Opswise Automation Center 5.1

Setting Up Security

Security

Overview

Setting up Opswise security involves the following steps:

- Creating users and assigning them passwords. You can also assign permissions to users.
- Creating groups of users. You can also assign permissions to groups.
- Assigning permissions to users and groups.
- Using Roles to assign administrative permissions.
- Creating credentials that allow Opswise to log in to remote machines and execute jobs.

Default Users and Groups

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

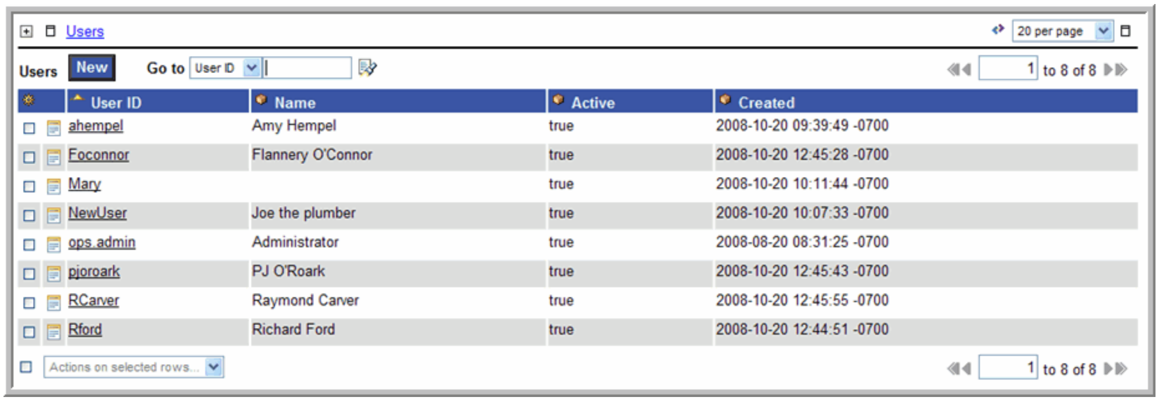
Two default user groups are also provided:

- Administrator Group has access to everything within Automation Center.
- Everything Group has access to everything except user and group administration.

Adding Users

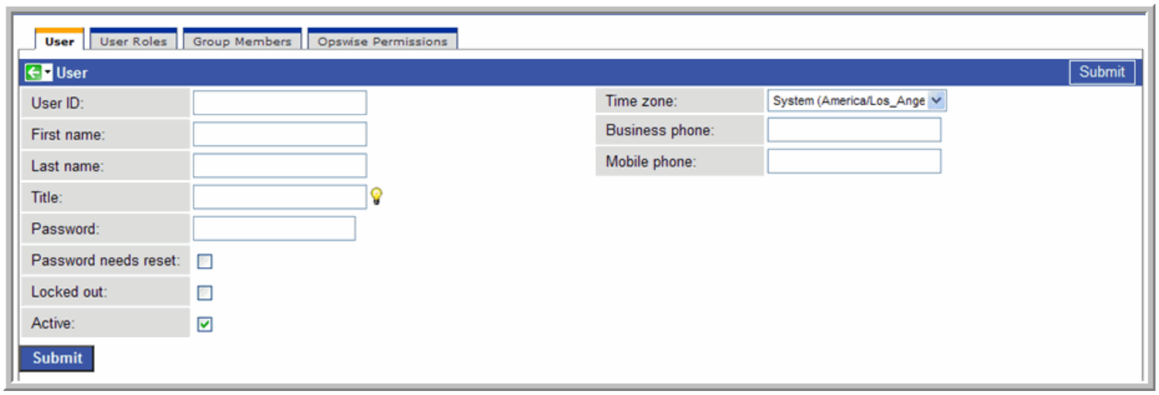
By default, a new user has no permissions. Until permissions are granted, a user can log into the system and can see options in the navigation pane but will not be able to do anything. You need administrative privileges to add users.

1. Select **Security > Users**. The User list appears, as shown in the sample below.



User ID	Name	Active	Created
ahempel	Amy Hempel	true	2008-10-20 09:39:49 -0700
Foconnor	Flannery O'Connor	true	2008-10-20 12:45:28 -0700
Mary		true	2008-10-20 10:11:44 -0700
NewUser	Joe the plumber	true	2008-10-20 10:07:33 -0700
ops.admin	Administrator	true	2008-08-20 08:31:25 -0700
pjoroark	PJ O'Roark	true	2008-10-20 12:45:43 -0700
RCarver	Raymond Carver	true	2008-10-20 12:45:55 -0700
Rford	Richard Ford	true	2008-10-20 12:44:51 -0700

2. Click the **New** button. A blank user form displays.



User ID:		Time zone:	System (America/Los_Ange
First name:		Business phone:	
Last name:		Mobile phone:	
Title:			
Password:			
Password needs reset:	□		
Locked out:	□		
Active:	☑		

3. Using the field descriptions provided below, fill in the fields.
4. Right-click on the title bar to save the new user record.
5. Optionally, assign one or more roles to the group, assign the user to a group, or assign permissions to this user.
6. Click **Submit** to save the new user record.

