Universal Controller 6.3.x

Security

Security

Setting Up Security

Overview

Adding Users

Adding Groups

Assigning Roles to Users or Groups

Assigning Permissions to Users or Groups

Login Credentials

Business Services

Audit Records

Viewing Audit Records

The information on these pages also is located in the Universal Controller 6.3.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.

Users and Groups

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.

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

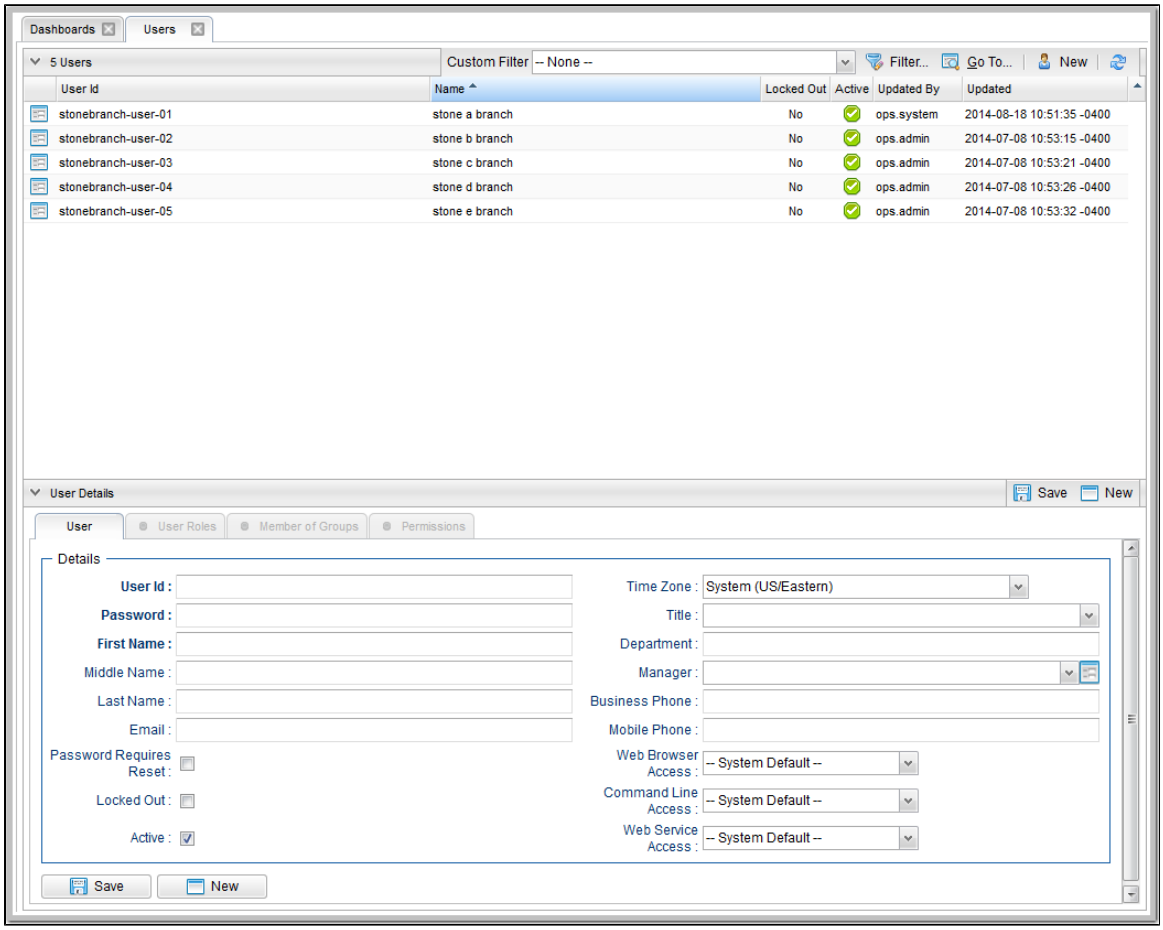
There are two default groups:

- **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.

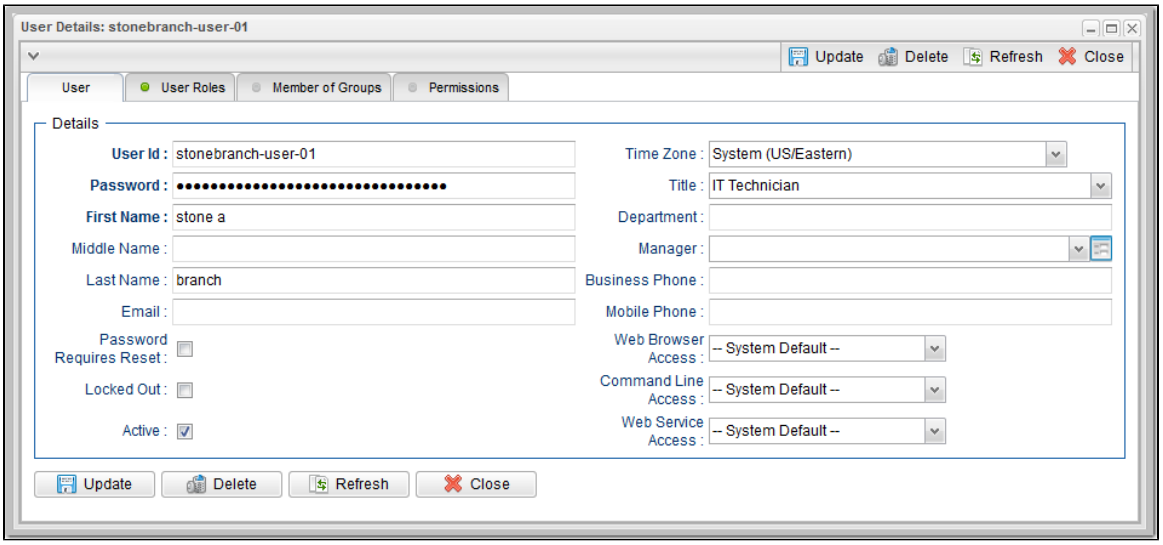
Step 1	From the Administration navigation pane, select **Security > Users**. The Users list displays a list of all currently defined users. Below the list, User Details for a new user displays. 
Step 2	Enter/select Details for a new user, using the field descriptions below as a guide. • Required fields 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 the **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 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.
First Name	First name of this user.
Middle Name	Middle name of this user.
Last Name	Last name 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.
Active	If enabled, the user ID is active and the user can log in. If disabled, the user is permanently deactivated; the user will not appear in user lists and cannot be used for access to the Controller.
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.

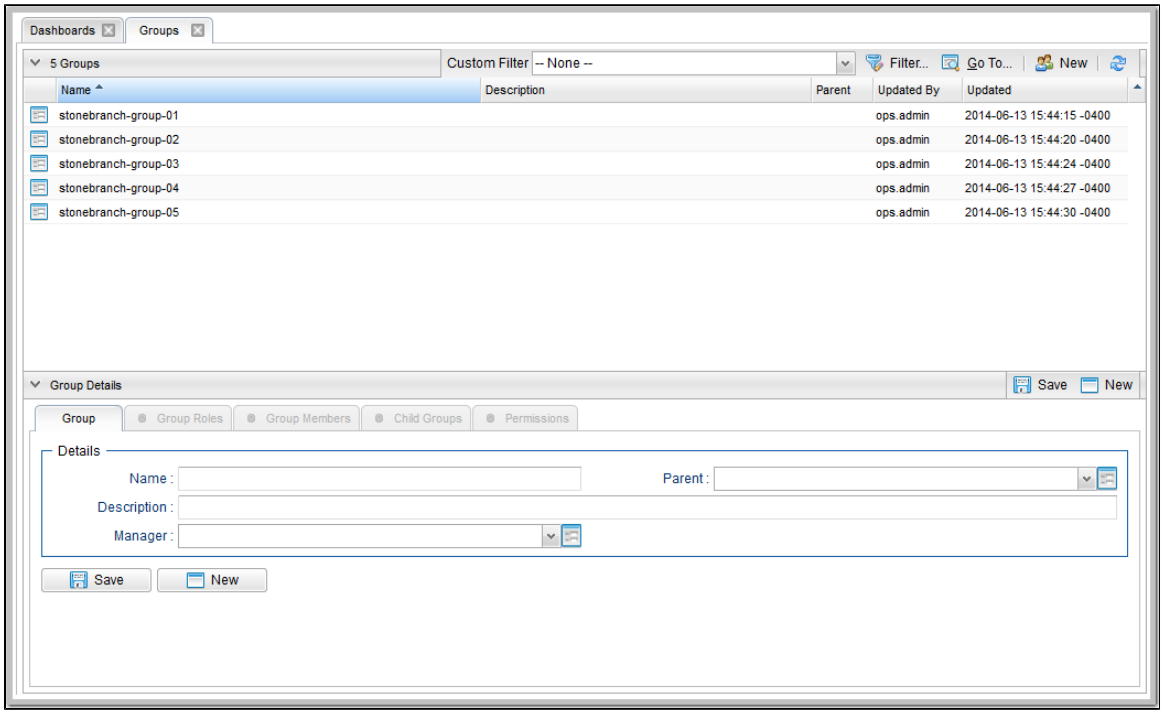
Web Browser Access	Specifies whether or not the user can log in to the user interface. Options: • System Default - User restriction for logging in to the user interface is based on the current system default value of the System Default Web Browser Access Universal Controller system property. • Yes - User is not restricted from logging in to the user interface. • No - User is restricted from logging in to the user interface.
Command Line Access	Specifies whether or not the user can log in to the Universal Controller Command Line Interface (CLI). Options: • System Default - User restriction for logging in to the CLI is based on the current system default value of the System Default Command Line Access Universal Controller system property. • Yes - User is not restricted from logging in to the CLI. • No - User is restricted from logging in to the CLI.
Web Service Access	Specifies whether or not the user can log in to the Universal Controller RESTful Web Services API. Options: • System Default - User restriction for logging in to the Universal Controller Web Services is based on the current system default value of the System Default Web Service Access Universal Controller system property. • Yes - User is not restricted from logging in to the Universal Controller Web Services. • No - User is restricted from logging in to the Universal Controller Web Services.
Buttons	This section identifies the buttons displayed above and below the User Details that let you perform various actions.
Save	Saves a new user record in the Controller database.
Update	Saves updates to the record.
New	Displays empty (except for default values) Details for creating a new user.
Delete	Deletes the current record.
Refresh	Refreshes any dynamic data displayed in the Details.
Close	For pop-up view only; closes the pop-up view of this user.
Tabs	This section identifies the tabs across the top of the User Details that provide access to additional information about the user.
User Roles	Allows you to assign roles to this user.
Member of Groups	Allows you to assign this user to one or more groups.
Permissions	Allows you to assign permissions 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.

