# Opswise Automation Center 5.1.1

# Security

# Security

# Opswise Automation Center Security

## Setting Up Security



## Audits



The information on these pages also is located in the Opswise Automation Center 5.1.1 Security.pdf.

# Security Overview

## Opswise Automation Center Security

Setting up Opswise Automation Center security involves the following steps:

- Creating users and assigning them passwords.
- Creating groups of users.
- Assigning permissions (access to Opswise records) to users and groups.
- Assigning roles (permission to perform administrative functions) to users and groups.
- Creating credentials that allow Opswise to log in to remote machines and execute jobs.
- Setting up Opswise Automation Center to use LDAP authentication.

# Users and Groups



## Default Users and Groups

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

Two default user groups also are provided:

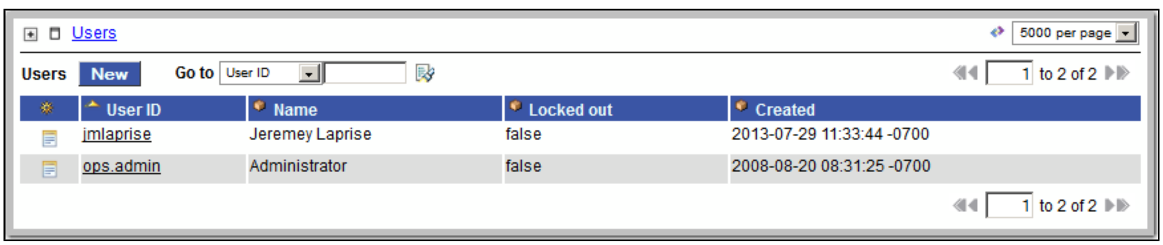
- **Administrator Group** has access to everything within Opswise Automation Center.
- **Everything Group** has access to everything except user and group administration.

## Adding Users

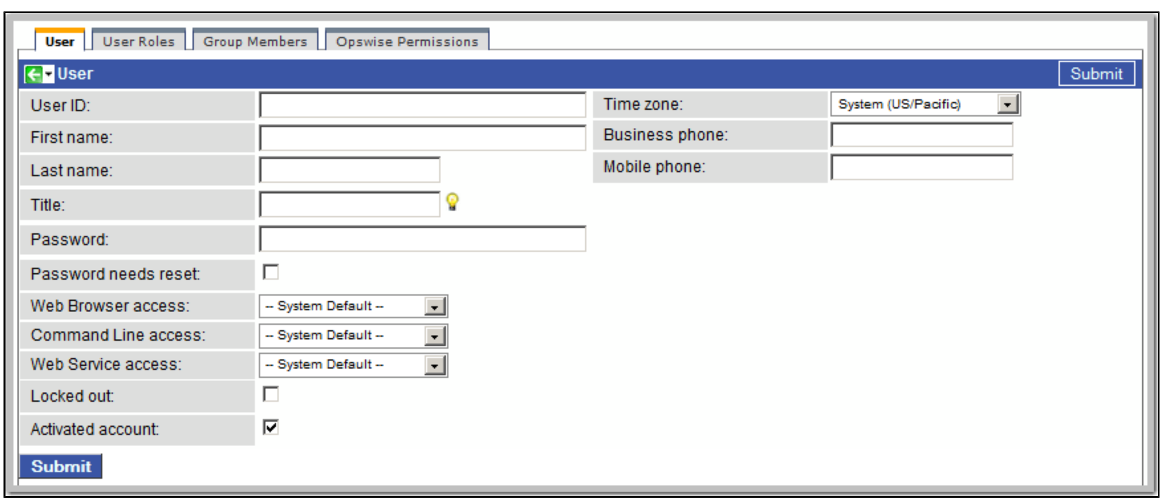
**Note**
You must have administrative privileges to add users.

By default, a new user has no permissions. Until permissions are granted, a user can log into Opswise 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 User List screen displays.




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




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

| | |
|---|---|
| **Step 4** | Right-click on the title bar to save the new user 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 new user 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 Opswise Automation Center user interface. Options:<br>• System Default - User restriction for logging in to the Opswise Automation Center user interface is based on the current system default value of the System Default Web Browser Access Opswise system property.<br>• Yes - User is not restricted from logging in to the Opswise Automation Center user interface.<br>• No - User is restricted from logging in to the Opswise Automation Center user interface. |
| Command Line access | Specifies whether or not the user can log in to the Opswise Command Line Interface (CLI). Options:<br>• 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 Opswise system property.<br>• Yes - User is not restricted from logging in to the CLI.<br>• No - User is restricted from logging in to the CLI. |
| Web Service access | Specifies whether or not the user can log in to the Opswise RESTful Web Services API. Options:<br>• System Default - User restriction for logging in to the Opswise Web Services is based on the current system default value of the System Default Web Service Access Opswise system property.<br>• Yes - User is not restricted from logging in to the Opswise Web Services.<br>• No - User is restricted from logging in to the Opswise 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 Opswise. |
| **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. |