Field Descriptions

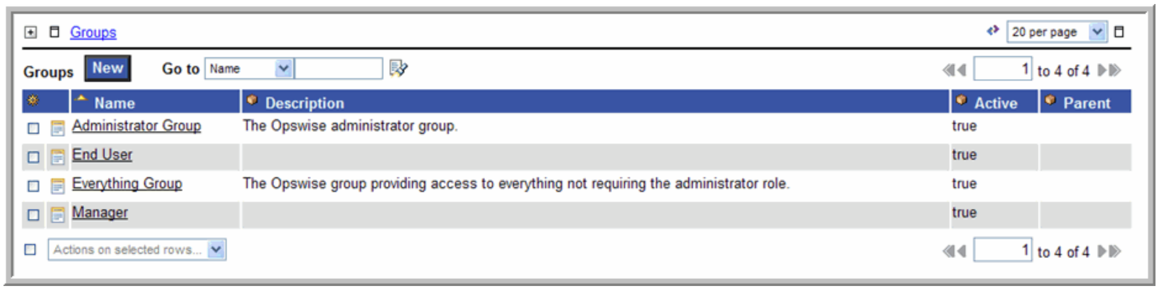
Field Name	Description
User ID	Log in ID for this user.
Time zone	Time zone of this user. When this user logs in, all scheduling times will be shown in the user's time zone, unless the trigger specifies a different time zone.
First name	User's first name.
Business phone	User's business phone number.
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.
Locked out	If enabled, locks out the user.
Active	If enabled, the user ID is active and the user can log in.
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.
Opswise Permissions tab	Allows you to assign permissions to this user.

Adding Groups

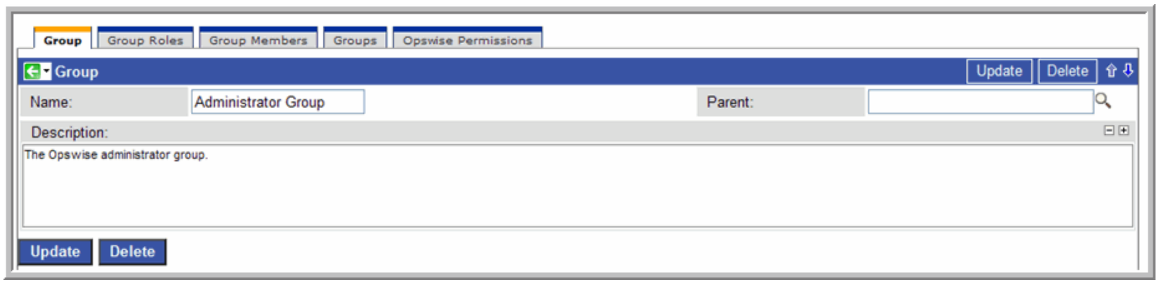
A group is a container for users. You can assign privileges and roles to groups or users. You can also assign groups to other groups. You need administrative privileges to add groups.

1. Select **Security > Groups**. The Groups list appears, as shown in the sample below.



	Name	Description	Active	Parent
□	Administrator Group	The Opswise administrator group.	true	
□	End User		true	
□	Everything Group	The Opswise group providing access to everything not requiring the administrator role.	true	
□	Manager		true	

2. Click the **New** button. A blank user form displays.



Name:	Administrator Group	Parent:	

Description:

The Opswise administrator group.

3. Using the field descriptions provided below, fill in the fields.
4. Right-click on the title bar to save the new group record.
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.
6. Click **Submit** to save the new group 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 the User record or from the Group record.

1. Open the user or group record.
2. Click the **Group Members** tab. This tab allows you to assign a user to one or more or vice versa. You can also add a new user or group record using this procedure.
3. To add a new user or group:
   a. Click **New**. A new user or new group screen displays.
   b. Fill in the field using the field descriptions for groups or users as guidance.
   c. Click **Submit** to save the new record. The record is added and assigned, and you are returned to the Group Members tab.
4. To add an existing record to this user or group:
   a. Click the **Edit** button. The Edit Members screen displays.
   b. 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**.
   c. Click **Save** to save your choices.

Using Roles to Assign Administrative Permissions

Some administrative functions within Opswise are assigned using roles instead of separate permissions. These functions include setting up security; creating reports, filters, and gauges; creating agent clusters; and creating and promoting bundles of records. Each role is a pre-defined collection of administrative permissions. By assigning the role to a user or group, you automatically give that user or group all permissions associated with the role. You cannot add new roles to the system and you must assign these permissions to groups or users using the pre-defined roles. (That is, these permissions cannot be assigned using the method described elsewhere in this section.)

Description of Roles

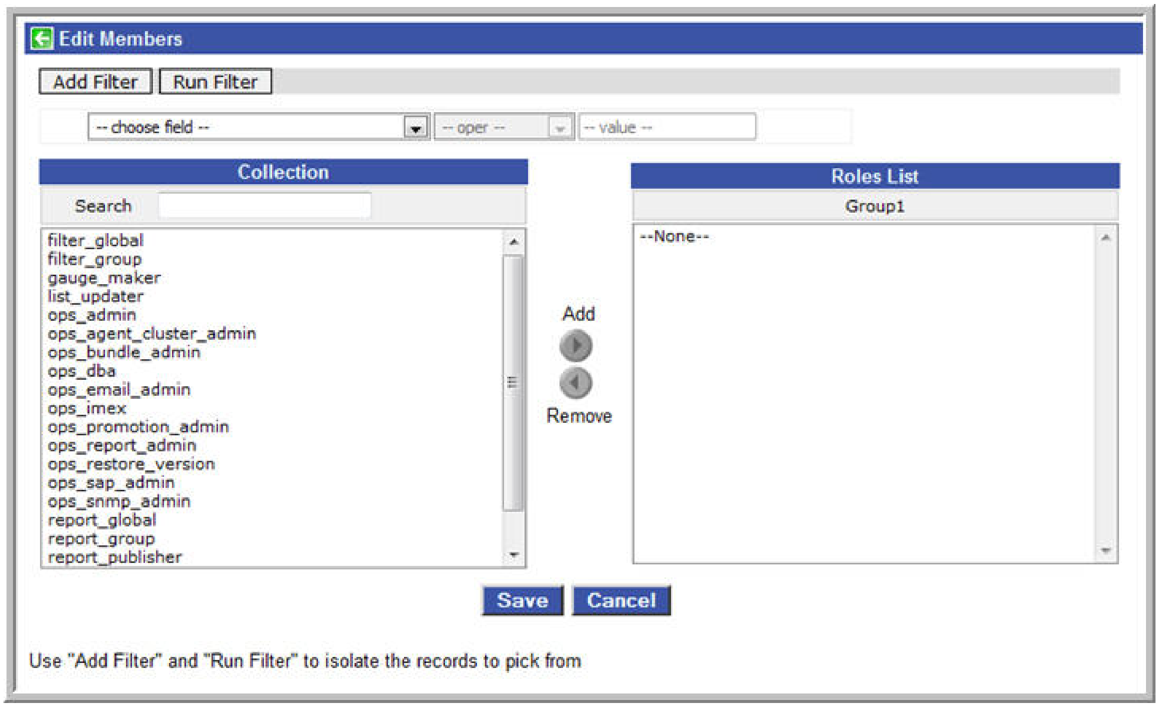
The following table summarizes the roles available in Opswise.

