



Opwise Controller 5.2.0

Security

© 2014 by Stonebranch, Inc. All Rights Reserved.

1. Security	3
1.1 Opwise Controller Security	4
1.2 Security Overview	5
1.3 Users and Groups	6
1.4 Roles and Permissions	10
1.5 Credentials	21
1.6 LDAP Security	23
1.7 Audits	25

Security

Opswise Controller Security



Setting Up Security

[Overview](#)

[Adding Users](#)

[Adding Groups](#)

[Assigning Roles to Users or Groups](#)

[Assigning Permissions to Users or Groups](#)

[Exporting Opswise Permissions for a Group](#)

[Login Credentials](#)

[LDAP Security](#)



Audits

[Viewing Audits](#)



The information on these pages also is located in the [Opswise Controller 5.2.0 Security.pdf](#).

Security Overview

Opswise Controller Security

Setting up Opswise 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.
- Setting up the Controller to use [LDAP](#) authentication.

Users and Groups

- Default Users and Groups
- Adding Users
 - User Definition Screen Field Descriptions
- Adding Groups
 - Field Descriptions
- Assigning Users to Groups

Default Users and Groups

The default user, **ops.admin**, has full permission on all Opwise Controller system features.

Two default user groups also are provided:

- **Administrator Group** has access to everything within the Controller.
- **Everything Group** has access to everything except user and group administration.

Adding Users



Note

You must have administrative privileges to add users.

By default, a new user has no permissions. Until permissions are granted, a user can log into the Opwise Controller user interface and view options in the navigation pane, but cannot perform any tasks.

Step 1 From the navigation pane, select **Automation Center Administration > Security > Users**. The Users list screen displays.

User ID	Name	Locked out	Created
jmlaprise	Jeremy Laprise	false	2013-07-29 11:33:44 -0700
ops.admin	Administrator	false	2008-08-20 08:31:25 -0700

Step 2 Click **New**. The User definition screen displays.

User ID: Time zone: System (US/Pacific)

First name: Business phone:

Last name: Mobile phone:

Title:

Password:

Password needs reset:

Web Browser access: -- System Default --

Command Line access: -- System Default --

Web Service access: -- System Default --

Locked out:

Activated account:

Step 3 Using the field descriptions provided below, fill in the fields.

Step 4	Access the Action menu and click Save to save the record.
Step 5	Optionally, assign one or more roles to the group, assign the user to a group, or assign permissions to this user.
Step 6	Click Submit to save the updated record.

User Definition Screen Field Descriptions

Field Name	Description
User ID	Log in ID for this user.
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.
First name	User's first name.
Business phone	User's business phone number.
Last name	User's last name.
Mobile phone	User's mobile phone number.
Title	User's title.
Password	User's password.
Password needs reset	If enabled, the user will be prompted to reset the password at first login.
Web Browser access	Specifies whether or not the user can log in to the user interface. Options: <ul style="list-style-type: none"> 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 Opwise 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 Opwise Command Line Interface (CLI) . Options: <ul style="list-style-type: none"> 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 Opwise 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 Opwise RESTful Web Services API . Options: <ul style="list-style-type: none"> System Default - User restriction for logging in to the Opwise Web Services is based on the current system default value of the System Default Web Service Access Opwise Controller system property. Yes - User is not restricted from logging in to the Opwise Web Services. No - User is restricted from logging in to the Opwise Web Services.
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.
Activated account	If enabled, the user ID is active and the user can log in. If disabled, the user is permanently deactivated; it will not appear in user lists and cannot be used for access to the Controller.
Submit button	Submits the new record to the database.
Update button	Saves updates to the record.
Delete button	Deletes the record from the database.

User Roles tab	Allows you to assign roles to this user.
Group Members tab	Allows you to assign this user to one or more groups .
Opwise Permissions tab	Allows you to assign permissions to this user.