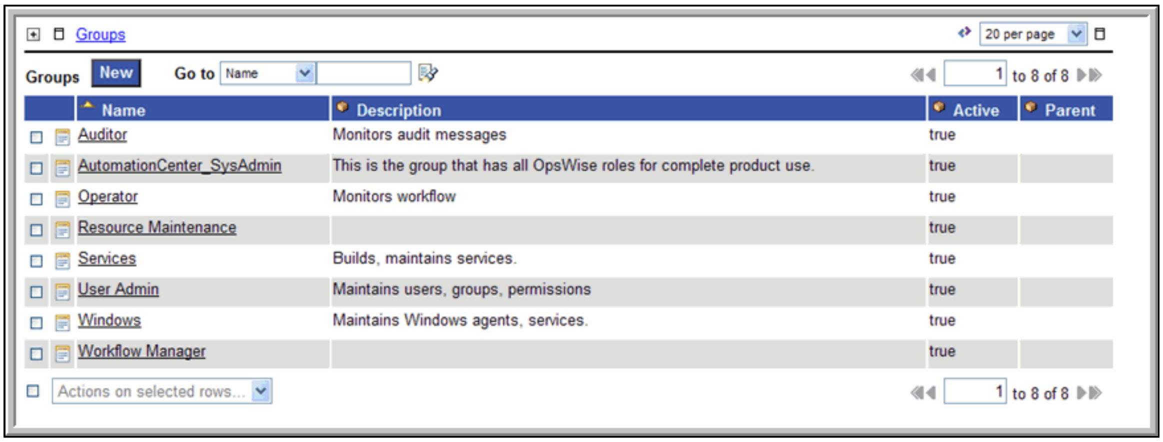
| | |
|---|---|
| **Opswise Permissions** tab | Allows you to assign permissions to this user. |

## Adding Groups

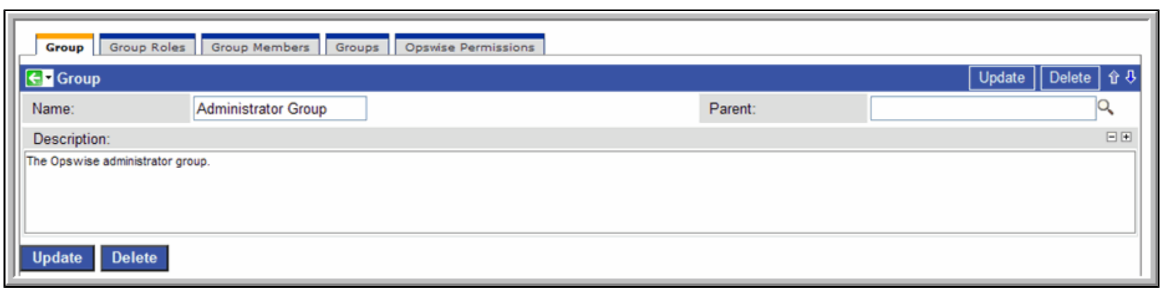
> **Note**
> You must have administrative privileges to add groups.

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.

<table>
<tr><td>Step 1</td><td>From the navigation pane, select Automation Center Administration > Security > Groups. The Groups List screen displays.



</td></tr>
<tr><td>Step 2</td><td>Click New. The Group Definition screen displays.



</td></tr>
<tr><td>Step 3</td><td>Using the field descriptions provided below, fill in the fields.</td></tr>
<tr><td>Step 4</td><td>Right-click on the title bar to save the new group record.</td></tr>
<tr><td>Step 5</td><td>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.</td></tr>
<tr><td>Step 6</td><td>Click Submit to save the new group record.</td></tr>
</table>

## 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 vice versa. You can also add a new user or group record using this procedure. |
| **Step 3** | To add a new user or group:<br>1. Click **New**. A new user or new group screen displays.<br>2. Fill in the field using the field descriptions for groups or users as guidance.<br>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:<br>1. Click the **Edit** button. The Edit Members screen displays.<br>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**.<br>3. Click **Save** to save your choices. |

# Roles and Permissions



## Assigning Roles to Users or Groups

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

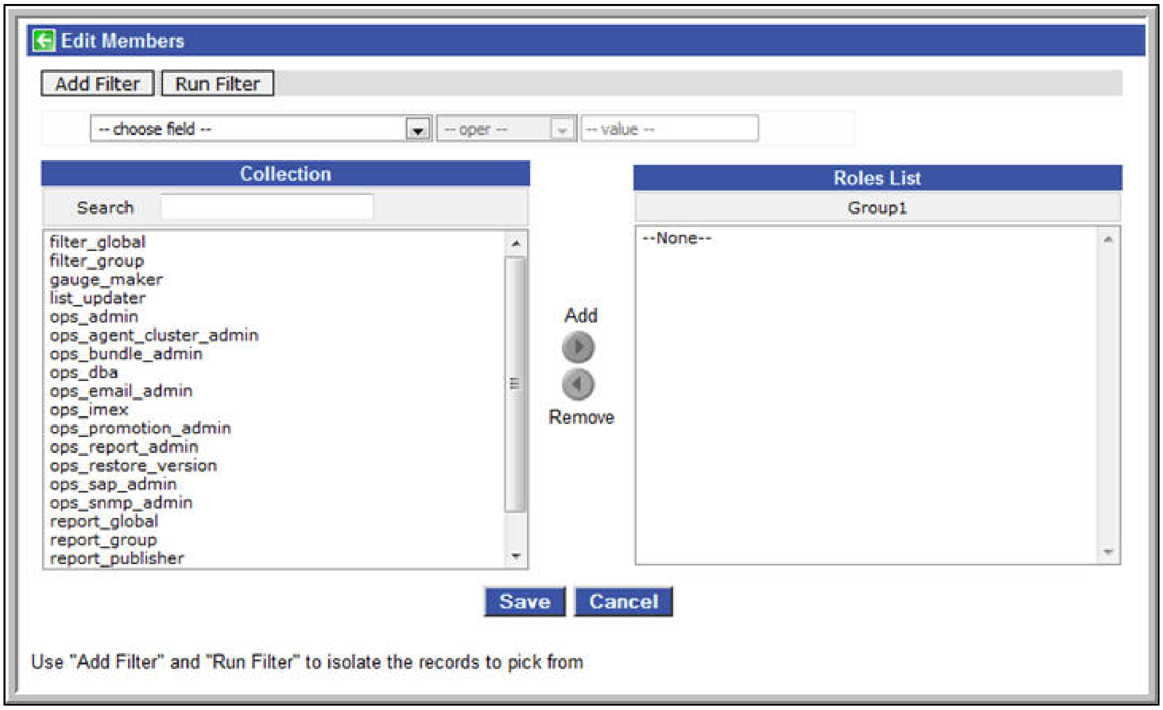
- Setting up security.
- Creating reports, filters, and gauges.
- Creating agent clusters.
- Creating and promoting bundles of records.