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 Opswise administrator role, which has permission on all Opswise features. The easiest way to grant Administration privileges to a user is to add the user to the Administrator Group.	• 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_bundle_admin	- Can create, read, update and delete Bundles. - Can read Bundle Targets including agent mappings. - Can read promotion history. - Can use **View Bundles** from the drop-down menu (available on records that can be bundled.) - Can use **Add To Bundle** from the drop-down menu, which adds the current record to the selected bundle. - Can use the **Create Bundle By Date** feature, which generates bundles of records created on or after a specified date. - Can generate a Bundle Report.	
ops_promotion_admin	- Can create, read, update and delete Bundle Targets including agent mappings. - Can read Bundles. - Can refresh Target Agents. - Can promote records. - Can promote Bundles. - Can generate a Bundle report. - Has "Accept Bundle" permission, which handles the promotion of a Bundle on the target server. This command is executed on the target server automatically as part of the "Promote" and "Promote Bundle" commands and does not involve user interaction.	
ops_agent_cluster_admin	Can create, update, and delete agent clusters.	
ops_dba	Can create, update, delete database connections.	
ops_email_admin	Can create, update, delete email connections.	
ops_imex	Can import/export records.	
ops_report_admin	Can create, update, and delete reports.	- gauge_maker - report_global - report_group - report_publisher - report_scheduler
ops_snmp_admin	Can create, update, delete SNMP connections.	
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 Roles to Users or Groups

1. From a User or Group screen, click the **User Roles** or **Group Roles** tab.
2. Click the **Edit** button. The Edit Members screen displays.



filter_global
filter_group
gauge_maker
list_updater
ops_admin
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
report_global
report_group
report_publisher

--None--

Use "Add Filter" and "Run Filter" to isolate the records to pick from

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

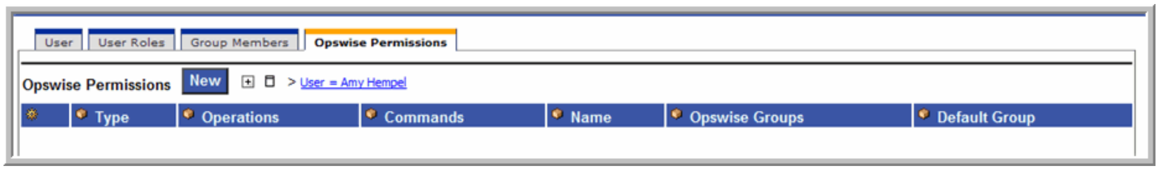
Assigning Permissions to Users or Groups

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

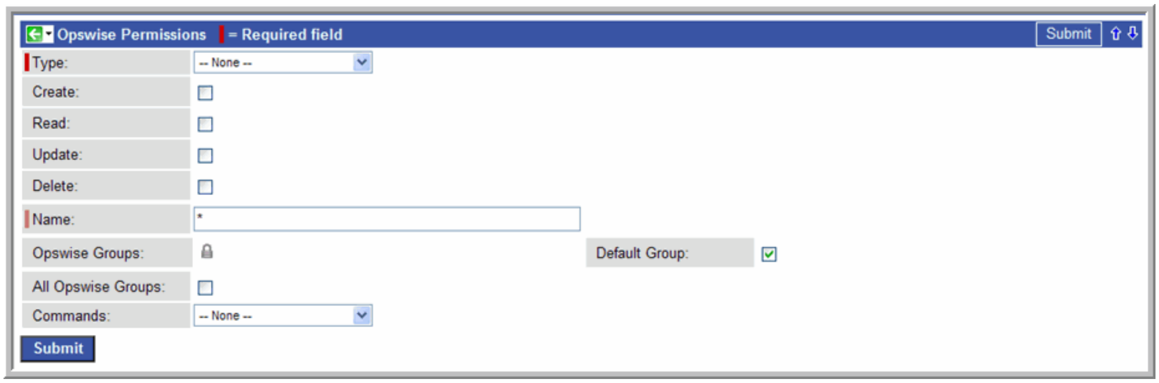
You can further narrow down which records each permission applies to by specifying either name parameters or Opswise groups. For example, a given permission might apply only to tasks whose name begins with "SF." Or, a permission might apply only to tasks that have been assigned to a specific Opswise group or to tasks that don't belong to any groups. See General Permissions Field Descriptions for more details.

