** field to select one or more Business Services for that record. This, in effect, assigns the record to that Business Service.

You cannot perform an operation (create, read, update, or delete) or issue a command (such as copy) on a record that is a member of a Business Service if you do not have a Permission defined for that record type that includes that operation/command and Business Service membership.

### Create

When creating a record that is a member of one or more Business Services, the user must have Create permission that applies for each Business Service that the record is becoming a member of; otherwise, the operation will be prohibited.

### Read

When reading/viewing a record (for example, a list or record Details), the user needs only Read permission for one of the Business Services that the record is a member of.

Note 

Depending on the value of the [Strict Business Service Membership Read Constraints](#) system property, users may be granted implicit Read permission for specific record types. Refer to the property for more details.

### Update

When updating a record, the user must have Update permission for both the original record and the updated record.

As long as an update is not changing the Business Service memberships of a record, the user needs only Update permission for one of the Business Services that the record is a member of.

If the update is adding or removing Business Service membership, further security constraints apply:

- For any added Business Service, the user must have Update permission for the modified record that applies explicitly for the Business Service being added.
- For any removed Business Service, the user must have Update permission for the original record that applies explicitly for the Business Service being removed.

**Delete**

When deleting a record that is a member of one or more Business Services, the user must have Delete permission that applies for each Business Service the record is a member of; otherwise, the operation will be prohibited.

**Execute**

At task instance run time, the task instance Execution User requires Execute permission, or Read permission if Execute permission is not applicable, for the following record type dependencies.

Tasks running on an Agent	Execution User requires Execute permission for that Agent.
Tasks requiring a Credential	Execution User requires Execute permission for that Credential. (References to Credentials can exist for both non agent-based and agent-based task types. Furthermore, agents can specify default Credentials, even if the Credentials are not directly defined on the task.)
Tasks running a Script	Execution User requires Execute permission for that Script.
Tasks needing to read a Global Variable	Execution User requires Read permission for that Global Variable.
Tasks requiring a Virtual Resource	Execution User requires Execute permission for that Virtual Resource.

# Audits

- [Overview](#)
- [Displaying Audits](#)
  - [Audit Details Field Descriptions](#)

## Overview

Audits are detailed records of all user interactions with the Controller, including before and after information related to any change and a description of the difference.

Audits are created when the user performs any of the following [actions](#):

- [Logging](#) actions: log in, log out, or login failure.
- Creates, updates, or deletes a [record](#).
- Issues an [action or command](#) (for example, Launch Task or Trigger Now).
- [Imports](#) or [exports](#) records on a list.

## Displaying Audits

**Step 1** From the [Administration](#) navigation pane, select **Security > Audits**.

You can change the default time constraint for the display of audits on the list via the [Audit Time Constraint](#) user preference.

Audit Type	Source	Status	Description	Created By	Created
Create	User Interface	Success	Create: TimeTriggerBean 51304 SET:SecondSundayOfMth-No, sys_id: 1c659e47b47e4222bedacbb2...	lawvver	2018-03-21 17:11:48 -0400
Create	User Interface	Success	Create: TimeTriggerBean 51304 SET:SecondSundayOfMthPlusOneDays-No, sys_id: b705c65047d...	lawvver	2018-03-21 17:13:47 -0400
Create	User Interface	Success	Create: TimeTriggerBean 51304 SET:SecondSundayOfMthPlusOneDays-No, sys_id: 454dcaff1b4a...	lawvver	2018-03-21 17:14:58 -0400
Create	User Interface	Success	Create: TimeTriggerBean 51304 SET:SecondSundayOfMthPlusTwoDays-No, sys_id: 98909903bec...	lawvver	2018-03-21 17:17:12 -0400
Delete	User Interface	Success	Delete: DatabaseConnectionBean Copy of stonebranch-databaseconnection-05, sys_id: a9c82ba5e...	ops.admin	2018-03-20 16:05:04 -0400
Delete	User Interface	Success	Delete: DatabaseConnectionBean Copy of stonebranch-databaseconnection-04, sys_id: f4285e2118...	ops.admin	2018-03-20 16:05:04 -0400
Delete	User Interface	Success	Delete: DatabaseConnectionBean Copy of stonebranch-databaseconnection-03, sys_id: 2b1990de2c...	ops.admin	2018-03-20 16:05:04 -0400
Command	User Interface	Success	Executing Command: COPY DATABASE CONNECTION on stonebranch-databaseconnection-05	ops.admin	2018-03-20 16:04:49 -0400
Command	User Interface	Success	Executing Command: COPY DATABASE CONNECTION on stonebranch-databaseconnection-04	ops.admin	2018-03-20 16:04:49 -0400
Command	User Interface	Success	Executing Command: COPY DATABASE CONNECTION on stonebranch-databaseconnection-03	ops.admin	2018-03-20 16:04:49 -0400
Command	Scheduled	Success	Executing Command: RUN DATA BACKUP/PURGE on System Default - Audit (Table: Audit)	ops.system	2018-03-21 02:22:00 -0400
Command	Scheduled	Success	Executing Command: RUN DATA BACKUP/PURGE on System Default - Migration (Table: Migration)	ops.system	2018-03-21 03:33:00 -0400



**Step 2** To display Details about a specified audit, click the icon next to the **Audit Type** for that audit, or click anywhere in the Audit row. The Audit Details for that audit then displays.