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 Opswise; 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.<br><br> |
| **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 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<br>• filter_group<br>• list_updater<br>• ops_agent_cluster_admin<br>• ops_bundle_admin<br>• ops_dba<br>• ops_email_admin<br>• ops_imex<br>• ops_promotion_admin<br>• ops_report_admin<br>• ops_restore_version<br>• ops_sap_admin<br>• ops_snmp_admin<br>• user_admin |
| ops_agent_cluster_admin | Can create, update, and delete agent clusters. | |

| | | |
|---|---|---|
| ops_bundle_admin | <ul><li>Can create, read, update, and delete Bundles.</li><li>Can view Promotion Targets, including agent mappings.</li><li>Can view Promotion History.</li><li>Can view a record's list of bundles.</li><li>Can add a record to a bundle.</li><li>Can create bundles by date.</li><li>Can generate a Bundle Report.</li></ul> | |
| 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><li>Can create, read, update, and delete Promotion Targets, including agent mappings.</li><li>Can view Bundles.</li><li>Can refresh Target Agents.</li><li>Can promote records.</li><li>Can promote Bundles.</li><li>Can generate a Bundle report.</li><li>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.)</li></ul> | |
| ops_report_admin | Can create, update, and delete reports. | <ul><li>gauge_maker</li><li>report_global</li><li>report_group</li><li>report_publisher</li><li>report_scheduler</li></ul> |
| 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. | |

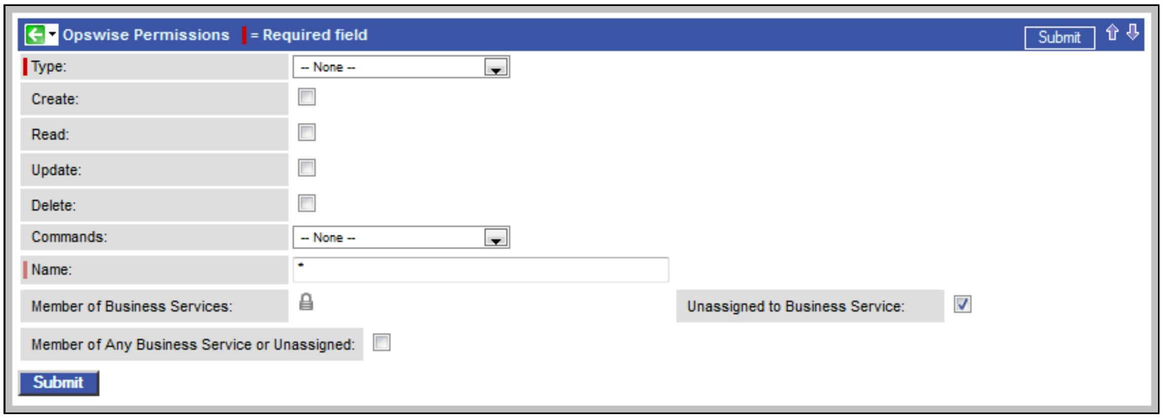
## Assigning Permissions to Users or Groups

Permissions control user access to Opswise 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:<br> |
| **Step 3** | Click **New** to open the Permissions form.<br> |
| **Step 4** | Select permissions for the selected user or group.<br><br>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.<br><br>Certain permissions include other permissions:<br>• **Create** permission includes **Read** and **Update** permissions.<br>• **Update** permission includes **Read** permission.<br>• **Delete** permission includes **Read** permission. |

# Types of Permissions

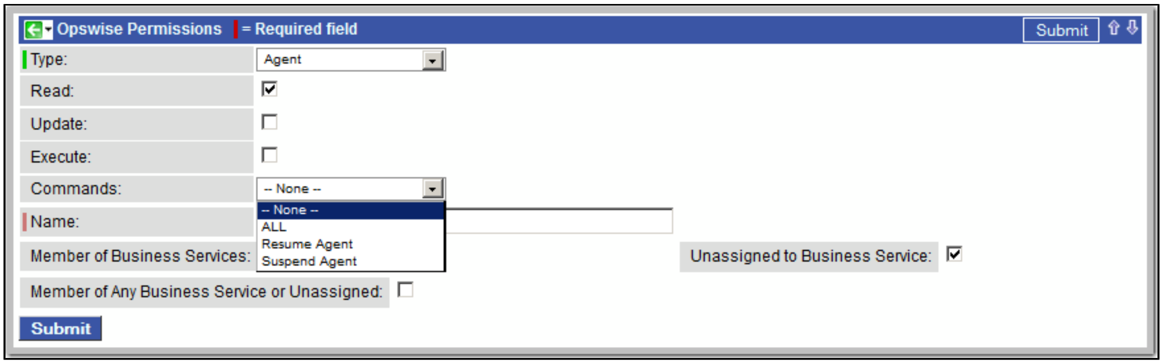
This section identifies the different types of permissions that you can add to a user or group.