You can add permissions to a user or a group, as described below.

1. Open the user or group to which you want to add permission.
2. Click the **Permissions** tab, shown below.



3. Click **New** to open the Permissions form.



Type:	-- None --		
Create:	□		
Read:	□		
Update:	□		
Delete:	□		
Name:	*		
Opswise Groups:		Default Group:	☑
All Opswise Groups:	□		
Commands:	-- None --		

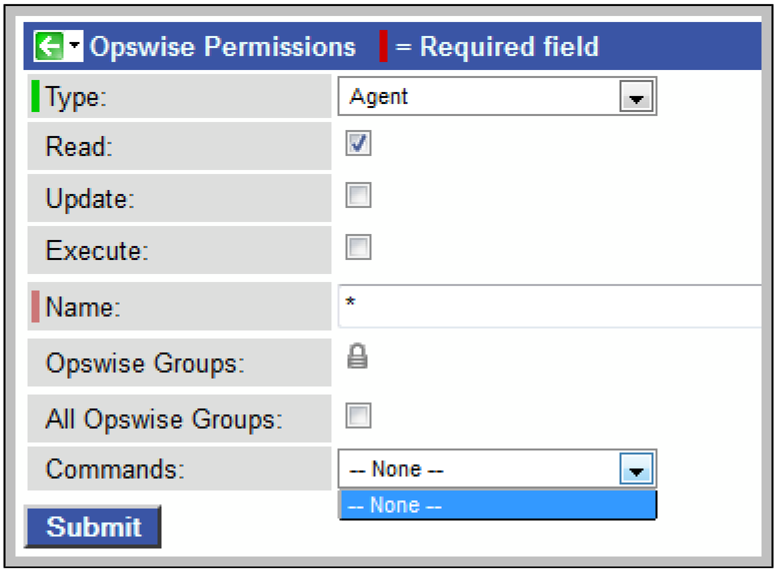
4. The permissions available differ depending on what you select in the Type field. Available permissions are Create, Read, Update, Delete, and Execute. For some record types, additional Commands are available. If the permission does not apply to the record type in the Type drop-down, the permission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

   Certain permissions include other permissions:
   - The **Create** permission implies **Read** and **Update** permissions.
   - The **Update** permission implies **Read** permission.
   - The **Delete** permission implies **Read** permission.

General Permissions Field Descriptions

Field Name	Description
Name	Applies this permission only to records whose name matches the string specified here. Wildcards are supported.
Opswise Groups	Applies this permission only to records that are members of the selected Opswise group(s). Note that Opswise groups are different from Security groups. Click on the lock icon to unlock the field and select groups.
Default Group	Applies this permission only to records that do not belong to any Opswise group. If this option is enabled, the user or user group will have the defined permissions on all records that do not belong to any Opswise group.
All Opswise Groups	Applies this permission to records that belong to any Opswise group (that is, the record must belong to at least one group).

Agent Permissions



Opswise Permissions = Required field

Type: Agent

Read: ☑

Update: □

Execute: □

Name: *

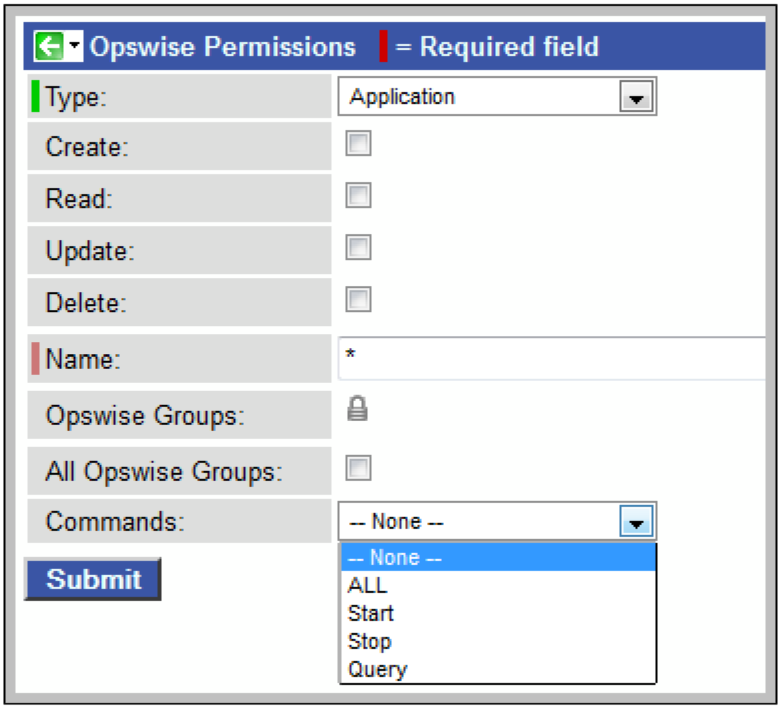
Opswise Groups: 🔒

All Opswise Groups: □

Commands: -- None --

Options	Description
Create	Agent records are created automatically so the **Create** checkbox does not appear.
Read	Grants permission to view a resource definition. All users can view configured agents in Opswise, so the **Read** checkbox always appears checked.
Update	Grants permission to update a resource definition. (Only certain fields can be updated.)
Delete	Only an Administrator can delete Agents, so the **Delete** checkbox does not appear.
Execute	Grants permission to execute a task on an agent.
Commands	N/A