Adding Groups

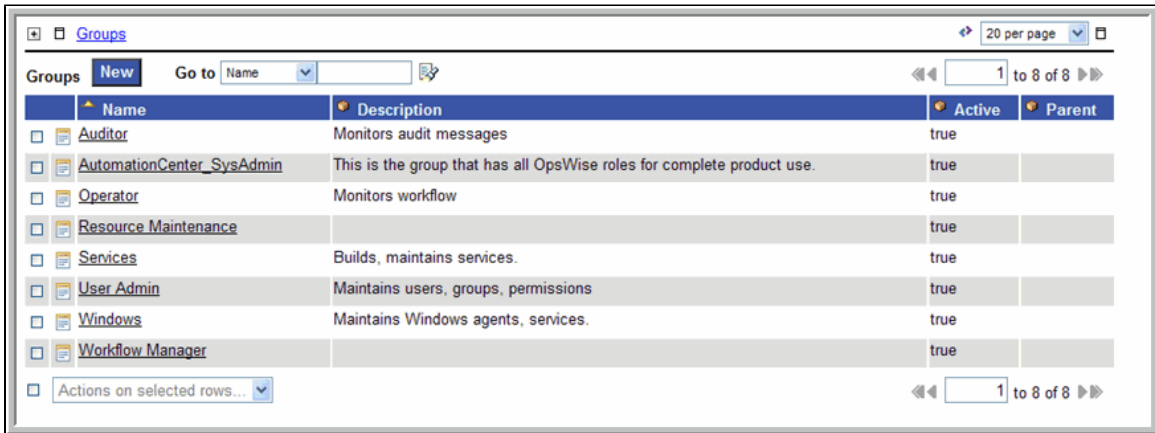


Note

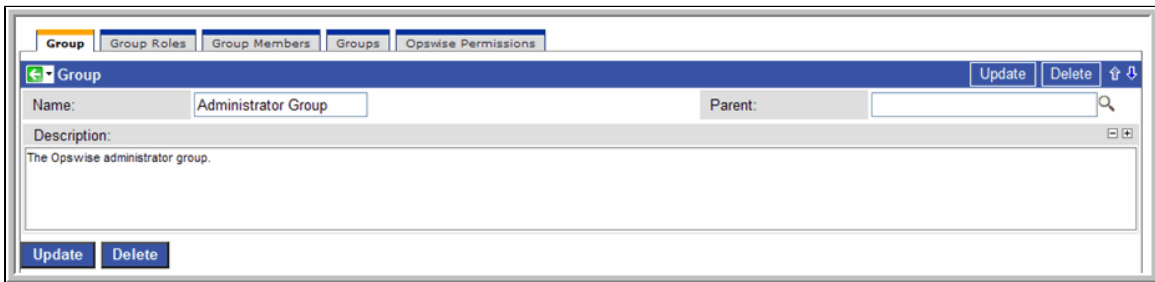
You must have administrative privileges to add groups.

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

Step 1 From the navigation pane, select **Automation Center Administration > Security > Groups**. The Groups list screen displays.



Step 2 Click **New**. The Group definition screen displays.



Step 3 Using the field descriptions provided below, fill in the fields.

Step 4 Access the [Action menu](#) and click **Save** to save the record.

Step 5 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 6 Click **Submit** to save the updated record.

Field Descriptions

Field Name	Description
Name	Name of this group.
Parent	Name of this group's parent group, if any.

Description	Description of this group.
Submit button	Submits the new record to the database.
Update button	Saves updates to the record.
Delete button	Deletes the record from the database.
Group Roles tab	Allows you to assign roles to this group.
Group Members tab	Allows you to assign users to this group.
Groups tab	Allows you to assign other groups to this group.
Opswise Permissions tab	Allows you to assign permissions to this group.

Assigning Users to Groups

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

Step 1	Open the User or Group record.
Step 2	Click the Group Members tab. This tab allows you to assign a user to one or more groups, or assign a group to one or more users. You can also add a new user or group record using this procedure.
Step 3	To add a new user or group: <ol style="list-style-type: none"> 1. Click New. A new user or new group screen displays. 2. Fill in the field using the field descriptions for groups or users as guidance. 3. Click Submit to save the new record. The record is added and assigned, and you are returned to the Group Members tab.
Step 4	To add an existing record to this user or group: <ol style="list-style-type: none"> 1. Click the Edit button. The Edit Members screen displays. 2. To add a user to this group or add a group to this user, click on the record in the Collection list and click Add. To remove a record, click on the record list and click Remove. 3. Click Save to save your choices.

Roles and Permissions

- Assigning Roles to Users or Groups
 - Description of Roles
- Assigning Permissions to Users or Groups
- Types of Permissions
 - General Permissions Field Descriptions
 - Agent Permissions
 - Application Permissions
 - Calendar Permissions
 - Credential Permissions
 - Script Permissions
 - Task Permissions
 - Task Instance Permissions
 - Trigger Permissions
 - Variable Permissions
 - Virtual Resource Permissions
- Exporting Opwise Permissions for a Group

Assigning Roles to Users or Groups

Roles control user access to administrative functions within Opwise 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.