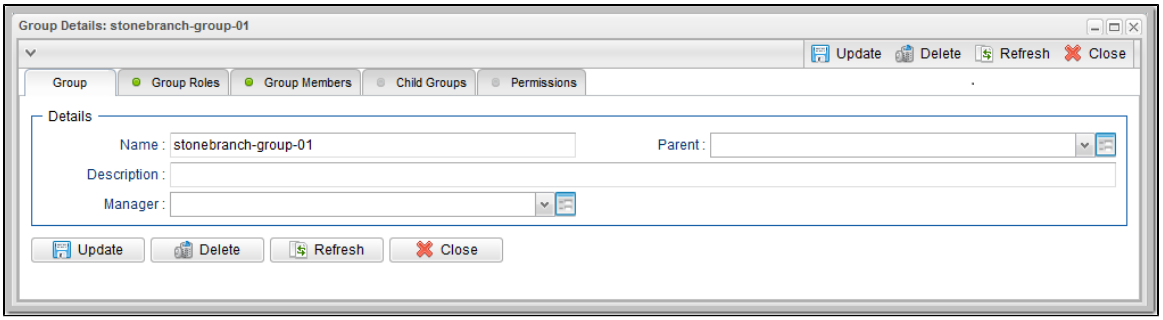
Step 1	From the Administration navigation pane, select **Security > Groups**. The Groups list displays a list of all currently defined groups. Below the list, Group Details for a new group displays. 
Step 2	Enter/select Details for a new group, using the field descriptions below as a guide. • Required 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 the **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

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 Field Descriptions

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

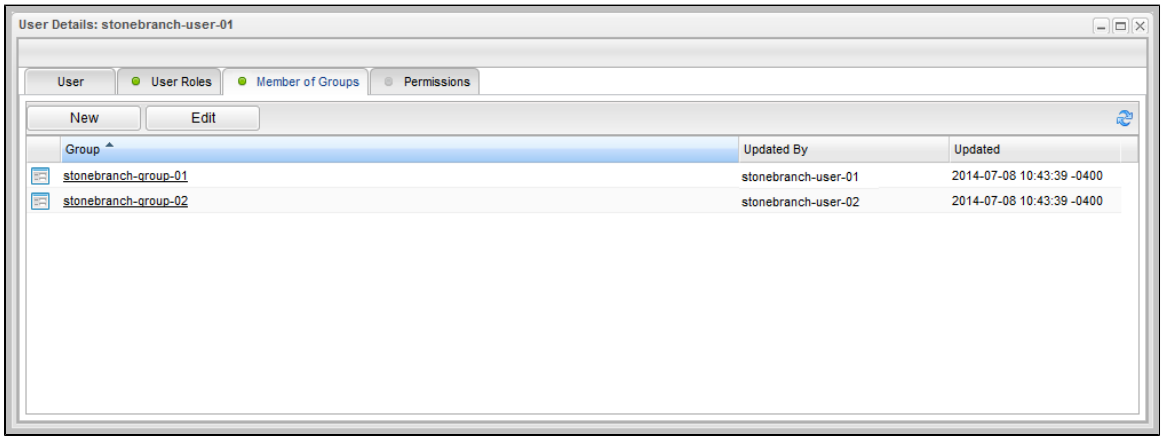
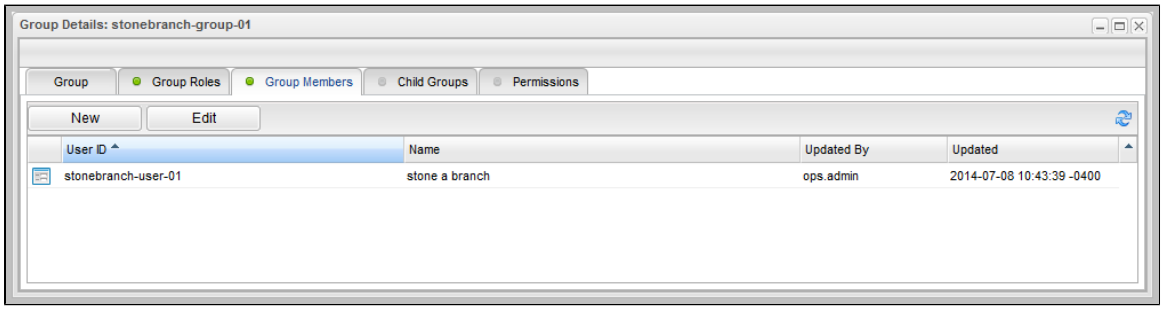
Field Name	Description
Details	This section contains detailed information about the group.
Name	Name of this group.
Parent	Name of this group's parent group, if any.
Description	Description of this group.
Manager	Universal Controller user that is the manager of this group.
Buttons	This section identifies the buttons displayed above and below the Group Details that let you perform various actions.
Save	Saves a new group record in the Controller database.
Update	Saves updates to the record.
New	Displays empty (except for default values) Details for creating a new group.
Delete	Deletes the current record.
Refresh	Refreshes any dynamic data displayed in the Details.
Close	For pop-up view only; closes the pop-up view of this group.
Tabs	This section identifies the tabs across the top of the Group Details that provide access to additional information about the user.
Group Roles	Allows you to assign roles to this group.
Group Members	Allows you to assign users to this group.
Child Groups	Allows you to assign other groups to this group.
Permissions	Allows you to assign permissions 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.

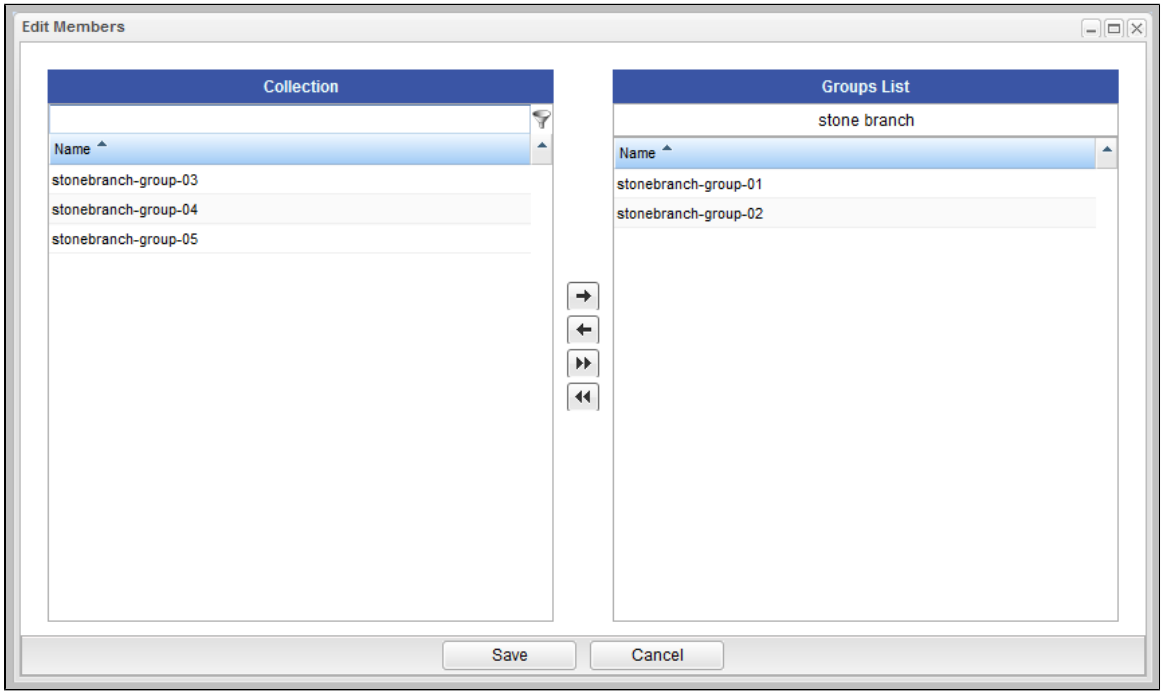
Assigning Users to Groups

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

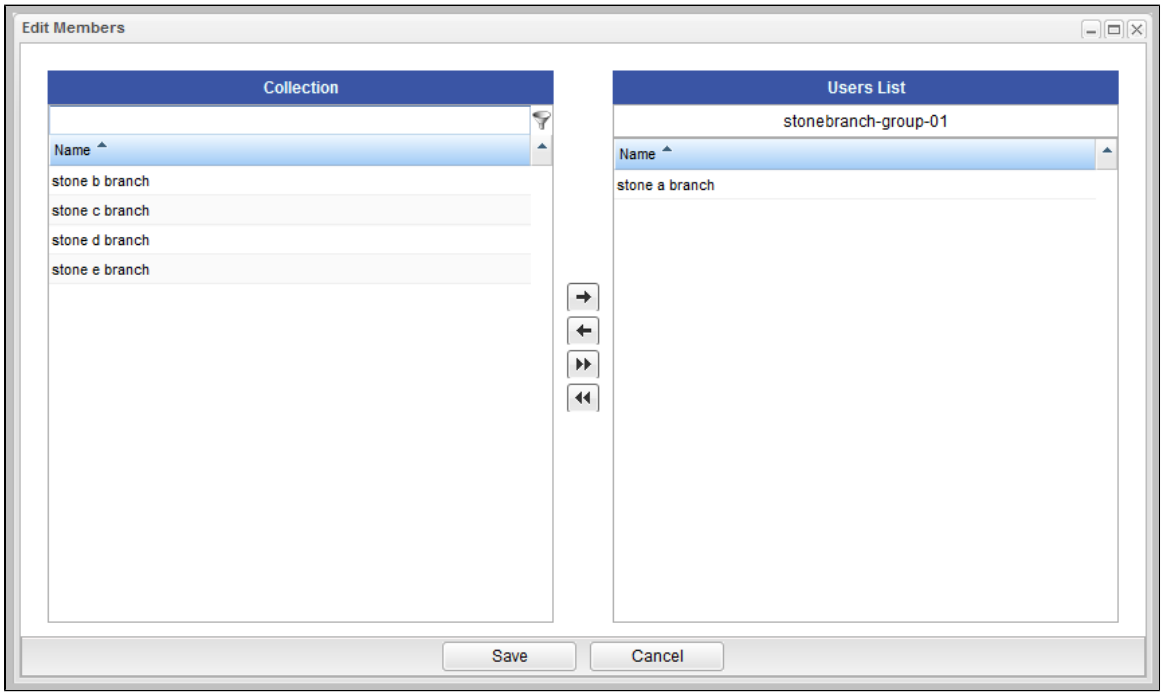
Step 3 For a User, either:

- 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.