Application Permissions

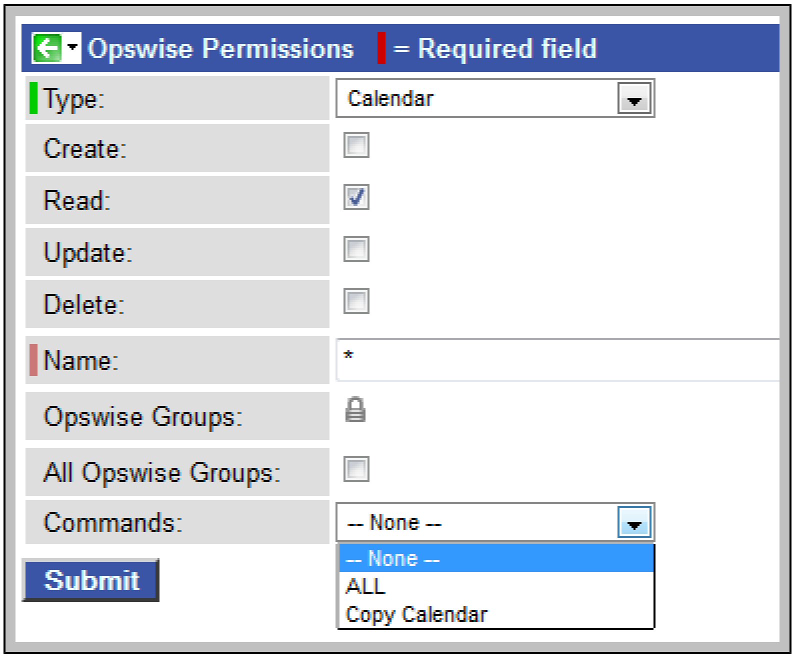


Opswise Permissions = Required field

Type:	Application
Create:	□
Read:	□
Update:	□
Delete:	□
Name:	*
Opswise Groups:	
All Opswise Groups:	□
Commands:	-- None --

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.
Execute	N/A
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

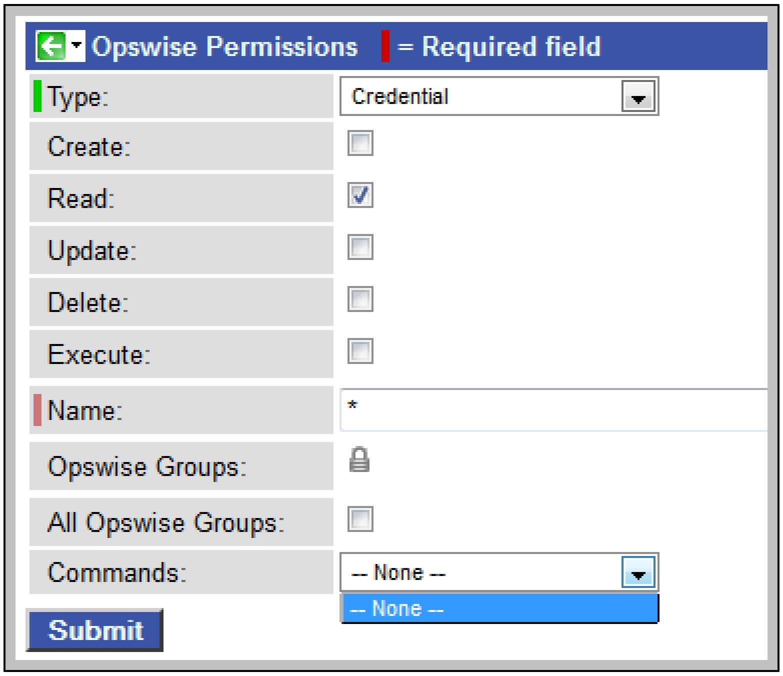


Opswise Permissions = Required field

Type:	Calendar
Create:	□
Read:	☑
Update:	□
Delete:	□
Name:	*
Opswise Groups:	🔒
All Opswise Groups:	□
Commands:	-- None --

Options	Description
Create	Grants permission to create a new calendar.
Read	Grants permission to read a calendar. All users can view Calendars in Opswise, so the **Read** checkbox always appears checked.
Update	Grants permission to update a calendar.
Delete	Grants permission to delete a calendar.
Execute	N/A
Commands	• ALL. Grants permission to copy a calendar. • Copy Calendar. Grants permission to copy a calendar.

Credentials Permissions

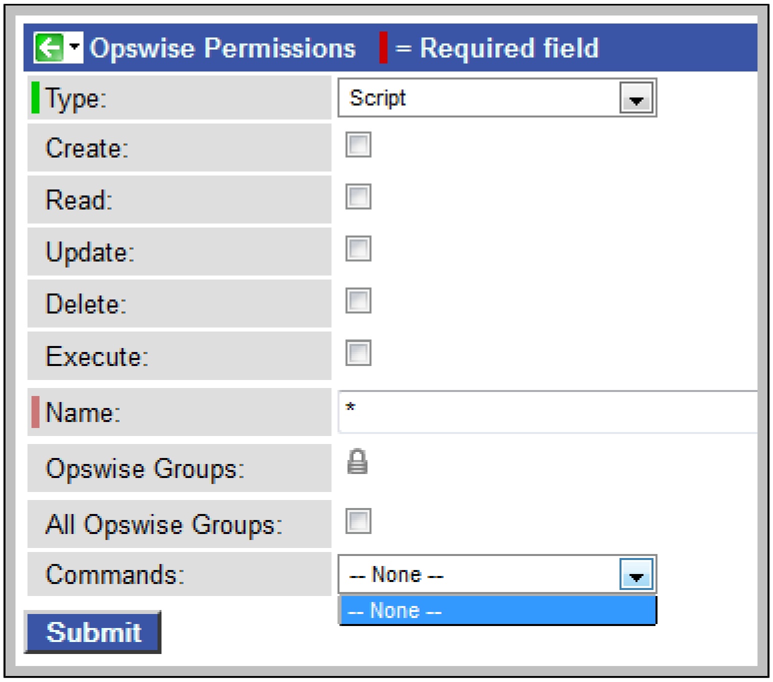


Opswise Permissions = Required field

Type:	Credential
Create:	□
Read:	☑
Update:	□
Delete:	□
Execute:	□
Name:	*
Opswise Groups:	🔒
All Opswise Groups:	□
Commands:	-- None --