Audit Details: Update

Refresh

Close

Audit

Child Audits

Details

Audit Type : Update

Source : User Interface

Created : 2016-12-09 10:33:50 -0500

Created By : ops.admin

Node Id : qa-cntrir-mysql.stone.branch:8080-qa\_cntrir\_mysql

Node Mode : Active

Status : Success

Table Name : ops\_credentials

Table Key : 444e0cf355894a179b06b932c38f1238

Table Record Name : stonebranch-credential-04

Parent Audit :

Description : Update: CredentialsBean stonebranch-credential-04, sys\_id: 444e0cf355894a179b06b932c38f1238

Before : CredentialsBean [ {credentials=stonebranch-credential-04} {description=null} {opswise\_groups=null} {runtime\_key\_location=null} {runtime\_pass\_phrase=null} {runtime\_password=\*\*\*\*} {runtime\_user=runuser04} {sys\_created\_by=ops.admin} {sys\_created\_on=2016-05-24 14:29:09 -0400} {sys\_id=444e0cf355894a179b06b932c38f1238} {sys\_updated\_by=ops.admin} {sys\_updated\_on=2016-05-24 14:29:09 -0400} {type=Standard} {version=1} ]

After : CredentialsBean [ {credentials=stonebranch-credential-04} {description=standard credential for runuser04} {opswise\_groups=null} {runtime\_key\_location=null} {runtime\_pass\_phrase=null} {runtime\_password=\*\*\*\*} {runtime\_user=runuser04} {sys\_created\_by=ops.admin} {sys\_created\_on=2016-05-24 14:29:09 -0400} {sys\_id=444e0cf355894a179b06b932c38f1238} {sys\_updated\_by=ops.admin} {sys\_updated\_on=2016-12-09 10:33:50 -0500} {type=Standard} {version=2} ]

Difference : [Added description: standard credential for runuser04] [Changed version: 1 -> 2]

Additional Information :

Refresh

Close

Audit Details Field Descriptions

The following table describes the fields and tabs that display in the Audit Details.

Field Name	Description
Details	This section contains detailed information about the audit.

Audit Type	Type of audit for which this Audit record was created.  Options: <ul style="list-style-type: none"> <li>• CLI</li> <li>• Create</li> <li>• Command</li> <li>• Delete</li> <li>• Delete Override File</li> <li>• Delete Version</li> <li>• Email</li> <li>• Export</li> <li>• Import</li> <li>• Restore Version</li> <li>• Server Operation</li> <li>• Update</li> <li>• User Login</li> <li>• z/OS Auto-Restart</li> </ul>
Table Name	Name of the table for which the user interaction was performed.
Source	Location of the user interaction.  Options: <ul style="list-style-type: none"> <li>• Agent Message</li> <li>• Command Line</li> <li>• Email Notification</li> <li>• Scheduled</li> <li>• Set Variable Action</li> <li>• Task Instance</li> <li>• User Interface</li> <li>• Web Service</li> </ul>
Table Key	Encrypted key to the table for which the user interaction was performed.
Created	Date when this audit was created.
Table Record Name	Name of the table record for this user interaction was performed.
Created By	User that created this audit.
Node ID	URL of the cluster node on which this Audit was created.
Parent Audit	Parent audit for which this audit was created automatically.
Node Mode	Mode of the cluster node on which this Audit was created.
Status	Status of the audit.
Description	Description of the user interaction for which this audit was created.
Before	Image of data before the user interaction.
After	Image of data after the user interaction.
Difference	Difference in the data as a result of the user interaction

Additional Information	Any additional information captured for this user interaction.
<b>Metadata</b>	This section contains <a href="#">Metadata</a> information about this record.
UUID	Universally Unique Identifier of this record.
Updated By	Name of the user that last updated this record.
Updated	Date and time that this record was last updated.
Created By	Name of the user that created this record.
Created	Date and time that this record was created.
<b>Buttons</b>	This section identifies the buttons displayed above and below the Audit Details that let you perform various actions.
<b>Refresh</b>	Refreshes any dynamic data displayed in the Audit Details.
<b>Close</b>	Closes the Audit Details.
<b>Tabs</b>	This section identifies the tabs across the top of the Audit Details that provide access to additional information about the audit.
Child Audits	List of any child audits for this audit.