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	To assign a User to a Group, move the User/Group from the **Collection** window to the **List** window: 1. To move a single entry, double-click it or click it once and then click the **>** arrow. 2. To move multiple entries, Ctrl-click them and then click the **>** arrow. 3. To move all entries, click the **>>** arrow. To unassign the User to a Group, move the User/Group from the **List** window to the **Collection** window: 1. To move a single entry, double-click it or click it once and then click the **<** arrow. 2. To move multiple entries, Ctrl-click them and then click the **<** arrow. 3. To move all entries, click the **<<** arrow.
Step 6	Click **Save**.

Roles and Permissions

Assigning Roles to Users or Groups

Roles control user access to administrative functions within Universal Controller. These functions include:

- Setting up security.
- Creating reports, filters, and gauges.
- Creating agent clusters.
- Creating and promoting bundles of records.

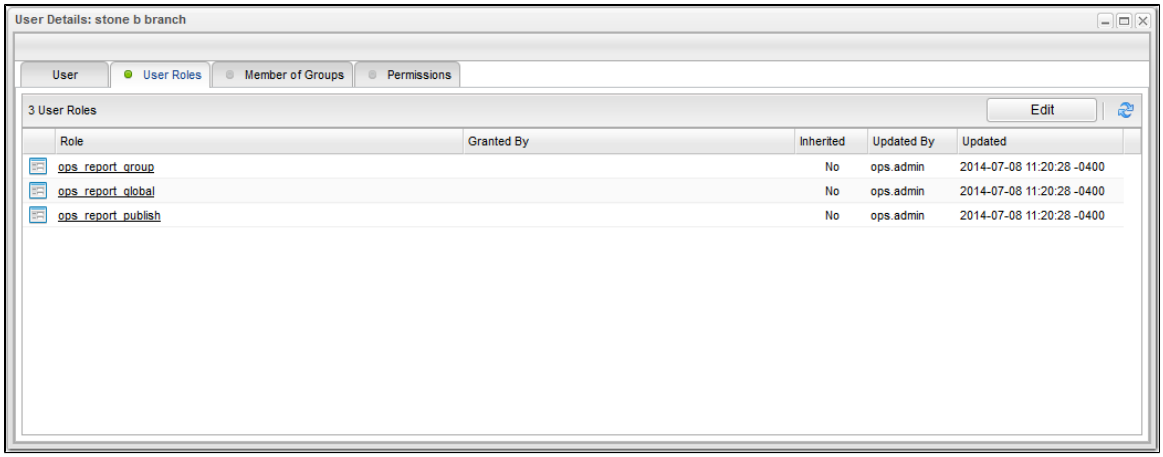
Each role is a predefined collection of administrative functions (see Description of Roles, below). By assigning a role to a user or group, you automatically give that user or group all functions associated with that role.

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

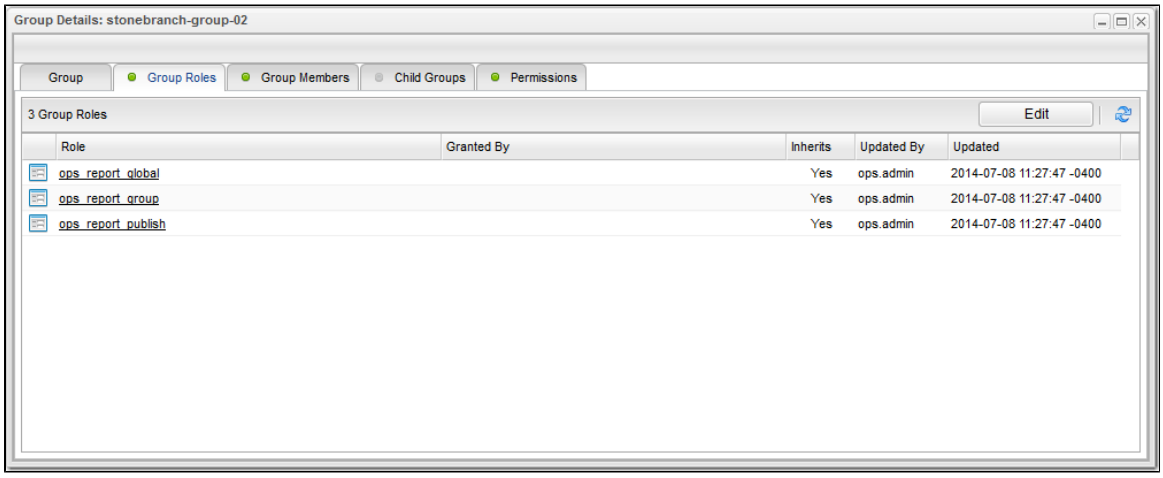
To assign roles to a user or group:

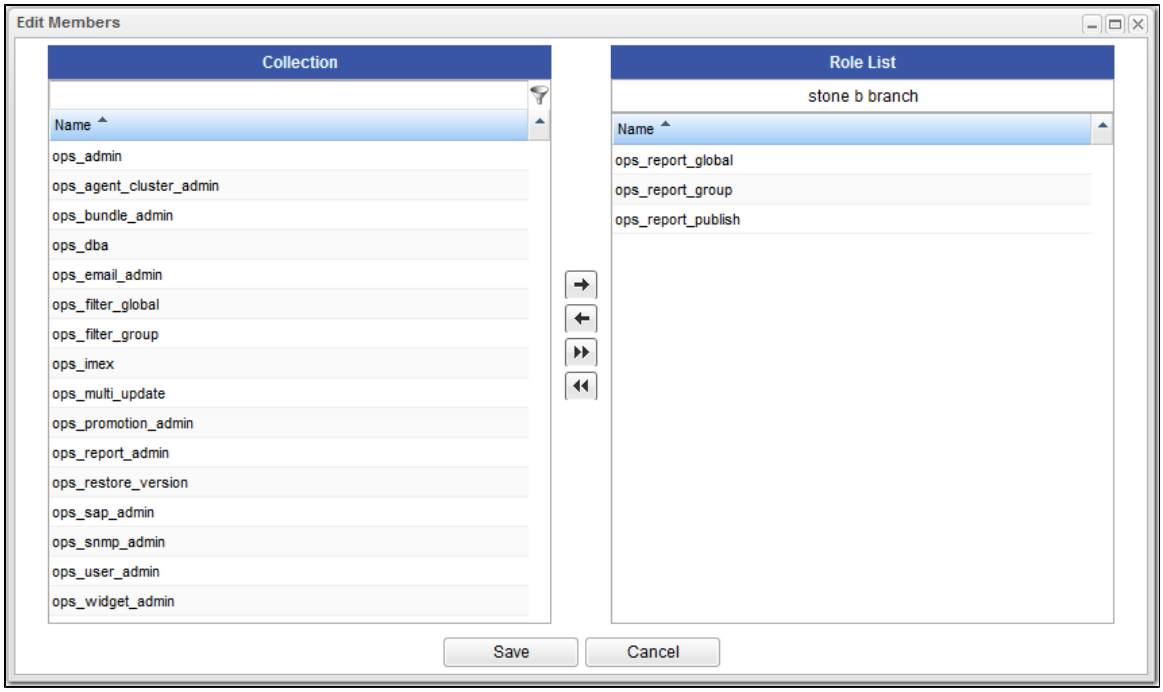
Step 1	Open a User or Group record.

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	To assign a Role to the User / Group, move the Role from the **Collection** window to the **Roles** window: 1. To move a single Role, double-click it or click it once and then click the **>** arrow. 2. To move multiple Roles, Ctrl-click them and then click the **>** arrow. 3. To move all Roles, click the **>>** arrow. To unassign a Role to the User / Group, move the Role from the **Roles** window to the **Collection** window: 1. To move a single Role, double-click it or click it once and then click the **<** arrow. 2. To move multiple Roles, Ctrl-click them and then click the **<** arrow. 3. To move all Roles, click the **<<** arrow.
Step 6	Click **Save**.

Description of Roles

The following table summarizes the roles available in the Controller.

Role Name	Available Functions	Contains Roles

ops_admin	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.	• ops_agent_cluster_admin • ops_bundle_admin • ops_dba • ops_email_admin • ops_filter_global • ops_filter_group • ops_imex • ops_multi_update • ops_promotion_admin • ops_report_admin • ops_restore_version • ops_sap_admin • ops_snmp_admin • ops_user_admin
ops_agent_cluster_admin	Create, update, and delete agent clusters.	
ops_bundle_admin	• Create, read, update, and delete Bundles. • View Promotion Targets, including agent mappings. • View Promotion History. • View a record's list of bundles. • View Promotion Schedules. • Add a record to a bundle. • Create bundles by date. • Generate a Bundle Report.	
ops_dba	Create, update, delete database connections.	
ops_email_admin	Create, update, delete email connections.	
ops_filter_global	Create global filters.	
ops_filter_group	Create filters that belong to a group of which this user is a member.	
ops_imex	List Import/Export XML.	
ops_multi_update	Update multiple records.	
ops_promotion_admin	• Create, read, update, and delete Creating Promotion Targets, including agent mappings. • View Bundles. • Refresh Target Agents. • Promote records. • Promote or schedule the promotion of a bundle. • Reschedule, cancel, and delete Promotion Schedules. • Generate a Bundle report. • Accept bundles being promoted to a target server. (The **Accept Bundle** command is executed on the target server automatically as part of the **Promote** and **Promote Bundle** commands and does not involve user interaction.)	
ops_report_admin	Create, update, and delete reports that are visible to Everyone or visible to all users within your Group(s), in addition to the roles granted by the ops_widget_admin role.	• ops_report_global • ops_report_group • ops_report_publish • ops_widget_admin
ops_report_global	Create global reports.	
ops_report_group	Create reports that belong to a group to which this user is a member.	
ops_report_publish	Publish reports.	
ops_restore_version	Restore old versions of records.	
ops_sap_admin	Create, update, and delete SAP Connections.	
ops_snmp_admin	Create, update, and delete SNMP Managers, to which the Controller sends SNMP notifications.	