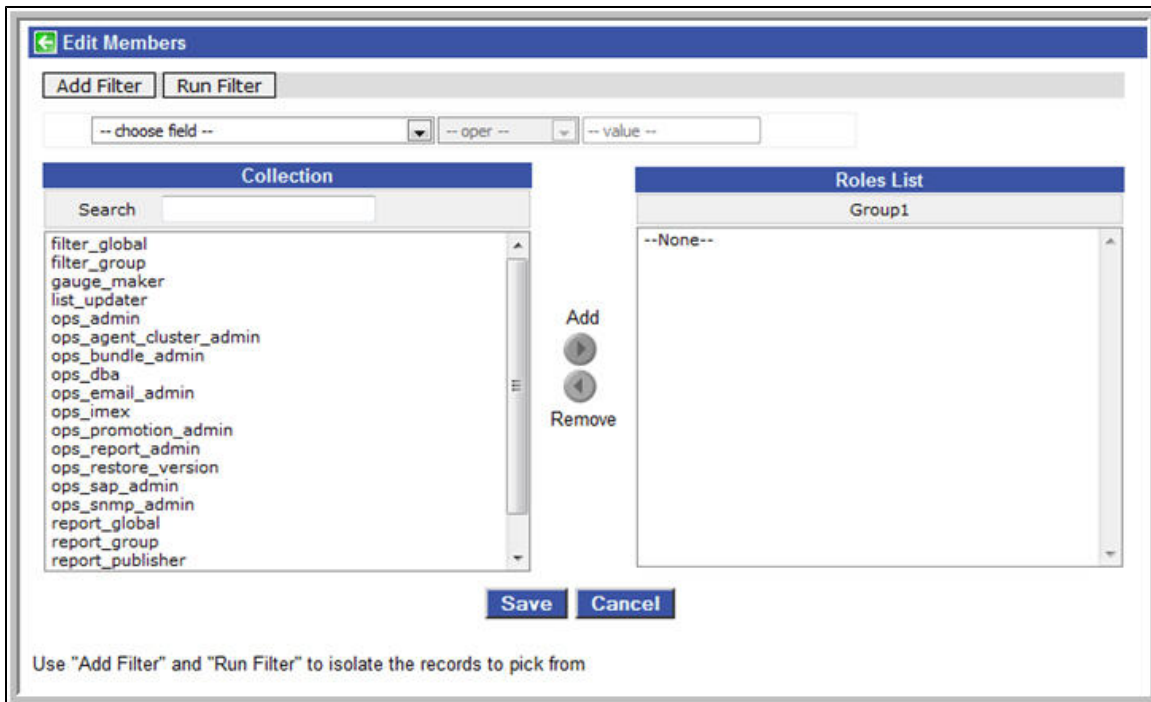
**Note**

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 From a User or Group screen, click the **User Roles** or **Group Roles** tab.

Step 2 Click the **Edit** button. The Edit Members screen displays.



Step 3 To add roles to this user or group, click on the roles in the Collection list and click **Add**. To remove roles, click on the roles in the Role list and click **Remove**.

Step 4 Click **Save** to save your choices.

Description of Roles

The following table summarizes the roles available in the Controller.

Role Name	Description	Contains Roles
filter_global	Can create global filters.	
filter_group	Can create filters that belong to a group of which this user is a member.	
gauge_maker	Can create gauges.	
list_updater	Can use Update Entire List and Update Selected menu options on lists.	
ops_admin	The Controller administrator role, which has permission on all Controller features. The easiest way to grant Administration privileges to a user is to add the user to the Administrator Group.	<ul style="list-style-type: none"> • filter_global • filter_group • list_updater • ops_agent_cluster_admin • ops_bundle_admin • ops_dba • ops_email_admin • ops_imex • ops_promotion_admin • ops_report_admin • ops_restore_version • ops_sap_admin • ops_snmp_admin • user_admin
ops_agent_cluster_admin	Can create, update, and delete agent clusters .	