## General Permissions Field Descriptions

The following fields of information display on the Permissions screen for all Permission types:

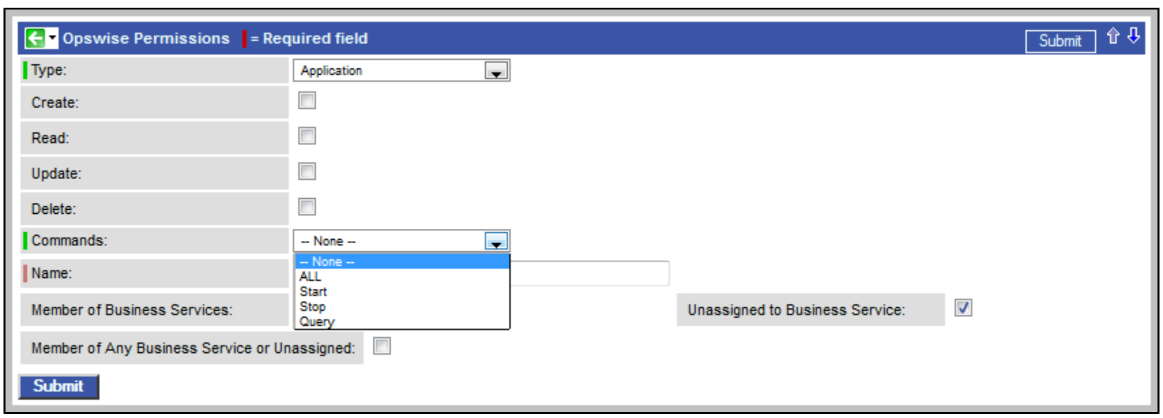
| Field Name | Description |
|---|---|
| Name | Applies this permission to records whose name matches the string specified here. Wildcards are supported. |
| Member of Business Services | Applies this permission to records that are members of the selected Business Service(s). Click the lock icon to unlock 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



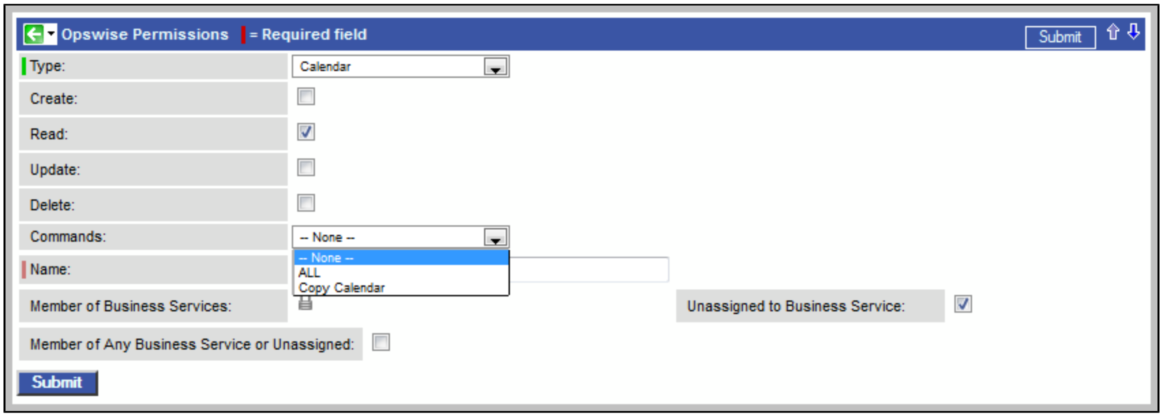

| Options | Description |
|---|---|
| Read | Grants permission to view an agent definition. All users can view configured agents in Opswise, so the **Read** check box always is checked. |
| Update | Grants permission to update an agent definition. (Only certain fields can be updated.) |
| Execute | Grants permission to execute a task on an agent. |
| Commands | • ALL: Grants permission to suspend and resume agents.<br>• Resume Agent: Grants permission to resume the ability of a suspended agent to run tasks.<br>• Suspend Agent: Grants permission to suspend the ability of an agent to run tasks. |

## Application Permissions



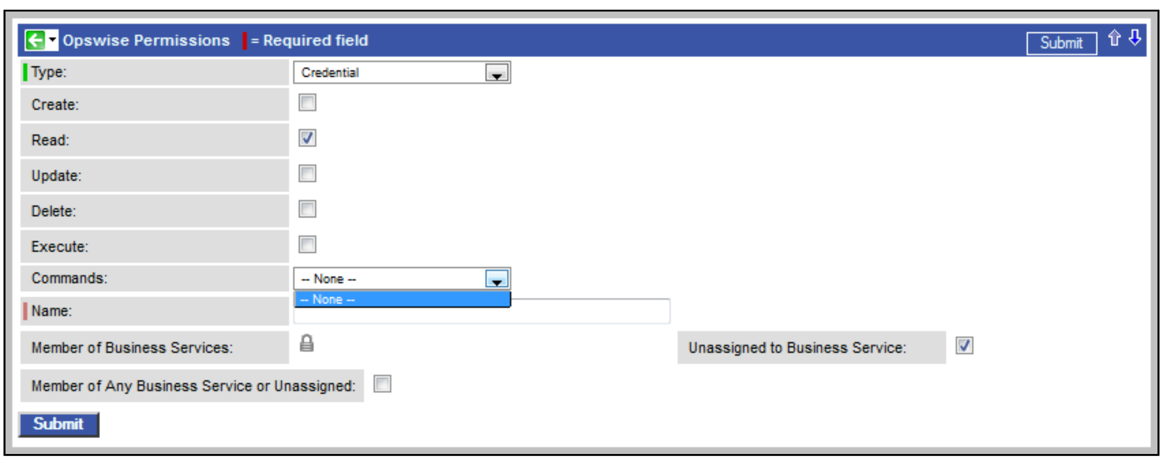

| Options | Description |
|---|---|
| Create | Grants permission to create a new application. |
| Read | Grants permission to read an application. |
| Update | Grants permission to update an application. |
| Delete | Grants permission to delete an application. |
| Commands | See Application Control Tasks for details. Options:<br>• ALL: Grants permission to execute a Start, Stop, and Query from the Application resource screen.<br>• Start: Grants permission to execute a Start from the Application resource screen.<br>• Stop: Grants permission to execute a Stop from the Application resource screen.<br>• Query: Grants permission to execute a Query from the Application resource screen. |