Options	Description
Create	Grants permission to create a new credential.
Read	Grants permission to read a credential. All users can view Credentials in Opswise, so the **Read** checkbox 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

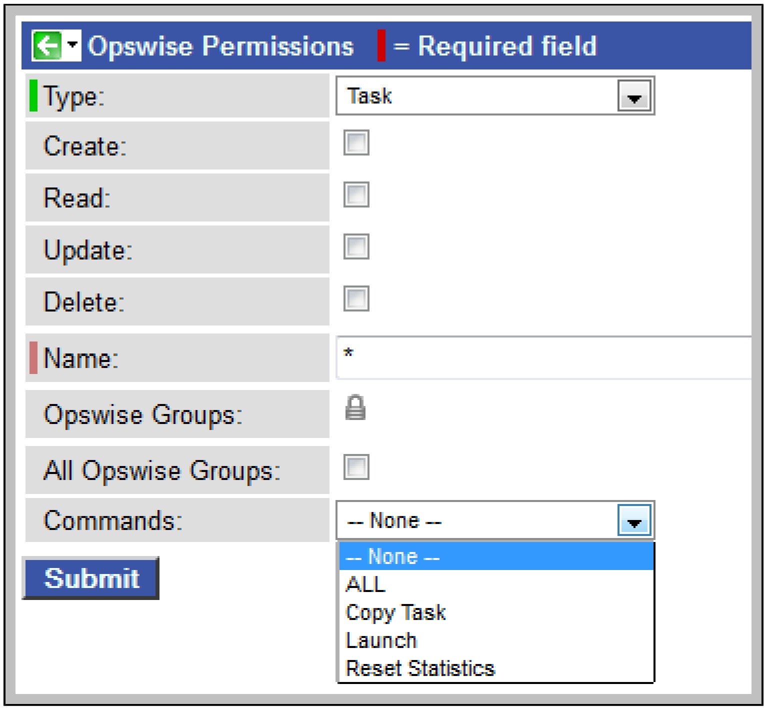


Opswise Permissions = Required field

Type:	Script
Create:	□
Read:	□
Update:	□
Delete:	□
Execute:	□
Name:	*
Opswise Groups:	🔒
All Opswise Groups:	□
Commands:	-- None --

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

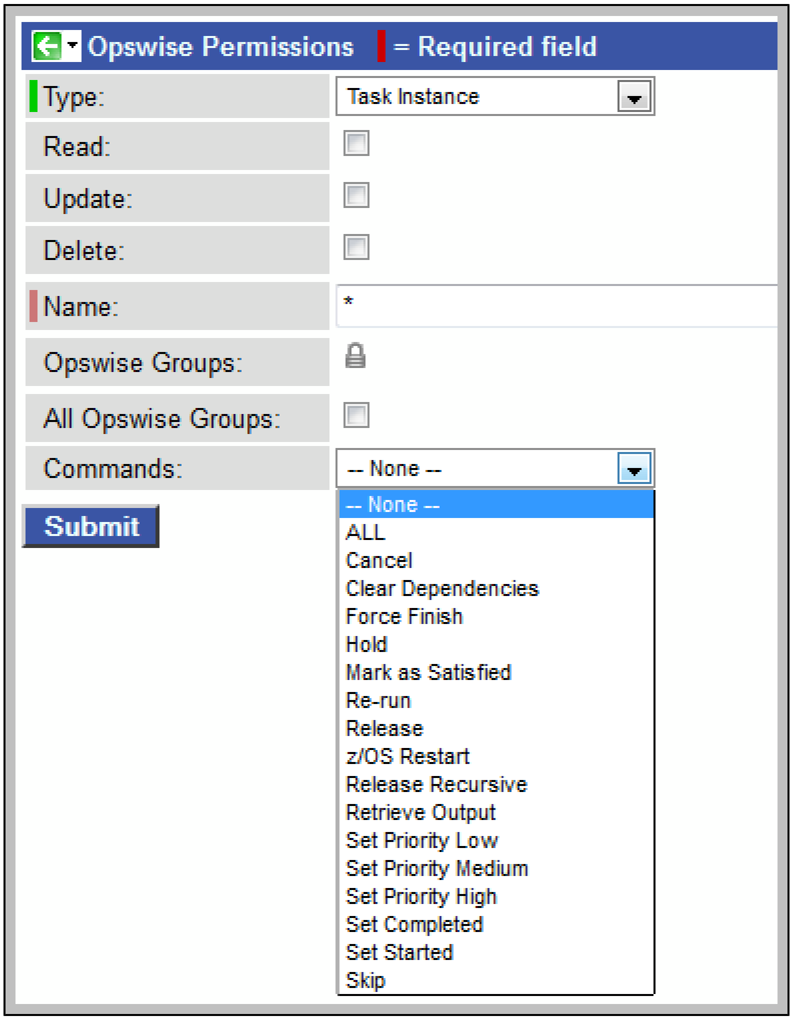


Opswise Permissions = Required field

Type:	Task
Create:	□
Read:	□
Update:	□
Delete:	□
Name:	*
Opswise Groups:	
All Opswise Groups:	□
Commands:	-- None --

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.
Execute	N/A
Commands	• All. Grants permission to issue any command. • Copy task. Grants permission to copy a task. • Launch. Grants permission to launch a task. • Reset Statistics. Grants permission to reset statistics.