ops_bundle_admin	<ul style="list-style-type: none"> • Can create, read, update, and delete Bundles. • Can view Promotion Targets, including agent mappings. • Can view Promotion History. • Can view a record's list of bundles. • Can add a record to a bundle. • Can create bundles by date. • Can generate a Bundle Report. 	
ops_dba	Can create, update, delete database connections .	
ops_email_admin	Can create, update, delete email connections .	
ops_imex	Can import/export records .	
ops_promotion_admin	<ul style="list-style-type: none"> • Can create, read, update, and delete Promotion Targets, including agent mappings. • Can view Bundles. • Can refresh Target Agents. • Can promote records. • Can promote Bundles. • Can generate a Bundle report. • Can 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	Can create, update, and delete reports .	<ul style="list-style-type: none"> • gauge_maker • report_global • report_group • report_publisher • report_scheduler
ops_restore_version	Can restore old versions of records.	
ops_sap_admin	Can create, update, and delete SAP Connections .	
ops_snmp_admin	Can create, update, and delete SNMP notifications .	
report_global	Can create global reports .	
report_group	Can create reports that belong to a group to which I am a member.	
report_publisher	Can publish reports .	
report_scheduler	Can schedule reports .	
user_admin	Can add, update, and delete users and groups .	

Assigning Permissions to Users or Groups

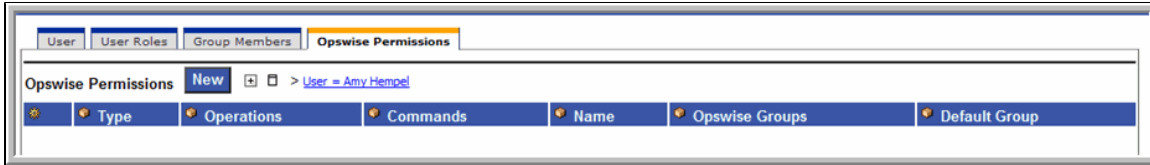
Permissions control user access to Controller records and the types of actions can be taken on the records. Each permission record specifies a record type, such as task or trigger, and the type of action can be taken on that record type, such as "create" or "delete."

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.

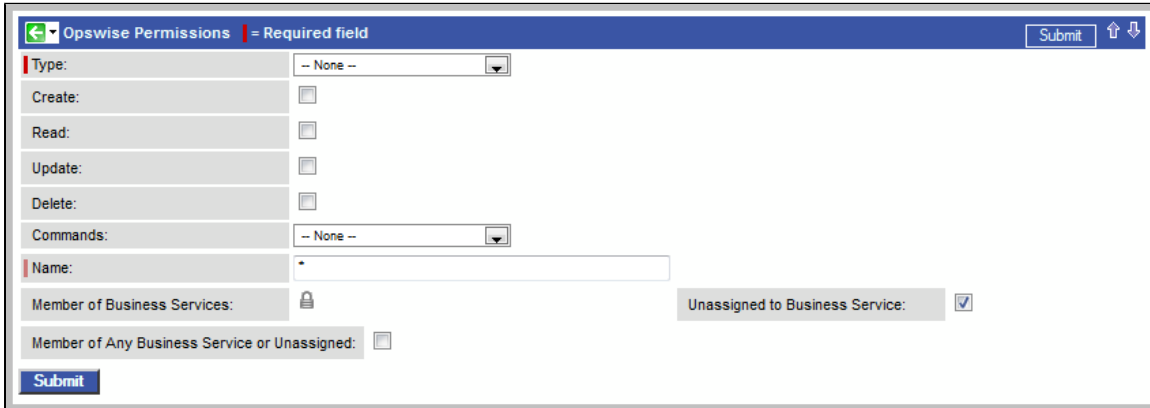
To add permissions to a user or group:

Step 1	Open the user or group to which you want to add permission.
---------------	---

Step 2 Click the **Permissions** tab:



Step 3 Click **New** to open the Permissions screen.



Step 4 Select permissions for the selected user or group.

The permissions available differ depending on what you select in the Type field. 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.

Certain permissions 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 on the Permissions screen 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 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 .
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 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.

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	<ul style="list-style-type: none"> • 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	<p>See Application Control Tasks for details. Options:</p> <ul style="list-style-type: none"> • 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

The screenshot shows the 'Opwise Permissions' configuration interface. The 'Type' is set to 'Calendar'. The 'Read' checkbox is checked. The 'Commands' dropdown is open, showing options: -- None --, -- None --, ALL, and Copy Calendar. The 'Unassigned to Business Service' checkbox is also checked.

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	<ul style="list-style-type: none"> • ALL: Grants permission to copy a calendar. • Copy Calendar: Grants permission to copy a calendar.

Credential Permissions

The screenshot shows the 'Opwise Permissions' configuration interface for a 'Credential' type. The 'Read' checkbox is checked. The 'Commands' dropdown is open, showing options: -- None -- and -- None --. The 'Unassigned to Business Service' checkbox is also checked.