## Calendar Permissions



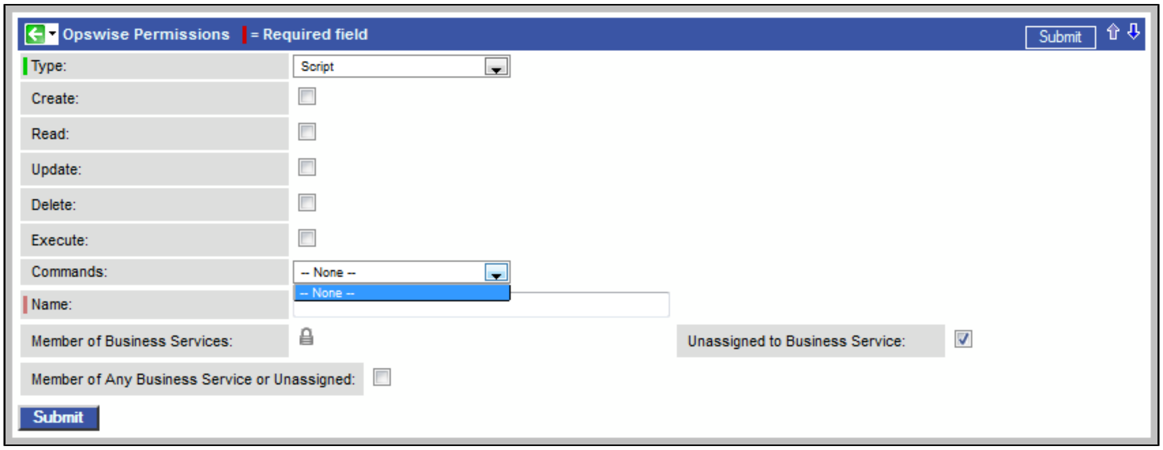

| Options | Description |
|---|---|
| Create | Grants permission to create a new calendar. |
| Read | Grants permission to read a calendar. All users can view Calendars in Opswise, so the **Read** check box always appears checked. |
| Update | Grants permission to update a calendar. |
| Delete | Grants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

## Credential Permissions



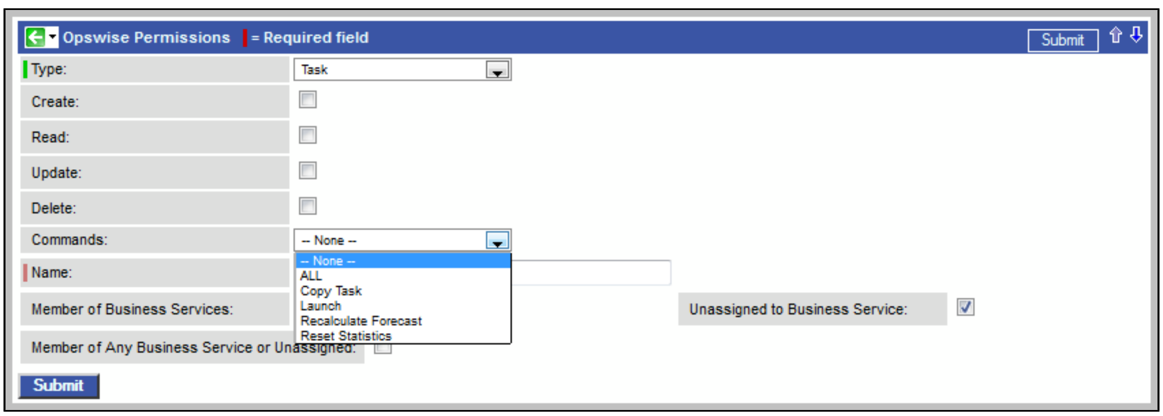

| Options | Description |
|---|---|
| Create | Grants permission to create a new credential. |
| Read | Grants permission to read a credential. All users can view Credentials in Opswise, so the **Read** check box always appears checked. |
| Update | Grants permission to update a credential. |
| Delete | 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 task containing a script. |
| Commands | n/a |