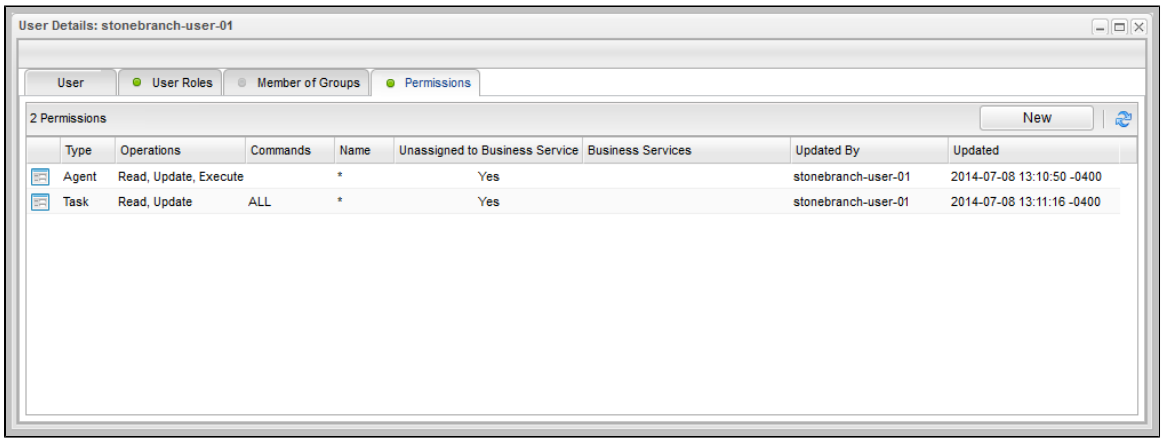
ops_user_admin	Create, update, and delete users and groups.	
ops_widget_admin	Create, update, and delete Widgets.	

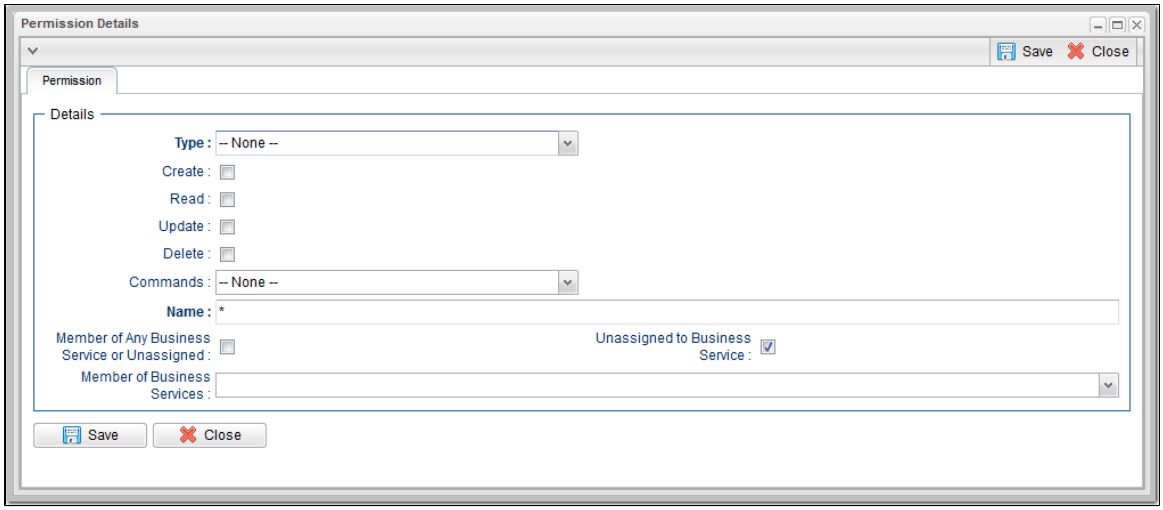
Assigning Permissions to Users or Groups

Permissions control user access to Controller records and the types of actions that can be taken on the records. Each permission record specifies a record type, such as task or trigger, and the type of action can be taken on that record type, 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:

Step 1	Open a User or Group record.
Step 2	Click the **Permissions** tab. A list of permissions assigned to the User / Group displays. For Example:  **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. 
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.

Types of Permissions

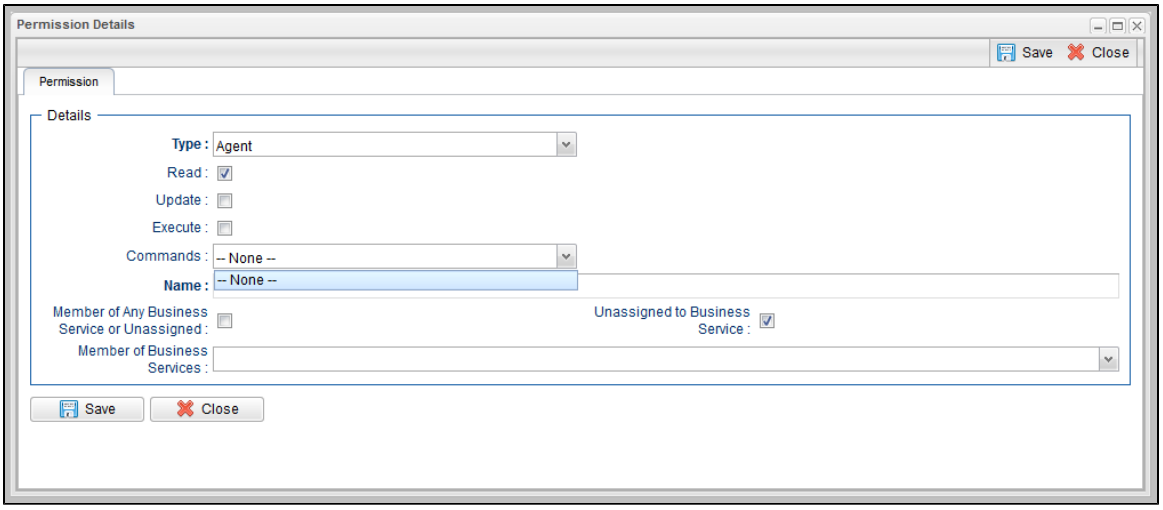
This section identifies the different types of permissions that you can add to a user or group.

General Permissions Field Descriptions

The following fields of information display in the Permissions Details for all Permission types:

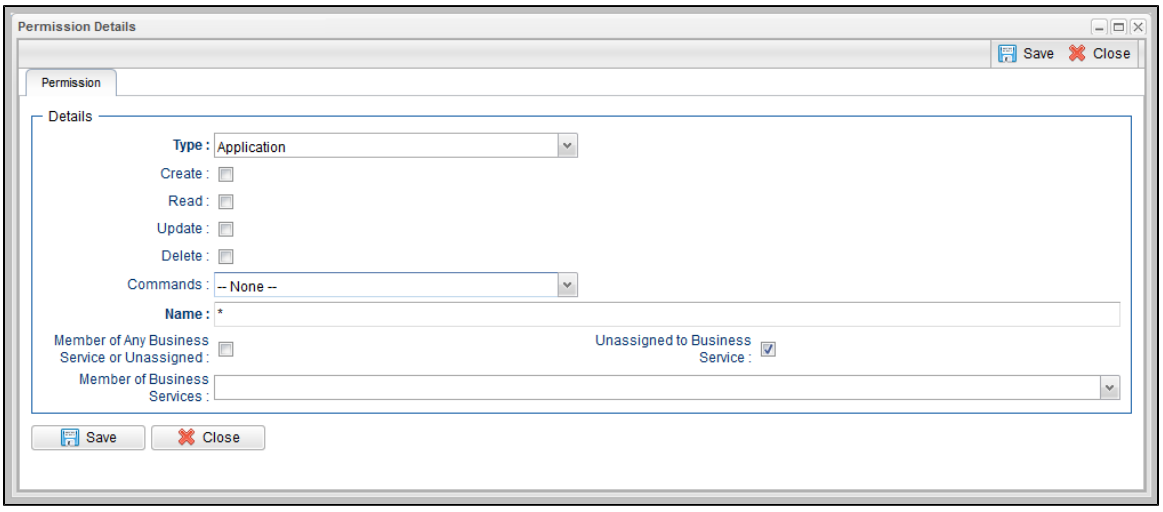
Field Name	Description
Name	Applies this permission to records whose name matches the string specified here. Wildcards are supported.
Member of Any Business Service or Unassigned	Applies this permission both to records that belong to any Business Service and to records that do not belong to any Business 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 Business Service(s). Click the lock icon to unlock the field and select Business Services.

Agent Permissions



Options	Description
Read	Grants permission to view an Agent definition. All users can view configured Agents in the Controller, so the **Read** check box always is checked.
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	• ALL: Grants permission to suspend and resume Agents. • Resume Agent: Grants permission to resume the ability of a suspended Agent to run tasks. • Suspend Agent: Grants permission to suspend the ability of an Agent to run tasks.