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

The screenshot shows the 'Opwise Permissions' configuration interface for a 'Script'. The 'Type' is set to 'Script'. The 'Commands' dropdown is set to 'None'. There are checkboxes for 'Create', 'Read', 'Update', 'Delete', and 'Execute', all of which are currently unchecked. The 'Name' field is empty. There is a checkbox for 'Member of Business Services' which is checked, and a checkbox for 'Member of Any Business Service or Unassigned' which is unchecked. A 'Submit' button is located at the bottom left.

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 task containing a script.
Commands	n/a

Task Permissions

The screenshot shows the 'Opwise Permissions' configuration interface for a 'Task'. The 'Type' is set to 'Task'. The 'Commands' dropdown is open, showing options: 'None', 'ALL', 'Copy Task', 'Launch', 'Recalculate Forecast', and 'Reset Statistics'. There are checkboxes for 'Create', 'Read', 'Update', and 'Delete', all of which are currently unchecked. The 'Name' field is empty. There is a checkbox for 'Member of Business Services' which is checked, and a checkbox for 'Member of Any Business Service or Unassigned' which is unchecked. A 'Submit' button is located at the bottom left.

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	<ul style="list-style-type: none"> • 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.
----------	---

Task Instance Permissions

The screenshot shows the 'Opwise Permissions' configuration window. The 'Type' is set to 'Task Instance'. The 'Name' dropdown is open, displaying a list of commands. The 'Unassigned to Business Service' checkbox is checked. The 'Submit' button is visible at the bottom left.

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	<p>For command descriptions, see Manually Running and Controlling Tasks.</p> <ul style="list-style-type: none"> • 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.

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	<ul style="list-style-type: none"> • ALL: Grants permission to do all listed below. • 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

By default, enhanced global variable security is disabled; all global variables can be managed and used by any valid Opwise user.

Any defined Variable permissions will not be enforced until enhanced global variable security has been enabled (see [Enabling Enhanced Variable Security](#), below).

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 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.

To enable enhanced global variable security, you must set the [Variable Security Enabled](#) Opswise Controller system property to **true**.

Once enabled, global variable access will be controlled as follows:

- Users with the `ops_admin` role will continue to have full access to all global variables.
- Users with the `ops_promotion_admin` role will continue to 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.

Virtual Resource Permissions

By default, enhanced virtual resource security is disabled; all virtual resources can be managed and used by any valid Opswise user.

Any defined Virtual Resource permissions will not be enforced until enhanced virtual resource security has been enabled (see [Enabling Enhanced Virtual Resource Security](#), below).

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.

To enable enhanced virtual resource security, you must set the [Virtual Resource Security Enabled](#) Opswise Controller system property to **true**.

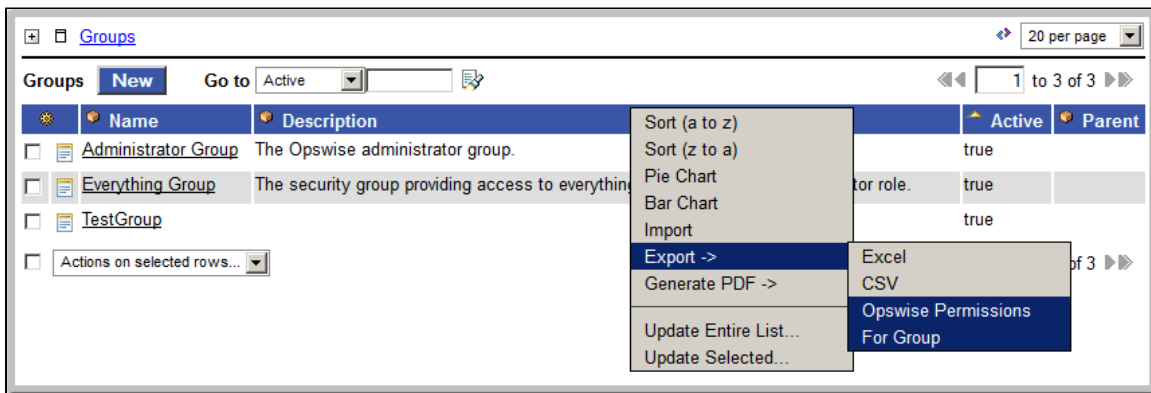
Once enabled, virtual resource access will be controlled as follows:

- All users will maintain **Read** access to virtual resources.
- Users with the [ops_admin](#) role will continue to 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.