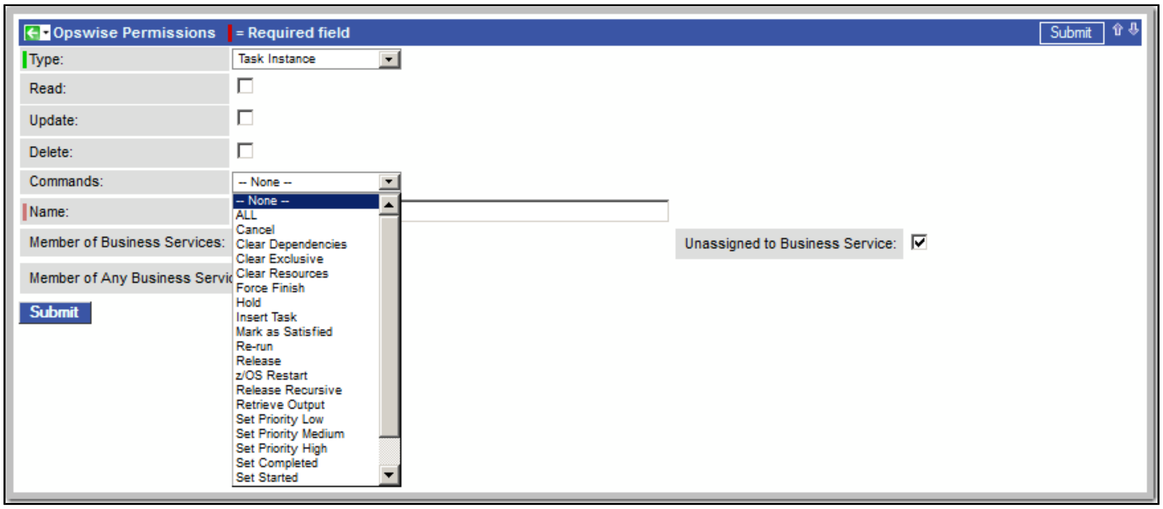
## Task Permissions




| 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. |

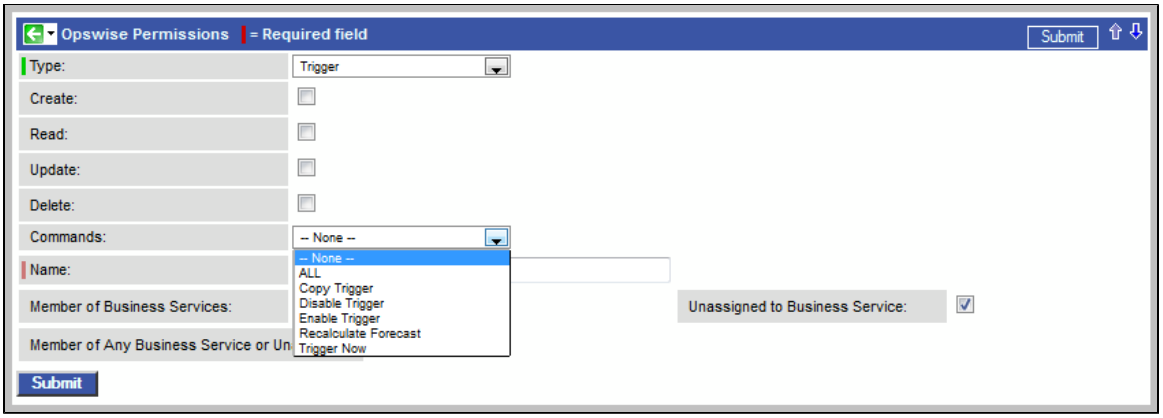
| | |
|---|---|
| Commands | • ALL: Grants permission to issue any command.<br>• Copy Task: Grants permission to copy a task.<br>• Launch: Grants permission to launch a task.<br>• Recalculate Forecast: Grants permission to recalculate a forecast.<br>• Reset Statistics: Grants permission to reset statistics. |

## 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.<br>• ALL: Grants permission to issue any command.<br>• Cancel: Grants permission to cancel a task instance.<br>• Clear Dependencies: Grants permission to clear all dependencies on a task instance.<br>• Clear Exclusive: Grants permission to clear all mutual exclusive dependencies from a task instance.<br>• Clear Resources: Grants permission to clear all resource dependencies of a task instance.<br>• Force Finish: Grants permission to force finish a task instance.<br>• Hold: Grants permission to put a task instance on hold.<br>• Insert Task: Grants permission to insert a task on the workflow monitor of a workflow task instance.<br>• Mark as Satisfied: Can mark a dependency as satisfied.<br>• Re-run: Grants permission to re-run a task instance.<br>• Release: Grants permission to release a task instance from hold.<br>• z/OS Restart: Grants permission to restart a z/OS task from a specific step.<br>• Release Recursive: Grants permission to release a workflow and all its tasks from hold.<br>• Retrieve Output: Grants permission to execute the Retrieve Output button.<br>• Set Priority Low: Grants permission to change the priority of a task to Low.<br>• Set Priority Medium: Grants permission to change the priority of a task to Medium.<br>• Set Priority High: Grants permission to change the priority of a task to High.<br>• Set Completed: Grants permission to set a Manual task instance status to completed.<br>• Set Started: Grants permission to set a Manual task instance status to a new started time.<br>• Skip: Grants permission to skip a task instance.<br>• Unskip: Grants permission to unskip a task instance selected to be skipped. |

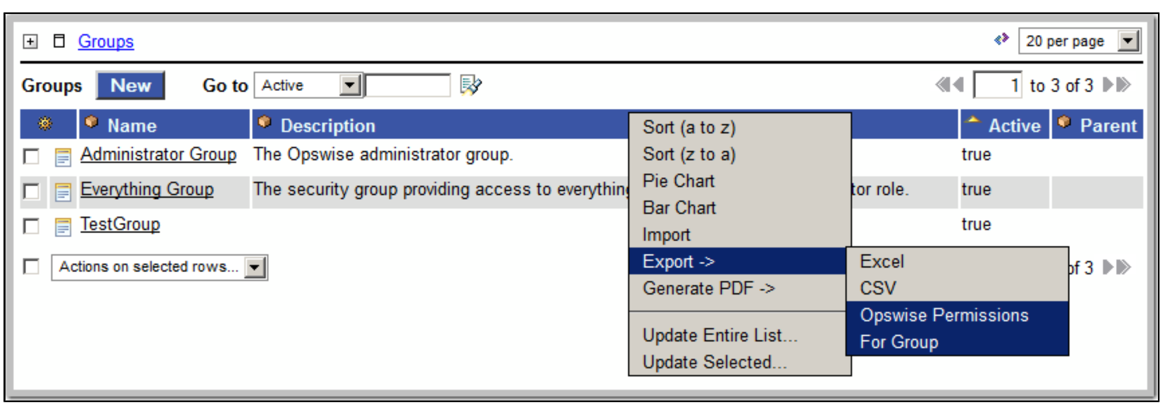
## Trigger Permissions




| 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 | • ALL: Grants permission to do all listed below.<br>• Copy Trigger: Grants permission to copy a trigger.<br>• Disable Trigger: Grants permission to disable a trigger.<br>• Enable Trigger: Grants permission to enable a trigger.<br>• Recalculate Forecast: Grants permission to recalculate a forecast.<br>• Trigger Now: Grants permission to trigger (launch) a task. |

## Exporting Opswise Permissions for a Group

Opswise lets you export Opswise security groups and their Opswise permissions, which then can be imported into another 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** | Right-click the Groups List screen title bar and from the pop-up menu 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 Opswise 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" tabs 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.