Task Instance Permissions

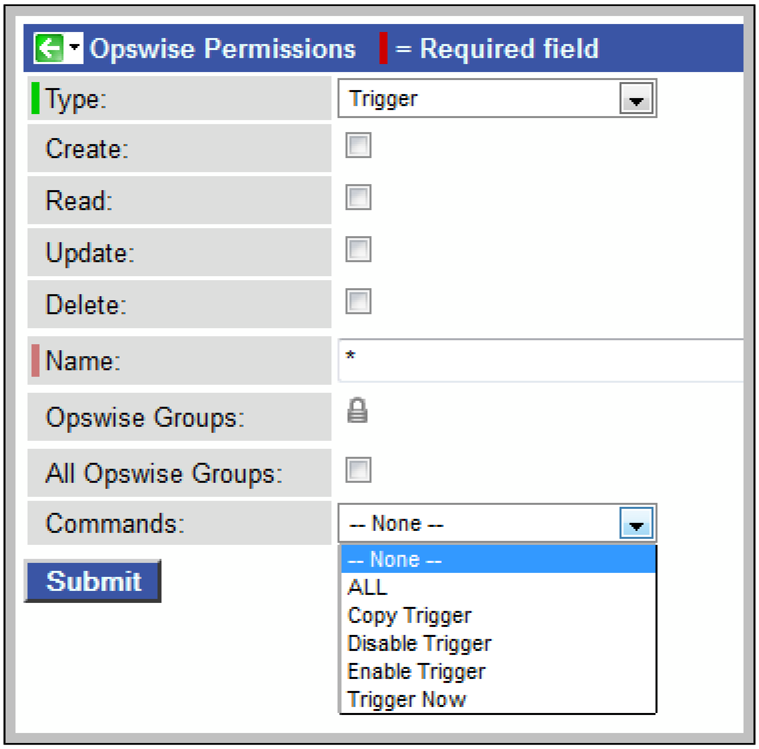


Opswise Permissions ▌= Required field

Type:	Task Instance
Read:	□
Update:	□
Delete:	□
Name:	*
Opswise Groups:	🔒
All Opswise Groups:	□
Commands:	-- None --

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.
Execute	N/A
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 Dependencies. Grants permission to clear all dependencies on a task instance. • Force Finish. Grants permission to force finish a task instance. • Hold. Grants permission to put a task instance on hold. • 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.

Trigger Permissions



Type:	Trigger
Create:	□
Read:	□
Update:	□
Delete:	□
Name:	*
Opswise Groups:	🔒
All Opswise Groups:	□
Commands:	-- None --

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.
Execute	N/A
Commands	• 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. • Trigger Now. Grants permission to trigger (launch) a task.

Credentials

Credentials are defined by the user and used by Opswise to log in to remote machines.

How Credentials are Used

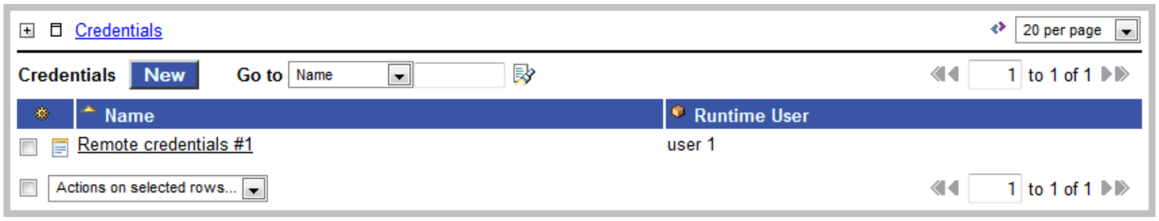
When Opswise executes a task on a remote machine, it may need a login ID and password to access the machine, also referred to as credentials. When prompted for credentials by a remote machine, Opswise looks in the following locations in the order shown for the ID and password:

1. If the task contains credential information, the agent uses those.
2. If the task does not provide credentials, the agent uses the credentials in the agent resource definition.

In the case of File Transfer tasks, the Opswise agent may need an additional credential for logging on to the FTP server.

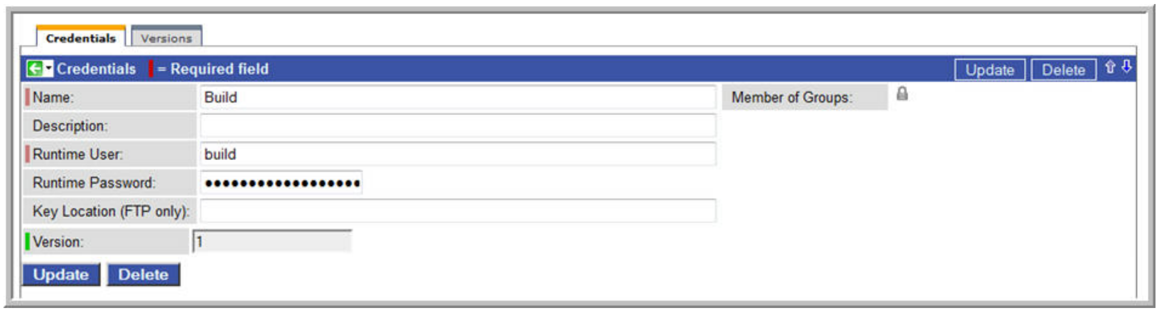
Defining Credentials

1. From the navigation pane, select **Credentials**. Opswise displays the credentials list.



Name	Runtime User
Remote credentials #1	user 1

2. Click **New**. A Credentials form displays, as shown below.



Name:	Build
Description:	
Runtime User:	build
Runtime Password:	••••••••••••••••••
Key Location (FTP only):	
Version:	1
Member of Groups:	

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 an Opswise group.
4. Click **Submit** to save the record.