Exporting Opswise Permissions for a Group

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

- Step 1** From the navigation pane, select **Automation Center Administration > Security > Groups**. The Groups List screen displays.
- Step 2** Use the filter to define the group(s) whose permissions you want to export (see [Sorting and Filtering](#)). When you perform the export, all groups matching the filter will be exported, even if they appear on a subsequent page.
- Step 3** Access the [Action menu](#) and select **Export -> > Opswise Permissions For Group**.



To export or import the **Opswise Permissions For Group XML**, you must have both the [ops_imex](#) and [ops_admin](#) roles.

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

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

Credentials

- [Overview](#)
- [Defining Credentials](#)
- [Credentials Definition Field Descriptions](#)

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.

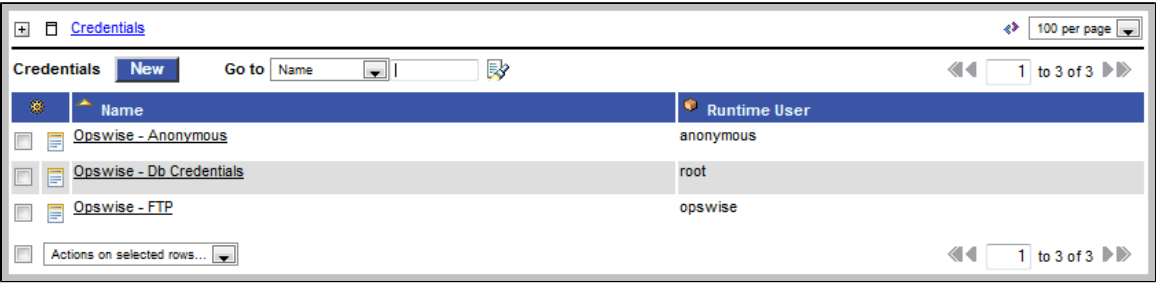
When prompted for credentials, the Agent looks in the following locations, in this order, for the ID and password:

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 resource definition.
3. If the Agent resource definition does not provide credentials, the Agent uses the credentials defined at installation.

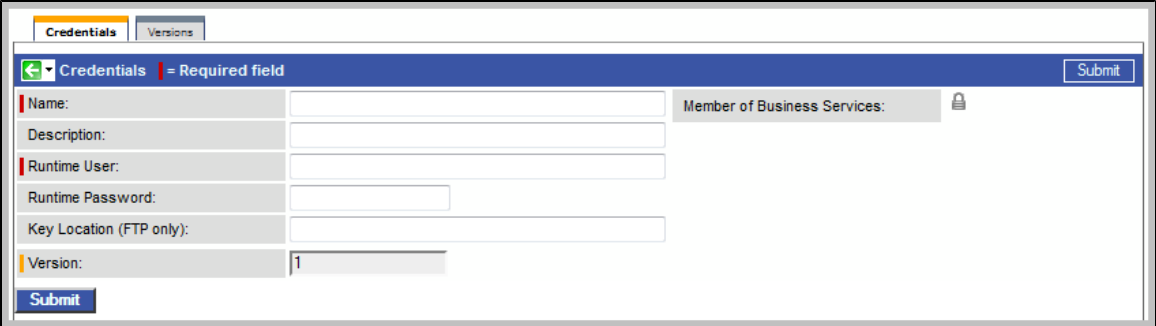
For [File Transfer tasks](#), the Agent may need additional credentials for logging on to the FTP server.

Defining Credentials

Step 1 From the navigation pane, select **Automation Center > Credentials**. The Credentials List screen displays.



Step 2 Click **New**. The Credentials Definition screen displays.



Step 3 Enter the Credential name, login ID (Runtime User), and the password. 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.

Optionally, assign the credential to a [Business Service](#).

Step 4 Click **Submit** to save the record. These credentials now can be selected on any Agent definition screen and any task definition screen.

Credentials Definition Field Descriptions

Field Name	Description
Name	Required. Name for this credential.
Member of Business Services	User-defined. Allows you to select one or more Business Services that this record definition belongs to. Click the lock icon to unlock the field and select Business Services .
Description	Description for this record.
Runtime User	Required. Runtime user ID under which the job will be run.
Runtime Password	Runtime user's password.
Key Location (FTP 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 ssh.</p>
Version	System-supplied. The version number of the current record, which is incremented by Opwise Controller every time a user updates a record. Click on the Versions tab to view previous versions. For details, see Record Versioning .
Versions tab	Stores copies of all previous versions of the current record. See Record Versioning .