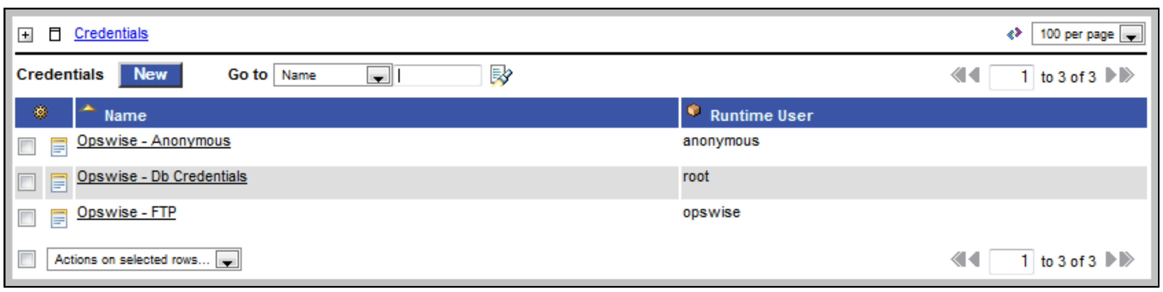
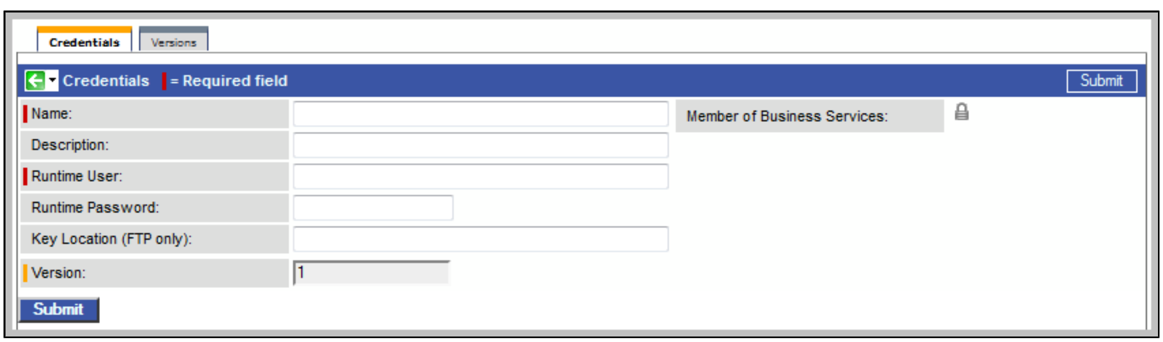
Agent credentials are defined during installation, but via the user interface, you also can define credentials and assign them to any task or agent.

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 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.<br><br> |
| **Step 2** | Click **New**. The Credentials Definition screen displays.<br><br> |
| **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.<br><br>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) | 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.<br><br>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 | System-supplied. The version number of the current record, which is incremented by Opswise 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

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:

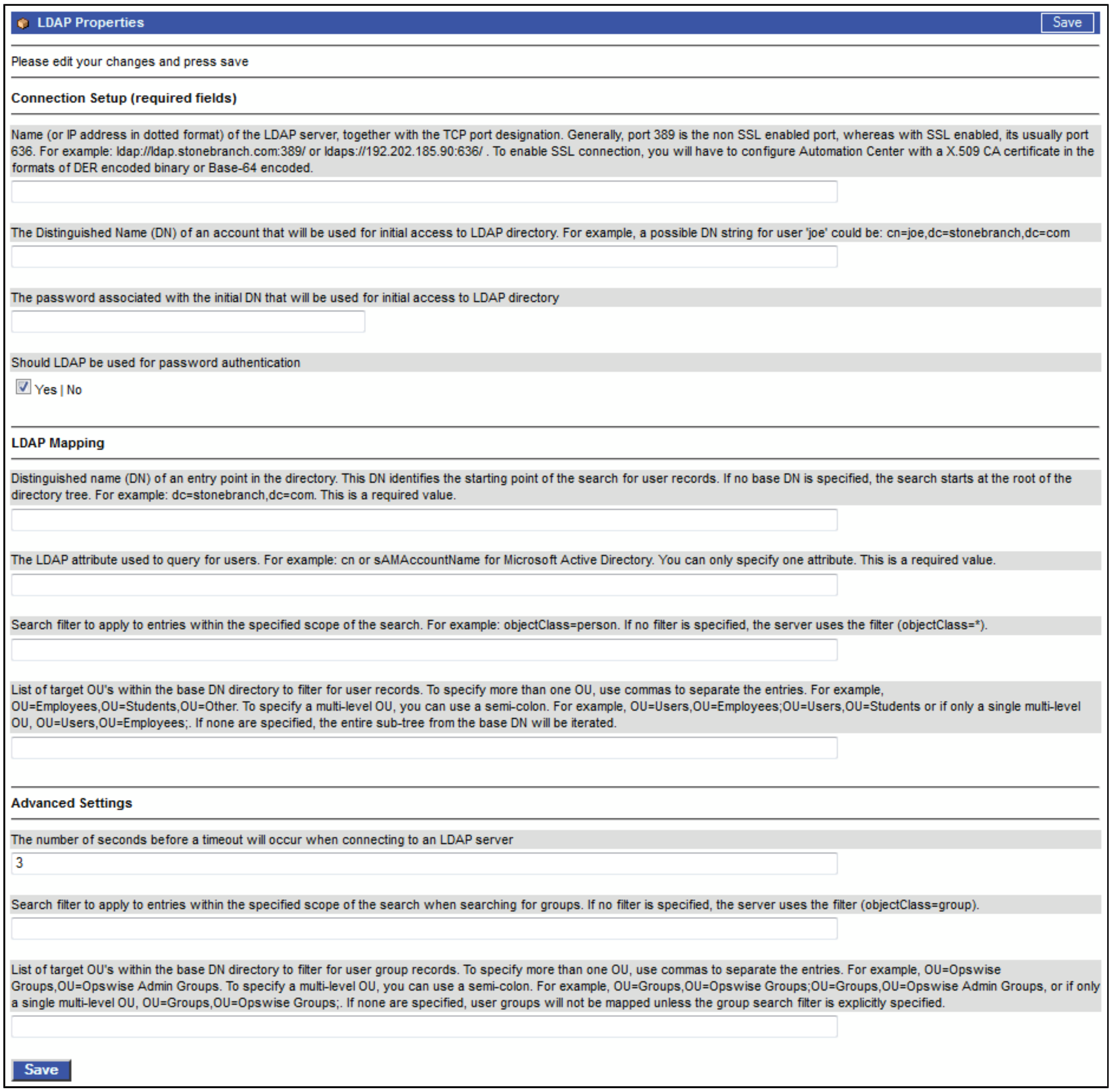
| | |
|---|---|
| **UNIX** | Set up your PAM configuration to use the PAM LDAP module. Depending on your LDAP version, some other configuration steps may be required. Once PAM is configured, tasks specifying credentials will authenticate over LDAP transparently. |
| **Windows** | No set-up steps are 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 Opswise 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.