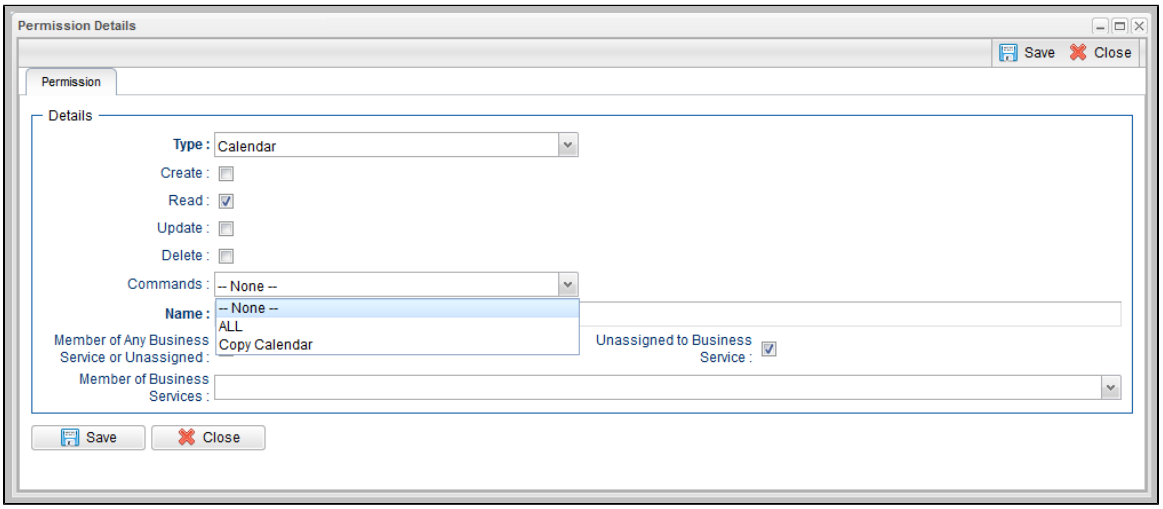
Application Permissions



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.

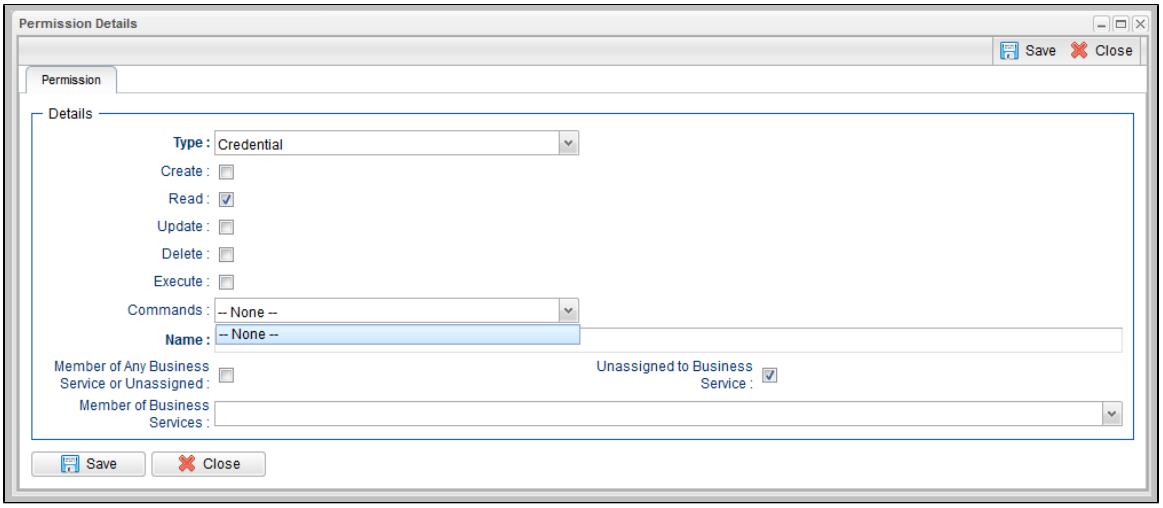
Commands	See Application Control Tasks for details. Options: • ALL: Grants permission to execute a Start, Stop, and Query from the Application resource screen. • Start: Grants permission to execute a Start from the Application resource screen. • Stop: Grants permission to execute a Stop from the Application resource screen. • Query: Grants permission to execute a Query from the Application resource screen.

Calendar Permissions



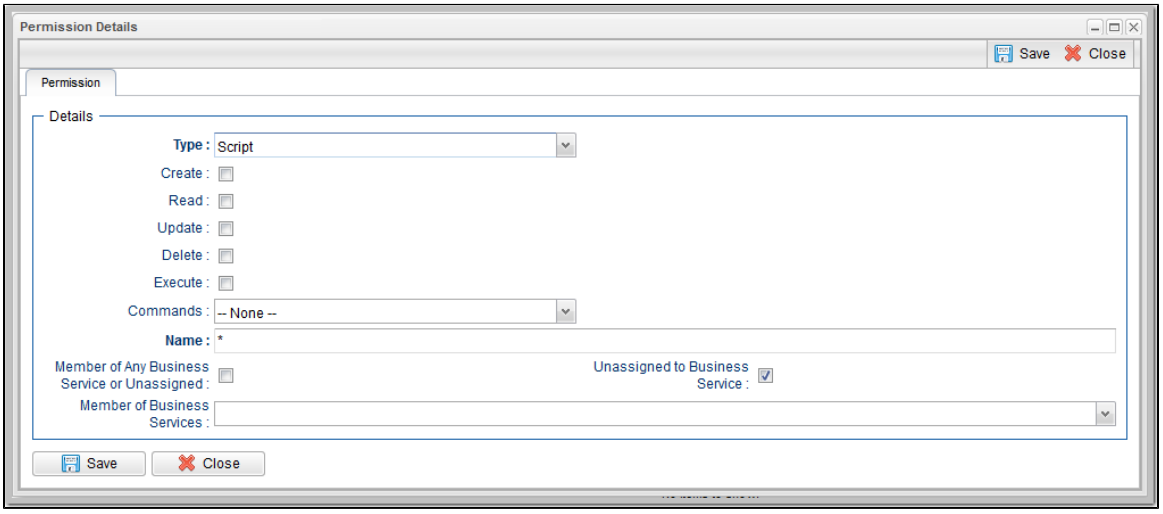
Options	Description
Create	Grants permission to create a new calendar.
Read	Grants permission to read a calendar. All users can view Calendars in the Controller, so the **Read** check box always appears checked.
Update	Grants permission to update a calendar.
Delete	Grants permission to delete a calendar.
Commands	• ALL: Grants permission to copy a calendar. • Copy Calendar: Grants permission to copy a calendar.

Credential Permissions



Options	Description
Create	Grants permission to create a new credential.
Read	Grants permission to read a credential. All users can view Credentials in the Controller, so the **Read** check box always appears checked.
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

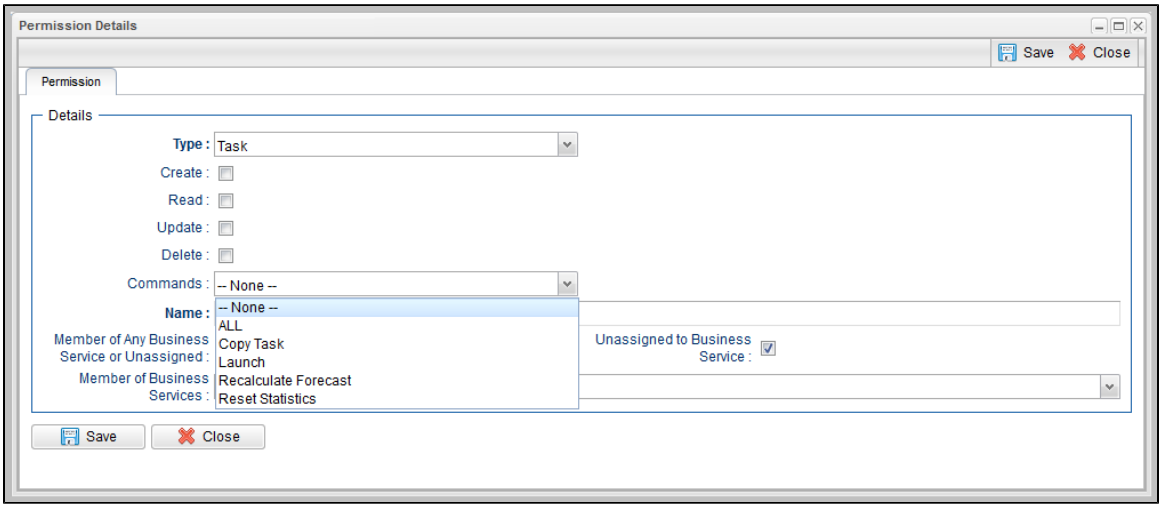
Script Permissions



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.

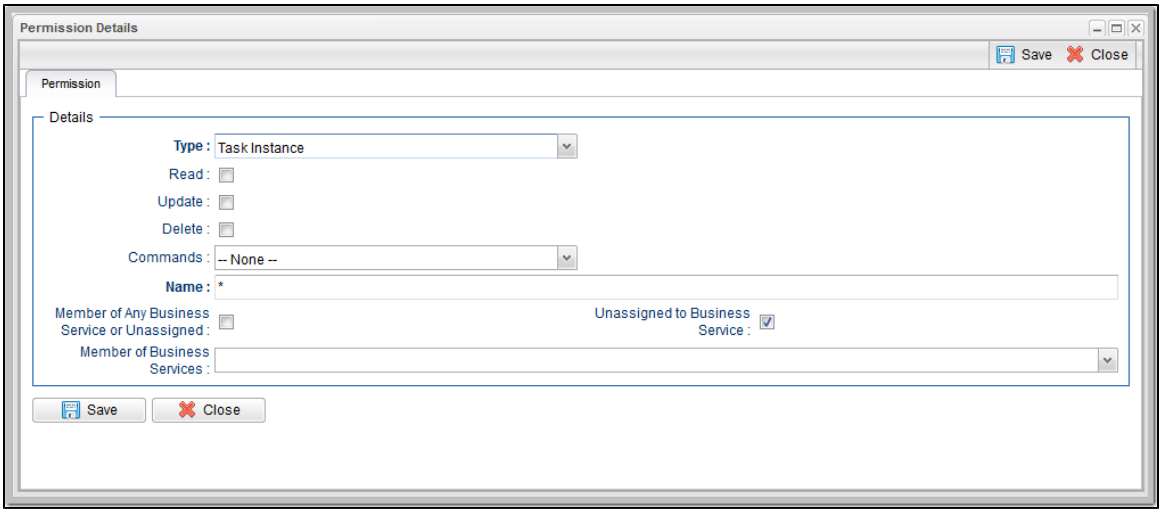
Execute	Grants permission to execute a script contained by a task.
Commands	n/a