Field Name	Description
Name	Record name for this credential.
Member of Groups	User-defined. Allows you to select one or more Opswise groups that this record definition belongs to. Click on the lock icon to unlock the field and select groups.
Description	Description for this record.
Runtime User	Runtime user ID under which the job will be run.
Runtime Password	Runtime user's password.
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. Opswise does not currently 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 Opswise to use it. For example, to validate the keys, log into your destination server from your agent server using ssh.
Version	Task definition only; system-supplied. The version number of the current record, which is incremented by the system 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

You can set up Opswise 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

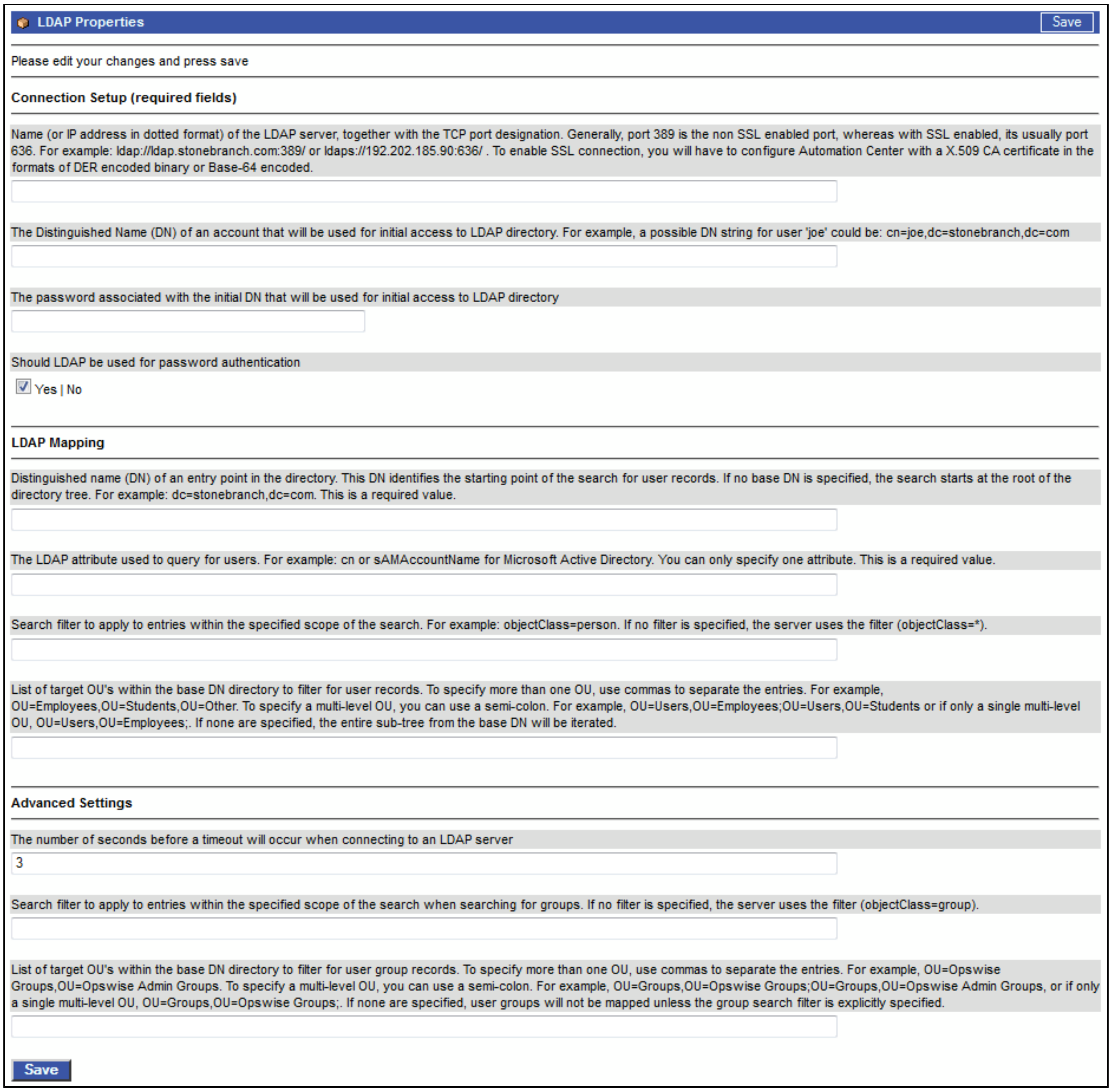
To use LDAP authentication for Opswise user credentials, follow these steps:

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

User Login Authentication

For either operating system, you must configure Opswise LDAP properties to enable the LDAP bridge.

1. From the navigation pane, select **Automation Center Administration > Configuration > LDAP Properties.**
2. Using the field descriptions provided on the screen and in the following table, complete the required fields.



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

3

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=Opswise Groups,OU=Opswise Admin Groups. To specify a multi-level OU, you can use a semi-colon. For example, OU=Groups,OU=Opswise Groups;OU=Groups,OU=Opswise Admin Groups, or if only a single multi-level OU, OU=Groups,OU=Opswise Groups;. If none are specified, user groups will not be mapped unless the group search filter is explicitly specified.