## Additional LDAP Properties

For additional LDAP properties not configurable from the user interface, see Controller Properties (glide.properties).

# Audits

## Overview

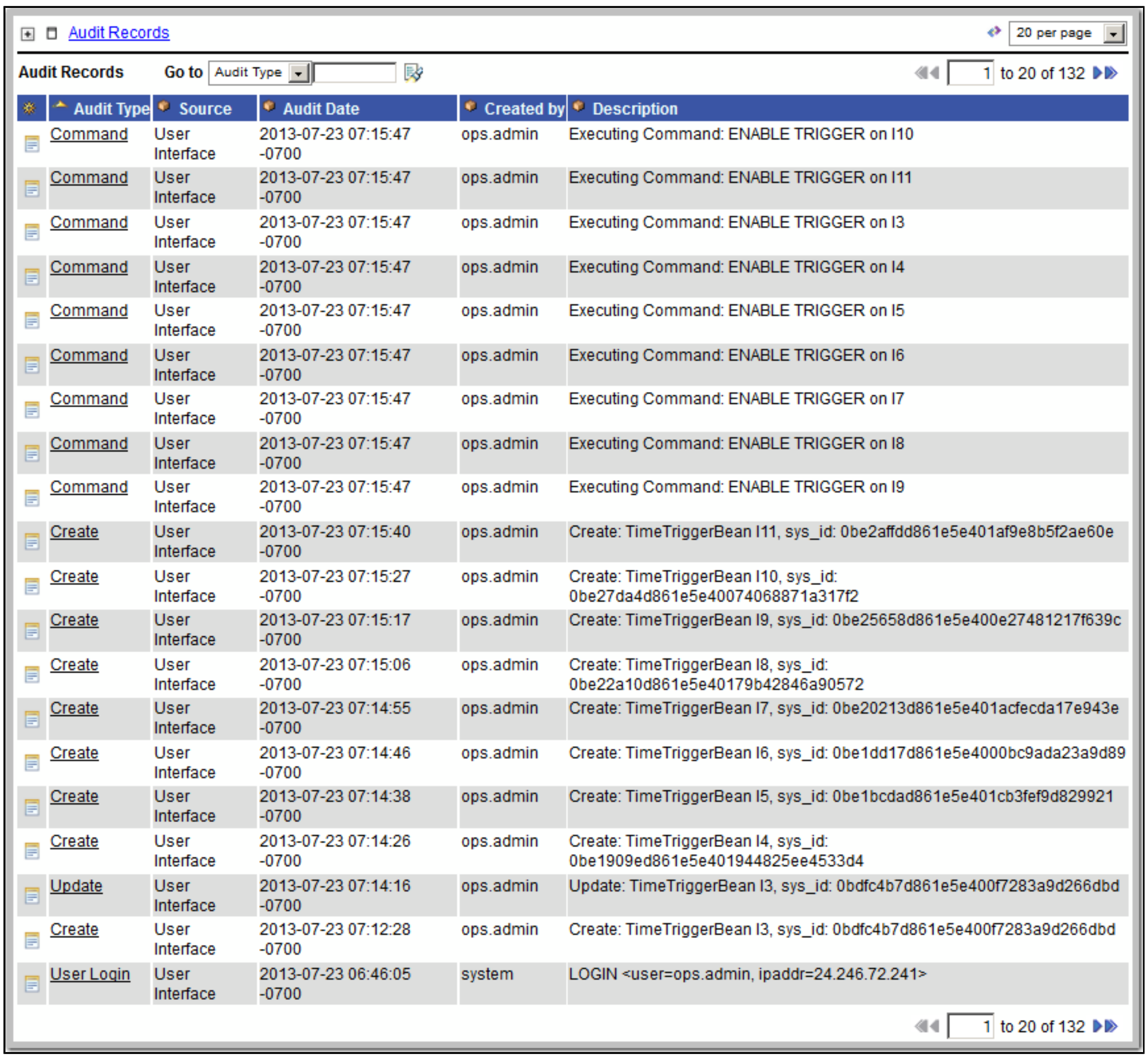
The Opswise Audit function maintains a detailed record of all user interactions with Opswise, including before and after images related to any change and a description of the differences.

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 Records

20 per page

Audit Records Go to Audit Type

1 to 20 of 132

| 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> |

1 to 20 of 132

**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. |