Task Permissions



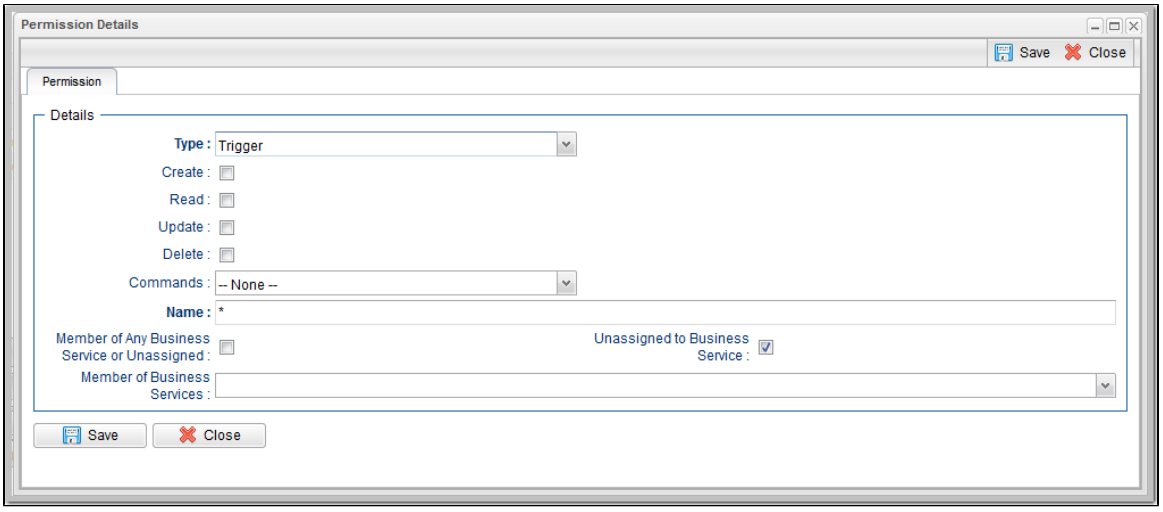
Options	Description
Create	Grants permission to create a new task.
Read	Grants permission to read a task.
Update	Grants permission to update a task.
Delete	Grants permission to delete a task.
Commands	• ALL: Grants permission to issue any command. • Copy Task: Grants permission to copy a task. • Launch: Grants permission to launch a task. • Recalculate Forecast: Grants permission to recalculate a forecast. • Reset Statistics: Grants permission to reset statistics, including statistics being tracked by each parent Workflow of a task. • Reset z/OS Override Statistics: Grants permission to reset z/OS override statistics.

Task Instance Permissions



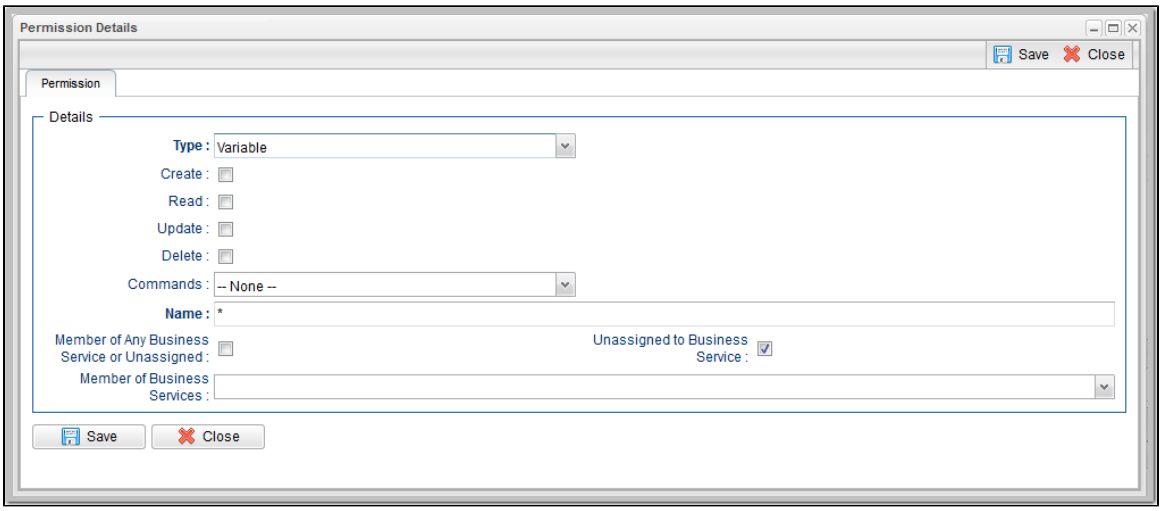
Options	Description
Create	Task instances are created automatically when the task launches, so the **Create** permission does not appear.
Read	Grants permission to read a task instance
Update	Grants permission to update certain fields on a task instance.
Delete	Grants permission to delete a task instance.
Commands	For command descriptions, see Manually Running and Controlling Tasks. • ALL: Grants permission to issue any command. • Cancel: Grants permission to cancel a Task Instance. • Clear All Dependencies: Grants permission to clear all dependencies on a Task Instance. • Clear Predecessors: Grants permission to clear all predecessors on a Task Instance. • Clear Exclusive: Grants permission to clear all mutual exclusive dependencies from a Task Instance. • Clear Resources: Grants permission to clear all resource dependencies of a Task Instance. • Force Finish: Grants permission to force finish a task instance. • Hold: Grants permission to put a Task Instance on hold. • Insert Task: Grants permission to insert a task on the workflow monitor of a workflow Task Instance. • Mark as Satisfied: Can mark a dependency as satisfied. • Re-run: Grants permission to re-run a Task Instance. • Release: Grants permission to release a Task Instance from hold. • z/OS Restart: Grants permission to restart a z/OS task from a specific step. • Release Recursive: Grants permission to release a workflow and all its tasks from hold. • Retrieve Output: Grants permission to execute the Retrieve Output button. • Set Priority Low: Grants permission to change the priority of a task to Low. • Set Priority Medium: Grants permission to change the priority of a task to Medium. • Set Priority High: Grants permission to change the priority of a task to High. • Set Completed: Grants permission to set a Manual Task Instance status to completed. • Set Started: Grants permission to set a Manual Task Instance status to a new started time. • Skip: Grants permission to skip a Task Instance. • Unskip: Grants permission to unskip a Task Instance selected to be skipped. **Note** Universal Controller will initially check for command permission specifically for the task instance. 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.

Trigger Permissions



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	• ALL: Grants permission to do all listed below. • Assign Execution User: Grants permission to override the execution user of task instances launched by a trigger. • Copy Trigger: Grants permission to copy a trigger. • Disable Trigger: Grants permission to disable a trigger. • Enable Trigger: Grants permission to enable a trigger. • Recalculate Forecast: Grants permission to recalculate a forecast. • Trigger Now: Grants permission to trigger (launch) a task.

Variable Permissions



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.

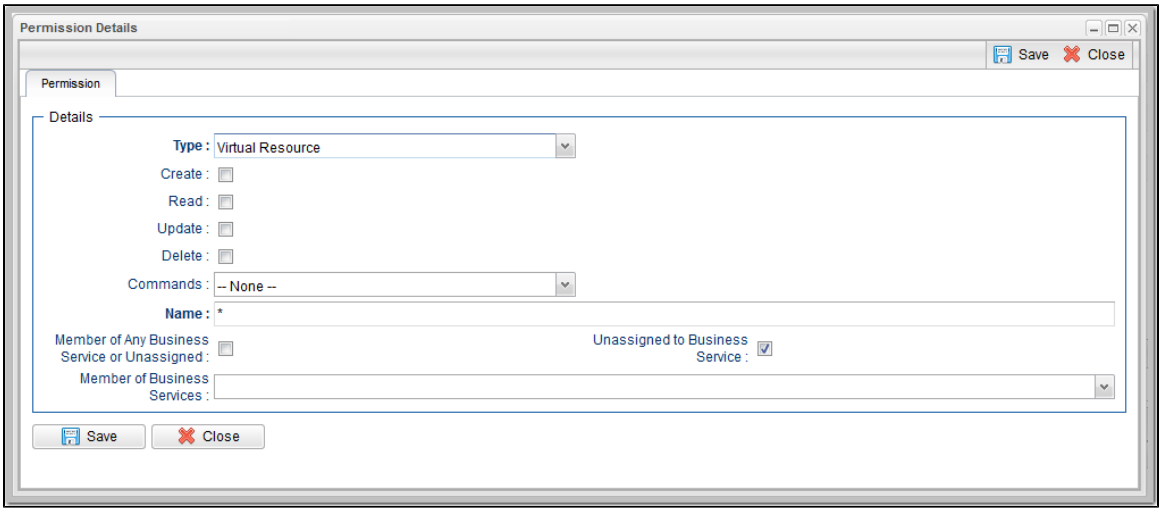
By default, enhanced global variable security is enabled; the Variable Security Enabled Universal Controller system property is set to **true**.

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



Options	Description
Create	Grants permission to create a virtual resource.
Read	Grants permission to read a virtual resource. All users can view virtual resources in the Controller, so the **Read** check box always appears checked.

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	n/a

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.

