

# Manage Admin User Accounts

Creating and managing administrator accounts in OPS-COM is essential for granting system access to staff, defining their responsibilities through roles, and maintaining secure and accurate user records. This article guides OPS-COM administrators through the process of creating new admin accounts, editing existing ones, resetting passwords, and disabling accounts as needed.

## Using this Feature

1. Hover over **System Configuration**, click **Admin Management**, then **Edit Admin Users**. The **Manage Active Administrators** screen displays, providing options for both new user creation and existing user modification.

### Creating a New Admin Account

1. On the **Manage Active Administrators** screen, select **+ Create New Admin**.
2. The screen will display the **Create New Administrator** form divided into two sections:
  - On the left, you will **enter the user information** for the new administrator (e.g., username, first name, last name, email, and initial password).
  - On the right, in the **Active Roles** form, you will **select the admin role(s)** this person will be granted. For more information about Roles and Permissions [refer to this wiki article](#).
3. Once all information is entered and roles are selected, click **Insert New User** to add the admin account to the system.

### Editing an Existing Admin Account

1. On the **Manage Active Administrators** page, select the user you wish to modify.
2. You can now change any of the available options for that selected user, including their personal information, roles, and account status.
3. Click **Update User** when you are finished making your changes.

### Viewing Login Activity

- For any selected user, you can click the **Login Activity** button to view a log of when the administrator last logged into the OPS-COM system or a handheld device.

## Resetting an Admin's Password

1. Locate the specific administrator's account.
2. In the **Password** field, enter a temporary password. The password is hidden (displayed as asterisks "\*\*\*\*\*"), but you can simply type over the existing symbols.
3. **Inform the admin of this temporary password.**
4. When the admin logs in using the temporary password, they will be prompted to update their password to a more secure, personal one.

## Disabling an Admin Account

Admin users cannot be permanently deleted from the system because their accounts are often linked to historical data (e.g., ticket issuance, system changes). If an admin user changes roles or leaves the organization, the best practice is to disable their account.

**Important Reporting Note** - It is very important to leave the admin user's permissions in place even when disabling their account, as these permissions will still affect historical reporting (e.g., showing which permissions were active at the time certain actions were performed). Once the account is disabled, any existing permissions obviously cannot be actioned by that user, but they remain associated for reporting purposes.

1. Hover over the **System Configuration** menu, click **Admin Management**, then **Edit Admin Users**.
2. Select the user's account you wish to disable (e.g., "jim\_daniels").
3. The user's profile will display. Locate the checkbox titled **Activate this account and allow system login**.
4. **Uncheck** this box to disable the account.
5. Click **Update User** to apply the change.

After disabling, the account will now appear on the **Manage Disabled Administrators** page, accessed by clicking on **View Disabled** on the **Manage Active Administrators** page.

This action can be reversed at any time by editing the user account and re-checking the **Activate this account and allow system login** checkbox.

## Best Practices & Considerations

- **Secure Initial Passwords:** When creating new accounts or resetting passwords, use strong, temporary passwords and instruct users to change them immediately upon first

login.

- **Role-Based Access:** Always assign appropriate roles to admin users. Avoid giving **Primary Administrator** access unless absolutely necessary. Granular roles ensure users only have access to the functions they need.
  - **Prompt Disabling:** Disable accounts promptly when an employee's role changes or they leave the organization. This is a critical security measure.
  - **Audit Login Activity:** Regularly review the **Login Activity** for admin accounts to monitor for unusual patterns or unauthorized access attempts.
  - **Clear Documentation:** Maintain internal records of your admin accounts, their assigned roles, and any specific notes, especially for disabled accounts.
- 

## Related Video

<https://www.youtube.com/embed/pKpDFhMcTXA?wmode=opaque>

<https://www.youtube.com/embed/VDg5pjzDc28?wmode=opaque>

---

Revision #8

Created 15 May 2024 08:04:18

Updated 25 June 2025 13:08:11 by Cedar Boulianne