Overview

Druva administrators use the services enabled for their account to protect data created and managed on devices and servers in their organization. Druva administrators are categorized as:

- Druva Cloud Administrator
- Product Administrators
  - Administrators for inSync
  - Administrators for Druva Phoenix

Druva Cloud Administrator

A Druva Cloud Administrator is a super administrator account manager who can:

- Create additional Druva Cloud Administrator
- Create product administrators
- Use inSync services enabled for the account
- Use Phoenix services enabled for the account
- Configure and manage Single Sign-On (SSO)
- Can login to Druva Cloud Platform Console without SSO (failsafe administrator privilege)
- Enable or disable Geofencing
- Enforce a Password Policy

Druva Cloud Administrators get all the rights of all the administrative roles across products, based on the services enabled for your account and the privileges needed to modify account settings.

inSync Administrator

For optimized use of Druva services, a Druva Cloud Administrator creates administrators to backup and restore data that resides on user endpoints such as laptops, desktops, and cloud apps like Microsoft 365. To prevent unauthorized
account configuration and restrict access to user data, a Druva Cloud Administrator assigns roles that define the rights available to inSync administrators. inSync administrator roles are described below:

The following table lists the predefined administrator roles for each edition.

<table>
<thead>
<tr>
<th>Administrator Role</th>
<th>Available in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Druva Cloud Administrator</td>
<td>Available for all the license types</td>
<td>Druva Cloud Administrator can configure Druva services (inSync and Druva Phoenix) and has the privileges to set up and manage the product account, create another Druva Cloud Administrator and other administrators. Only a Druva Cloud Administrator can manage another Druva Cloud Administrator. Also, a Druva Cloud Administrator inherits the privileges of the Cloud Administrator.</td>
</tr>
<tr>
<td>Cloud Administrator</td>
<td>Available for all the license types</td>
<td>An administrator assigned to this role can perform all core inSync activities such as configuring, managing, and monitoring inSync. Cloud Administrators can create and manage other administrators and also manage another Cloud Administrator. Cloud Administrators can configure a compliance policy. They can also place users on legal hold.</td>
</tr>
<tr>
<td>Workload Administrator</td>
<td>Available for all the license types</td>
<td>An administrator assigned to this role can manage operations for a specific data source individually. For example, a Workload Administrator for the Endpoints data source will have access only related to Endpoints. Similarly, a Data Source administrator for Microsoft 365 &gt; Exchange Online, will have access to only Exchange Online and to no other workloads.</td>
</tr>
<tr>
<td>Data Protection administrator</td>
<td>• Elite • Elite Plus (deprecated) • Elite • Enterprise</td>
<td>An administrator assigned to this role has restricted access associated with their profiles. They have the necessary permissions to manage data privacy and data access settings for the users. The Data Protection administrator cannot place or view users on Legal Hold.</td>
</tr>
<tr>
<td>Help Desk administrator</td>
<td>Available for all the license types</td>
<td>An administrator assigned to this role has restricted access associated with their profiles. They have the necessary permissions to manage day-to-day activities such as performing backup and restore operations, resetting passwords for the users, and addressing user complaints. The Help Desk administrator cannot place or view users on legal hold.</td>
</tr>
<tr>
<td>Administrator Role</td>
<td>Available in</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Legal administrator</td>
<td>• Elite Plus (deprecated) • Elite</td>
<td>An administrator assigned to this role can perform activities related to legal hold, such as creating and deleting Legal Hold policies, viewing users who are on legal hold, adding and removing users from legal hold, viewing and accessing backed up data.</td>
</tr>
<tr>
<td>Profile administrator</td>
<td>Available for all the license types</td>
<td>An administrator assigned to this role has restricted access associated with their profiles. They have the necessary permissions to manage users and devices, backups and restores. Profile administrators can access the Non-Compliance report only for the profiles they are mapped to. However, they cannot view the compliance summary at the inSync Compliance Dashboard, or configure a compliance policy. Additionally, profile administrators cannot place or view users on legal hold.</td>
</tr>
<tr>
<td>inSync Compliance administrator</td>
<td>Elite Plus (deprecated) Or with the Sensitive Data Governance</td>
<td>An administrator assigned to this role has access to all pages of inSync Compliance and they can define, edit, and delete policies, templates, and sensitive data as well as edit compliance settings. They also have access to inSync reports.</td>
</tr>
<tr>
<td>View Only administrator</td>
<td>Available for all the license types</td>
<td>An administrator assigned to this role has restricted access associated with their profiles. They have the necessary permissions to view the inSync settings and user details. They also have access to inSync reports. The View Only administrator cannot place or view users on legal hold.</td>
</tr>
</tbody>
</table>

Based on the administrator roles, rights are allocated to the administrators. For more information on roles and rights, see Predefined roles and rights.

**Phoenix Administrator**

For optimized use of Druva services, a Druva Cloud Administrator can create Phoenix administrators to backup and restore data that reside on remote servers such as virtual machines and NAS devices. To prevent unauthorized account configuration, a Druva Cloud Administrator assigns roles to the Phoenix administrators that specify the rights available to them. Phoenix administrator roles are described below:
<table>
<thead>
<tr>
<th>Administrator role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud administrator</td>
<td>Cloud administrators can create organization administrators and additional Cloud administrators. Cloud administrators get all the rights available to the organization administrator. Cloud administrators for Druva Phoenix cannot access inSync services.</td>
</tr>
<tr>
<td>Organization administrator</td>
<td>Organization administrators can register servers under the organization they are assigned to, and configure them for backup and restore. Organization administrators can create group administrators, additional organization administrators and can access dashboards, servers, and reports of the assigned organization. Group administrators have restricted access to the associated administrative groups. They have necessary permissions for administrative group-related activities such as managing servers belonging to their administrative groups. One group administrator can manage multiple administrative groups. Similarly, more than one group administrator can manage a single administrative group.</td>
</tr>
</tbody>
</table>

Based on the administrator roles, rights are allocated to the administrators. For more information on roles and rights, see Predefined roles and rights.