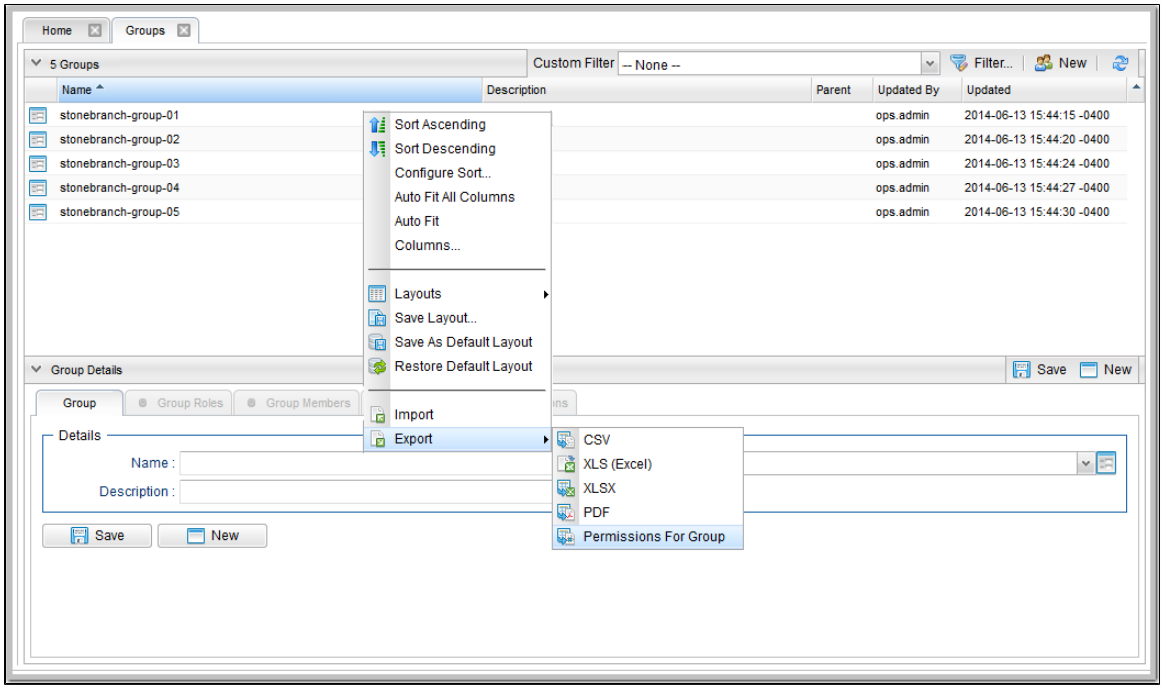
All defined Virtual Resource permissions will be enforced unless enhanced virtual resource security has been disabled by setting Virtual Resource Security Enabled to **false**. This allows all virtual resources to be managed and used by any valid Universal Controller user.

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 Administration navigation pane, select **Security > Groups**. The Groups list displays.
Step 2	As desired, filter 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

Credentials are the user ID and password under which an Agent runs tasks on the machine where the Agent resides.

Agent credentials are defined during installation, but via the 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 the ID and password:

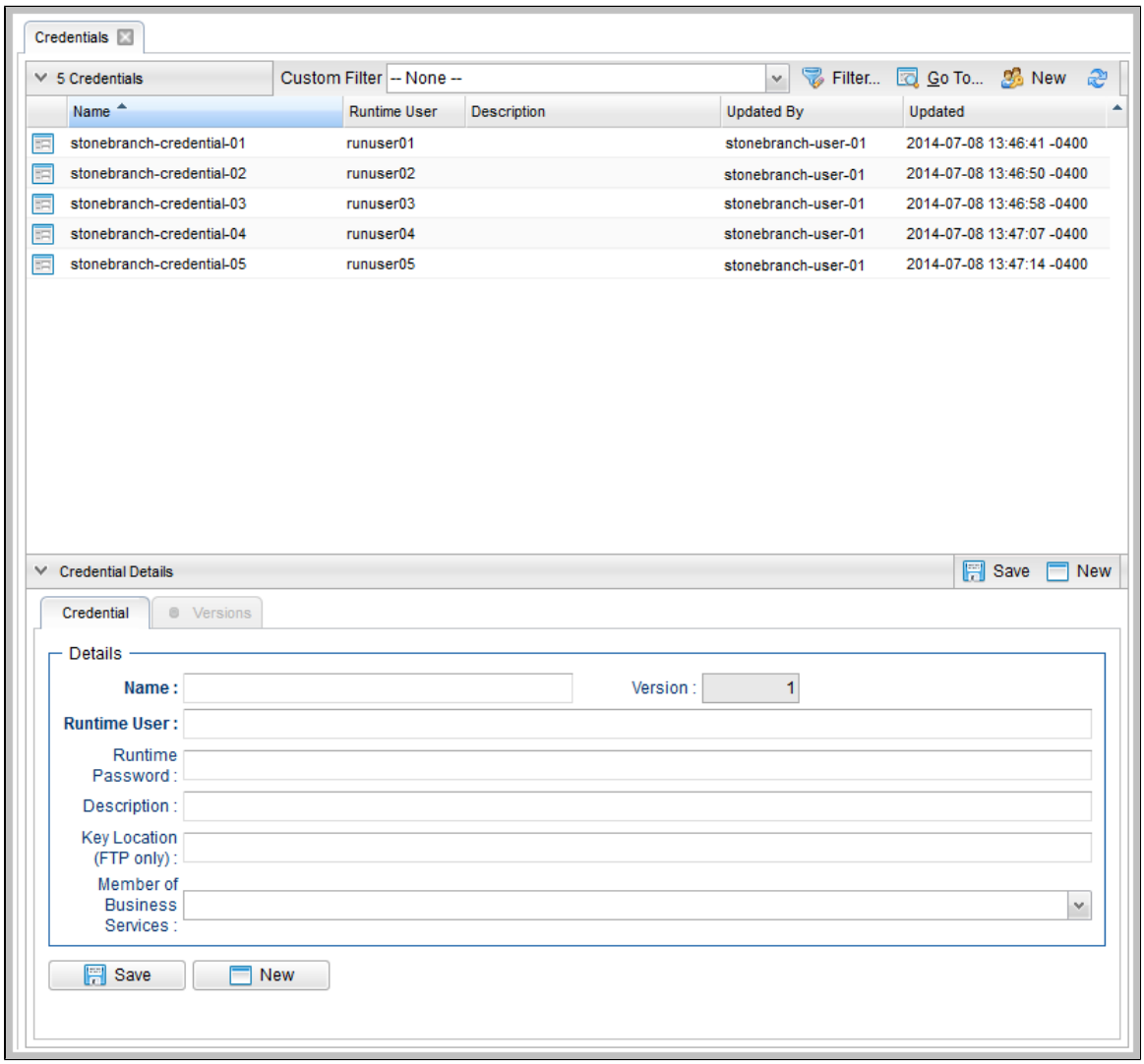
1. If the task provides credentials, the Agent uses those credentials.
2. If the task does not provide credentials, the Agent uses the credentials in its Agent Details record.
3. If the Agent resource definition does not provide credentials, the Agent uses the credentials defined at installation.

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.

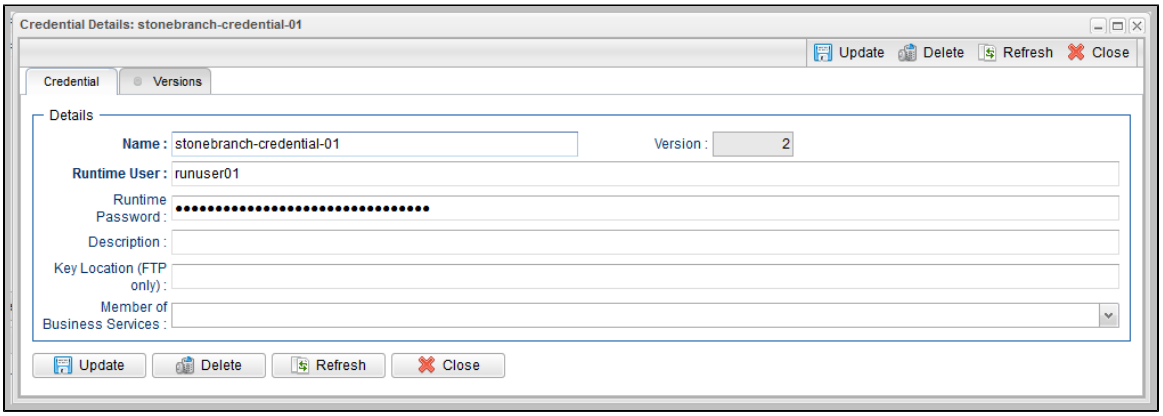
Step 3 Click the **Save** button. The credential is added to the database, and all buttons and tabs in the Credential Details are enabled.

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.



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 Versions tab to view previous versions. For details, see Record Versioning.
Runtime User	Runtime user ID, including an LDAP- or AD-formatted user ID, under which the job will be run.
Runtime Password	Runtime user's password.
Description	Description for this record.

Key Location (FTP only)	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. 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.
Member of Business Services	User-defined; allows you to select one or more Business Services that this record belongs to.
Buttons	This section identifies the buttons displayed above and below the Credential Details that let you perform various actions.
Save	Saves a new Credential record in the Controller database.
Update	Saves updates to the record.
New	Displays empty (except for default values) Details for defining a new credential.
Delete	Deletes the current record.
Refresh	Refreshes any dynamic data displayed in the Details.
Close	For pop-up view only; closes the pop-up view of this credential.
Tabs	This section identifies the tabs across the top of the Credential Details that provide access to additional information about the credential.
Versions	Stores copies of all previous versions of the current record. See Record Versioning.

Business Services

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.

You also can take advantage of Business Services when you set up security by assigning permissions only to users and/or user groups that belong to specific Business Services.

You also can promote Bundles that include records from one or more specific Business Services.