LDAP Security

- LDAP Security
- Credentials for Running Tasks
- User Login Authentication
- Additional LDAP Properties

LDAP Security

You can set up Opwise Controller to use LDAP authentication both for running tasks on agents and for user logins. These instructions assume you have a working knowledge of LDAP security.

Credentials for Running Tasks

To use LDAP authentication for Controller user credentials:

UNIX	Set up your PAM configuration to use the PAM LDAP module. Depending on your LDAP version, some other configuration steps may be required. Once PAM is configured, tasks specifying credentials will authenticate over LDAP transparently.
Windows	No set-up steps are required. When you specify credentials for a task, use "DOMAIN\user" as the user name

User Login Authentication

For both the UNIX and Windows operating systems, you must configure Controller LDAP properties to enable the LDAP bridge.

Step 1	From the navigation pane, select Automation Center Administration > Configuration > LDAP Properties .
---------------	--

Step 2 Using the field descriptions provided on the screen, complete the required fields.

LDAP Properties
Save

Please edit your changes and press save

Connection Setup (required fields)

Name (or IP address in dotted format) of the LDAP server, together with the TCP port designation. Generally, port 389 is the non SSL enabled port, whereas with SSL enabled, its usually port 636. For example: ldap://ldap.stonebranch.com:389/ or ldaps://192.202.185.90:636/. To enable SSL connection, you will have to configure Automation Center with a X.509 CA certificate in the formats of DER encoded binary or Base-64 encoded.

The Distinguished Name (DN) of an account that will be used for initial access to LDAP directory. For example, a possible DN string for user 'joe' could be: cn=joe,dc=stonebranch,dc=com

The password associated with the initial DN that will be used for initial access to LDAP directory

Should LDAP be used for password authentication

Yes | No

LDAP Mapping

Distinguished name (DN) of an entry point in the directory. This DN identifies the starting point of the search for user records. If no base DN is specified, the search starts at the root of the directory tree. For example: dc=stonebranch,dc=com. This is a required value.

The LDAP attribute used to query for users. For example: cn or sAMAccountName for Microsoft Active Directory. You can only specify one attribute. This is a required value.

Search filter to apply to entries within the specified scope of the search. For example: objectClass=person. If no filter is specified, the server uses the filter (objectClass=*)

List of target OU's within the base DN directory to filter for user records. To specify more than one OU, use commas to separate the entries. For example, OU=Employees,OU=Students,OU=Other. To specify a multi-level OU, you can use a semi-colon. For example, OU=Users,OU=Employees;OU=Users,OU=Students or if only a single multi-level OU, OU=Users,OU=Employees;. If none are specified, the entire sub-tree from the base DN will be iterated.

Advanced Settings

The number of seconds before a timeout will occur when connecting to an LDAP server

Search filter to apply to entries within the specified scope of the search when searching for groups. If no filter is specified, the server uses the filter (objectClass=group).

List of target OU's within the base DN directory to filter for user group records. To specify more than one OU, use commas to separate the entries. For example, OU=Opwise Groups,OU=Opwise Admin Groups. To specify a multi-level OU, you can use a semi-colon. For example, OU=Groups,OU=Opwise Groups;OU=Groups,OU=Opwise Admin Groups, or if only a single multi-level OU, OU=Groups,OU=Opwise Groups;. If none are specified, user groups will not be mapped unless the group search filter is explicitly specified.

Save

Additional LDAP Properties

For additional LDAP properties not configurable from the user interface, see [Additional Opwise Controller Properties](#).

Audits

Overview

The Opwise Controller Audit function maintains a detailed record of all user interactions with the Controller, including before and after images related to any change and a description of the differences.

Audit records are written when the user performs any of the following actions:

- User login, user login failure, and user logout.
- Creates a new record.
- Updates a record.
- Deletes a record.
- Issues a command (Launch, Trigger Now, etc.).

Displaying the Audit Table

Step 1 From the navigation pane, select **Automation Center Administration > Security > Audits**. The Audit Records screen displays the first page of audit activity.