## Create New Administrator

**Important:**
- Druva recommends that you create at least two members as Druva Cloud Administrator within your organization. A second Druva Cloud Administrator is required to reset the password if the primary Druva Cloud Administrator forgets the password.
- After you set your new password, ensure you keep the password secure and remember it. Druva does not have access to your data and cannot reset your account password if you forget it. Only the Druva Cloud Administrator and Cloud administrator can reset the password of other administrators in your organization.

If you are a Druva, inSync, or Phoenix Cloud administrator, perform the following steps to create a new administrator:

https://docs.druva.com/Druva_Cloud_Platform/020_Manage_Druva_Account/010_About_Druva_Administrators

Updated: Mon, 20 Sep 2021 05:55:37 GMT
Powered by
1. Launch a browser and
   ◦ For inSync Cloud, type https://login.druva.com in the address bar and press enter.
   ◦ On the login page, enter the email ID in the Email box and click Next.

2. If you have not configured SSO, enter the password and log in to Druva Cloud Platform Console.
   If you have configured SSO, you are taken to the identity provider page. Provide your credentials and login to Druva Cloud Platform Console.

3. Click the Druva logo to access the Global Navigation Panel > Manage Administrators. The Administrators page appears.


5. On the Create New Administrator page, provide Name, Email, Country, Time Zone, and select the Administrator Role.

6. Select Druva Cloud Administrator to create a Druva Cloud Administrator account.
   Select Product Administrator to create inSync and Phoenix administrator based on the roles and rights described in the inSync administrator and Druva Phoenix administrator sections above.

7. Select the Profiles from the dropdown for which you intend to provide access to the administrator.

8. After providing all the details, click Save. Druva sends an email to the specified email address, and the recipient can log in using the details mentioned in the email.

Administrators Page

The administrator page lists the administrators in an account, and only a Druva, inSync, or Phoenix Cloud administrator can access this page. It provides filters to easily segregate the administrators based on their role and a search bar to let a user easily find administrators and their information. In addition, this page provides the New Administrator button to add administrators to the account.

You can click on an administrator and navigate to the administrator details page. From the administrator details page, you can edit administrator settings such as name, country, time-zone, rights, and roles. You can also reset the password for the administrator and delete the administrator.

Details Page

To access the Administrators details page:

1. Click

   to access the Global Navigation Panel > Manage Administrators. The Administrators page appears.

2. Click on the administrator you want to see or update. The administrators details page appears that shows the information about the selected administrator.

   To see your account details, click
> your user ID. For example,

**Important** The administrator details page for Cloud administrators in Druva Phoenix displays rights to access the Druva Cloud settings, however, the Cloud administrators cannot make any modifications to the Druva Cloud settings.

**Summary**

Provides administrator information such as the email ID, country, time-zone, administrator role, and who added the user as an administrator.

**inSync rights**

For Druva Cloud Administrators, all inSync rights are available, the administrator can use all profiles, and has access to all Legal Hold policies. However, rights are disabled for administrators in inSync with different roles. For example, administrators with role specified as View Only cannot access profiles. For more information, see Predefined roles and rights. Few rights are exclusive to Cloud Administrators and Legal Administrators. For more information, see Exclusive rights for Cloud Administrators and Legal Admins.

If the role in the summary section is defined as Cloud Administrator, Phoenix rights sections are not available for the administrator.

**Phoenix rights**

For Druva Cloud Administrators, all Druva Phoenix rights are already available and the role is Cloud Administrator. Druva Cloud Administrator can access all organizations and use all Druva Phoenix services enabled for the account. However, access control only shows the organization allocated to the administrator if the administrator's role is specified as Organization administrator.

If the role in the summary section is defined as Cloud Administrator, inSync rights sections are not available for the
Edit

Use the Edit button to change details such as name, country, time-zone, rights, and roles. Options to change the details are based on the rights available to the administrator who can access the details page.

Change Password

To change the password associated with your account, do the following steps:

1. Click the Change Password button. The Change Password window appears.
2. In the Enter current Password box, type your current password.
3. In the Enter new Password box, type your new password.
4. In the Re-enter new Password box, type the same password that you provided in step 3.

   Note: The password can be only changed in accordance with the Password Policy configured for your organization.

5. Click Ok.

Reset Password

Important: After you set your new password, ensure you keep the password secure and remember it. Druva does not have access to your data and cannot reset your account password if you forget it. Only the Druva Cloud Administrators and Cloud administrators can reset the password of other administrators in your organization.

To reset the password associated with the other administrator's account, do the following steps:

1. Click to access the Global Navigation Panel > Manage Administrators. The Administrators page appears.
2. Click the administrator for whom you want to reset the password.
3. Click Reset Password.
4. Click Yes in the message window displayed. Druva Cloud Platform Console sends an email to the administrator, with the necessary details to reset the password.
Important: An email containing a link to reset the password is sent to the administrator and is valid for 24 hours only. If the password link expires before the password is reset, the administrator can resend the invitation email.