Business Service Usage

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

A Business Service of related records can be identified via:

- Permissions
- Reports
- Dashboard view
- Filtering

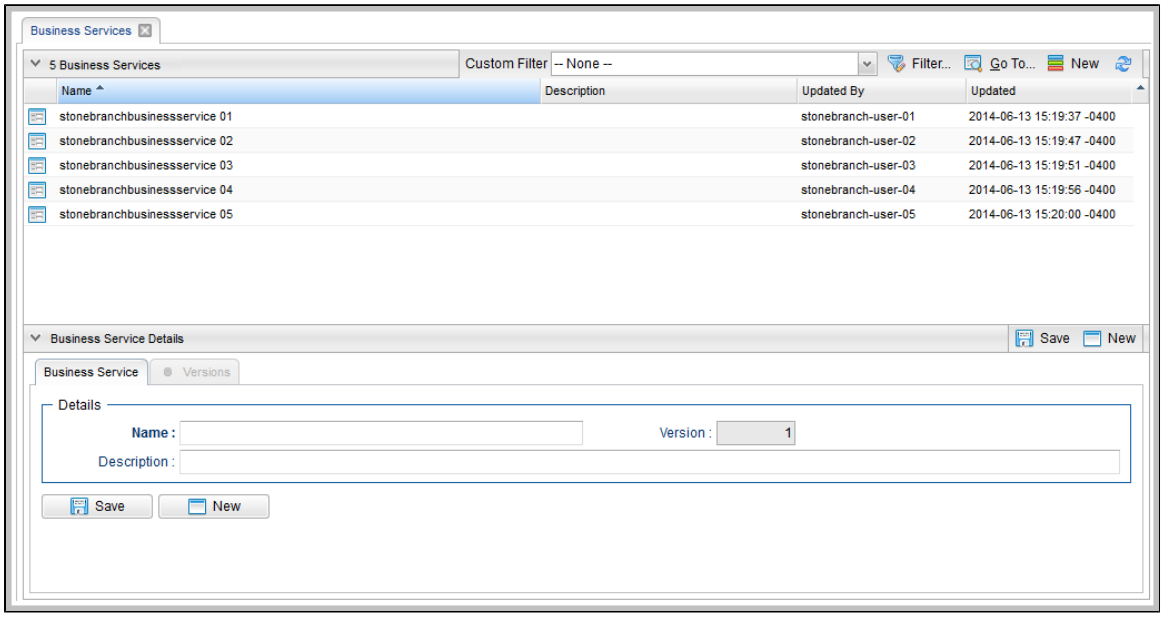
Record Types for Business Services

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

- Agents
- Applications
- Calendars
- Credentials
- Scripts
- Tasks
- Task Instances
- Triggers

Creating Business Services

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

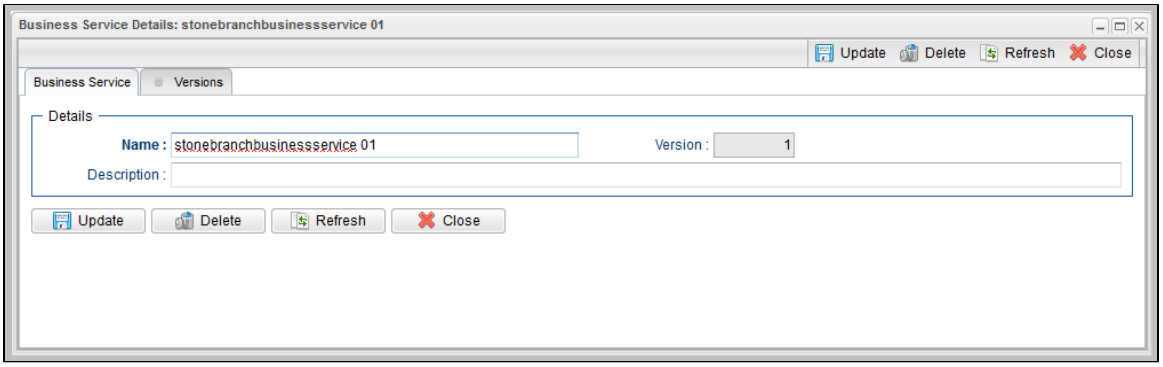
Step 1	From the Administration navigation pane, select **Security > Business Services**. The Business Services list displays. Below the list, Business Service Details for a new Business Service displays. 
Step 2	Enter/select Details for a new Business Service, using the field descriptions below as a 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 the **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).

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.



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 alphanumerics.
Version	System-supplied; version number of the current record, which is incremented by the Controller every time a user updates a record. Click the Versions tab to view previous versions. For details, see Record Versioning.
Description	User-defined: description of this record.
Buttons	This section identifies the buttons displayed above and below the Task Details that let you perform various actions.
Save	Saves a new task record in the Controller database.
Update	Saves updates to the record.
New	Displays empty (except for default values) Details for creating a new task.
Delete	Deletes the current record.
Refresh	Refreshes any dynamic data displayed in the Details.
Close	For pop-up view only; closes the pop-up view of this task.
Tabs	This section identifies the tabs across the top of the Task Details that provide access to additional information about the task.
Versions	Stores copies of all previous versions of the current record. See Record Versioning.

Assigning a Record to One or More Business Services

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.

Business Service Membership Considerations for Create, Update, and Delete

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.

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 only needs 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.

Audits

Overview

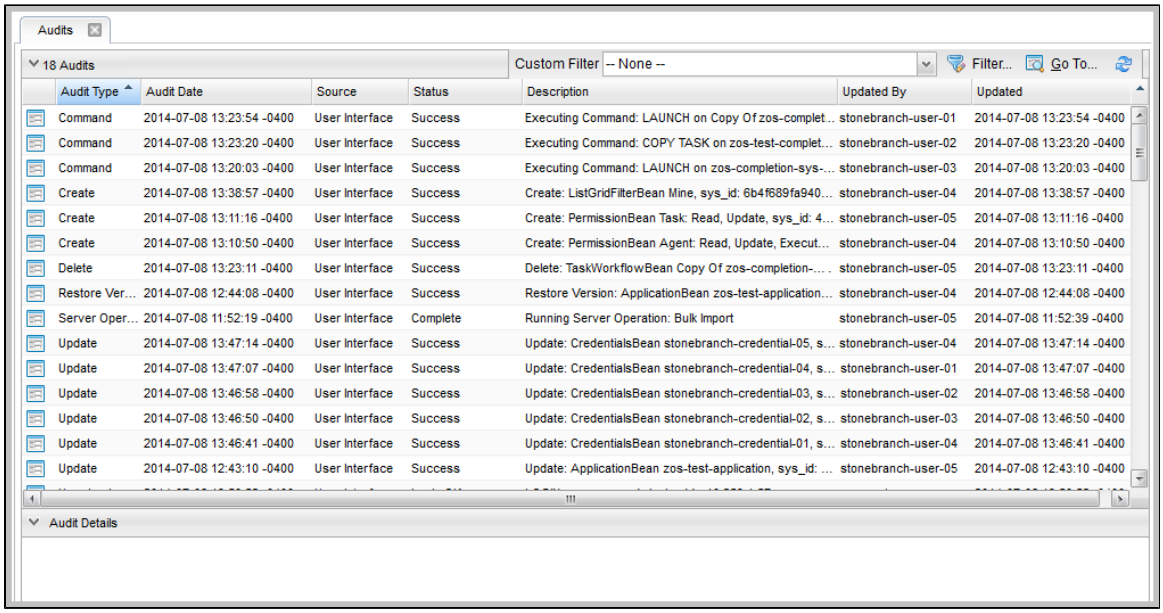
Audits are detailed records of all user interactions with the Controller, including before and after information related to any change and a description of the difference.

Audits are created when the user performs any of the following actions:

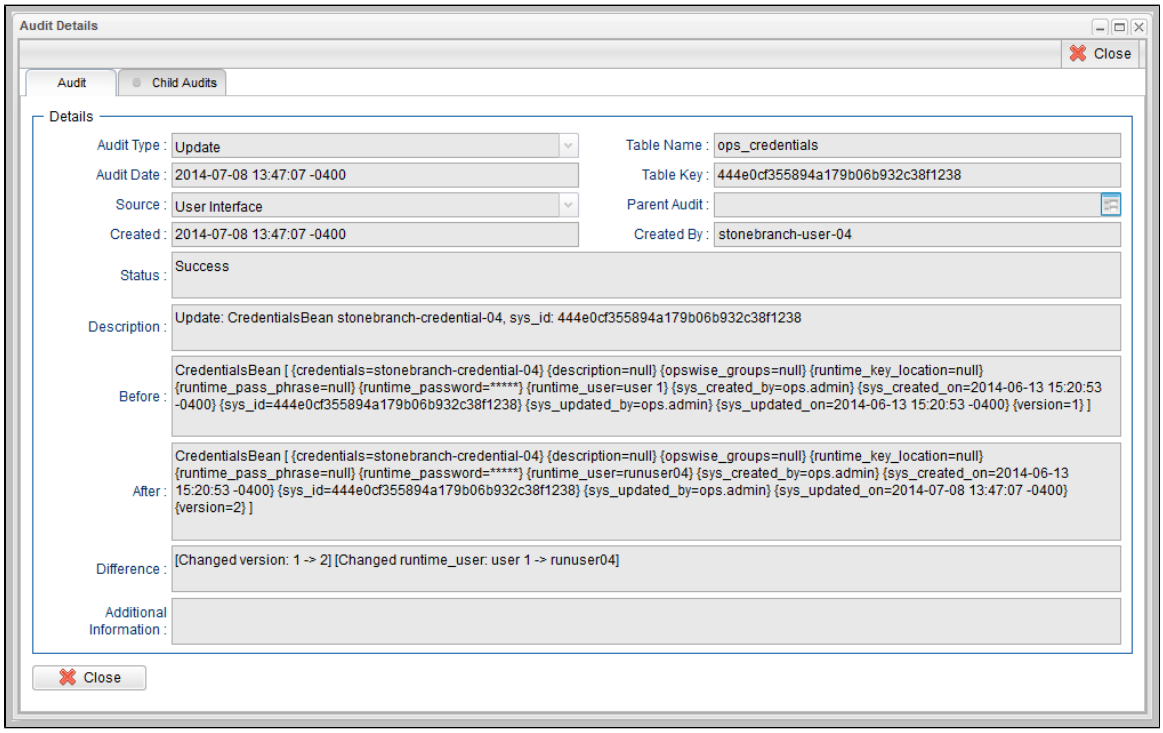
- Logging actions: log in, log out, or login failure.
- Creates, updates, or deletes a record.
- Issues an action or command (for example, Launch Task or Trigger Now).
- Imports or exports records on a list.

Displaying Audits

Step 1 From the Administration navigation pane, select **Security > Audits**. The Audits list displays audit activity for the last seven days.



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 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: • CLI • Create • Command • Delete • Delete Override File • Delete Version • Export • Import • Restore Version • Server Operation • Update • User Login • z/OS Auto-Restart
Table Name	Name of the table for which the user interaction was performed.
Audit Date	Date when this audit was created.
Table Key	Encrypted key to the table for which the user interaction was performed.

Source	Location of the user interaction. Options: • Agent Message • Command Line • Scheduled • Set Variable Action • Task Instance • User Interface • Web Service
Parent Audit	Parent audit for which this audit was created automatically.
Created	Date when this audit was created.
Created By	User that created this audit.
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.
Tabs	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.