Audit Type	Source	Audit Date	Created by	Description
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I10
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I11
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I3
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I4
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I5
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I6
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I7
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I8
Command	User Interface	2013-07-23 07:15:47 -0700	ops.admin	Executing Command: ENABLE TRIGGER on I9
Create	User Interface	2013-07-23 07:15:40 -0700	ops.admin	Create: TimeTriggerBean I11, sys_id: 0be2affdd861e5e401af9e8b5f2ae60e
Create	User Interface	2013-07-23 07:15:27 -0700	ops.admin	Create: TimeTriggerBean I10, sys_id: 0be27da4d861e5e40074068871a317f2
Create	User Interface	2013-07-23 07:15:17 -0700	ops.admin	Create: TimeTriggerBean I9, sys_id: 0be25658d861e5e400e27481217f639c
Create	User Interface	2013-07-23 07:15:06 -0700	ops.admin	Create: TimeTriggerBean I8, sys_id: 0be22a10d861e5e40179b42846a90572
Create	User Interface	2013-07-23 07:14:55 -0700	ops.admin	Create: TimeTriggerBean I7, sys_id: 0be20213d861e5e401acfecda17e943e
Create	User Interface	2013-07-23 07:14:46 -0700	ops.admin	Create: TimeTriggerBean I6, sys_id: 0be1dd17d861e5e4000bc9ada23a9d89
Create	User Interface	2013-07-23 07:14:38 -0700	ops.admin	Create: TimeTriggerBean I5, sys_id: 0be1bcdad861e5e401cb3fef9d829921
Create	User Interface	2013-07-23 07:14:26 -0700	ops.admin	Create: TimeTriggerBean I4, sys_id: 0be1909ed861e5e401944825ee4533d4
Update	User Interface	2013-07-23 07:14:16 -0700	ops.admin	Update: TimeTriggerBean I3, sys_id: 0bdfc4b7d861e5e400f7283a9d266dbd
Create	User Interface	2013-07-23 07:12:28 -0700	ops.admin	Create: TimeTriggerBean I3, sys_id: 0bdfc4b7d861e5e400f7283a9d266dbd
User Login	User Interface	2013-07-23 06:46:05 -0700	system	LOGIN <user=ops.admin, ipaddr=24.246.72.241>

Step 2 To change the record selection, modify the display filter. For example, you may want to display all Audit activity for the past month. For instructions, see [Sorting and Filtering a List](#).

Step 3 To display details about a particular audit record, click on the underlined Audit Type field (in the leftmost column) of the record.

Audit Record
Child Audit Records

← Audit Record ↑ ↓

Audit Type:	Create	Table Name:	ops_task_unix
Audit Date:	2012-06-28 09:43:14 -0700	Table Key:	33f9a3c0d861e5e40062
Parent Audit Record:		Source:	User Interface
		Created by:	ops.admin

Description:
Create: TaskUnixBean BOB test, sys_id: 33f9a3c0d861e5e40062cb2506e22e7f

Status:
Success

Before:

After:
TaskUnixBean [{agent=2fe7e2a4d861e5e4009eef017b7b4ad4} {agent_cluster=} {agent_cluster_var=} {agent_cluster_var_check=false} {agent_var=} {agent_var_check=false} {avg_run_time=null} {broadcast_cluster=} {command=ps -ef} {command_or_script=Command} {credentials=} {credentials_var=} {credentials_var_check=false} {desktop_interact=false} {ef_duration=null} {ef_enabled=false} {ef_time=00:00} {ef_type=TIME} {environment=} {exec_counter=0} {exit_code_output=} {exit_code_processing=Success Exitcode Range} {exit_code_text=} {exit_codes=0} {first_run=null} {last_run=null} {last_run_time=null} {if_duration=null} {if_enabled=false} {if_time=00:00} {if_type=TIME} {is_duration=null} {is_enabled=false} {is_time=00:00} {is_type=TIME} {max_run_time=null} {min_run_time=null} {name=BOB test} {opswise_groups=} {output_return_file=} {output_return_nline=100} {output_return_sline=1} {output_return_text=} {output_return_type=NONE} {output_type=STDOUT} {parameters=} {res_priority=10} {retry_indefinitely=false} {retry_interval=60} {retry_maximum=0} {run_as_sudo=false} {run_count=0} {run_time=0} {runtime_dir=} {script=} {start_held=false} {start_held_reason=} {summary=test} {sys_class_name=ops_task_unix} {sys_created_by=ops.admin} {sys_created_on=2012-06-28 16:43:14} {sys_id=33f9a3c0d861e5e40062cb2506e22e7f} {sys_mod_count=0} {sys_updated_by=ops.admin} {sys_updated_on=2012-06-28 16:43:14} {type=Workflow} {user_duration=null} {version=1}]

Difference:

Additional Information: