CENTRIFY DEPLOYMENT GUIDE

Centrify for Dropbox Deployment Guide

Abstract

Centrify provides mobile device management and single sign-on services that you can trust and count on as a critical component of your corporate identity and access infrastructure. Our thorough approach to availability, reliability, scalability, security and privacy ensures that you can depend on Centrify as a trusted partner and provider.

Contents

Overview 4
Prerequisites 4
To configure Dropbox for single sign-on overview: 5
Configuring Dropbox for SSO 5
To configure Dropbox for SSO: 5
Introduction and overview of Dropbox provisioning 13
Configuring Dropbox for automatic user provisioning (an overview): 13
Preparing your Dropbox account for provisioning 13
Configuring Dropbox in Cloud Manager for automatic provisioning 14
To configure Dropbox in Cloud Manager for automatic provisioning: 14
Provisioning users for Dropbox based on roles 15
To automatically provision users with Dropbox accounts: 16
Optional configurations for the Dropbox web application in Cloud Manager 20
How your users link their computers and mobile devices to Dropbox 23
Linking a computer to Dropbox 23
Linking a mobile device to Dropbox 23
Contact Centrify 24

Overview

Dropbox is the secure file sharing and storage solution that employees love and IT admins trust, while you maintain complete control over important company information and user activity. Files in your Dropbox folder stay updated on every device linked to your account. Save something on your laptop, and it automatically syncs to your desktop computer, as well as your iOS, Android, Windows, or Blackberry mobile devices.

Centrify enables quick and secure deployment of Dropbox. Centrify integrates with Active Directory and other user directories, to provide users with single sign-on to their applications with their most current credentials. IT can provision cloud and on-premises applications and resources for new employees from within Dropbox - based on their standard login.

Centrify is the leader in securing enterprise Identities against cyber threats, the predominant cause of breaches. Centrify enables organizations to use their existing infrastructure to manage a wide range of identity-related IT activities — including authentication, access control, privilege management, policy enforcement and compliance — across both cloud and data center based resources.

- Eliminate Complexity, Save Time and Improve Security.
- Simplify Dropbox access by providing a single username and password across Dropbox and all other apps.
- Get one-click access to all apps, without the integration hassles.
- Improve security by eliminating the use of easy-to-remember, reused and/or improperly stored passwords.
- Reduce helpdesk volume from forgotten passwords and device enrollment with user self-service.
- Reduce end-user frustration, and boost IT satisfaction.
- Save time by automatically creating or updating user accounts within Dropbox.
- Improve efficiency by deploying the right apps the first time, with SSO.
- Improve security with automatic role-based permissions within Dropbox.
- See who has access to which apps, how they received access, and when changes occurred.
- Prevent unauthorized access by automatically revoking access to all Dropbox apps at once.
- Provide a consistent user experience for all IT related tasks for end users and IT-users.

Prerequisites

- Active DropBox account.
- Active Centrify Identity Service Account.

To configure Dropbox for single sign-on overview:

1. Prepare Dropbox for SSO:

- Verify that you have a Dropbox for Business account.

2. Configure Dropbox for SSO. For details, see Configuring Dropbox for SSO.
3. Add, configure, and deploy the Dropbox web application in Cloud Manager. For details, see Configuring the Dropbox web application in Cloud Manager.
4. Configure Cloud Manager for automated account provisioning.
5. Your users are ready to launch Dropbox from the user portal.
6. As needed, have your users link or re-link their computers or mobile devices to Dropbox. For details, see How your users link their computers and mobile devices to Dropbox.

Configuring Dropbox for SSO

- You need administrator privileges in Dropbox to perform these steps.

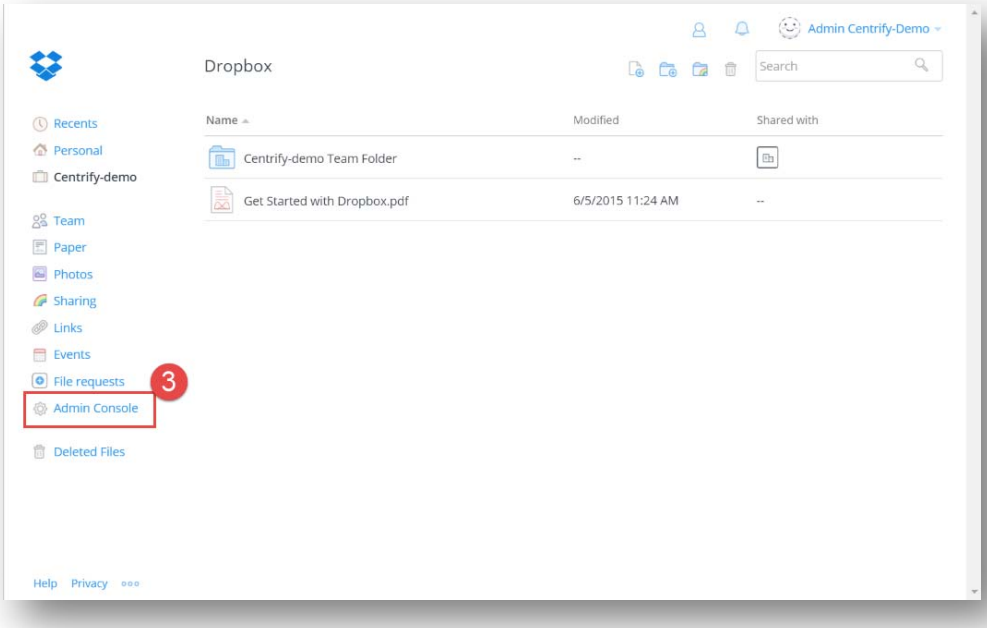
Note: If you plan on using the certificate generated by Cloud Manager, go log in there first and download the certificate before continuing. Also copy the Identity Provider's Sign-in URL from the application settings in the Cloud Manager so that you can paste the URL into Dropbox's configuration page.

Tip: It can be useful to open the web application and Cloud Manager simultaneously and have them both open, perhaps side by side. As part of the SSO configuration process, **you'll need to copy and paste settings between the two browser windows**.

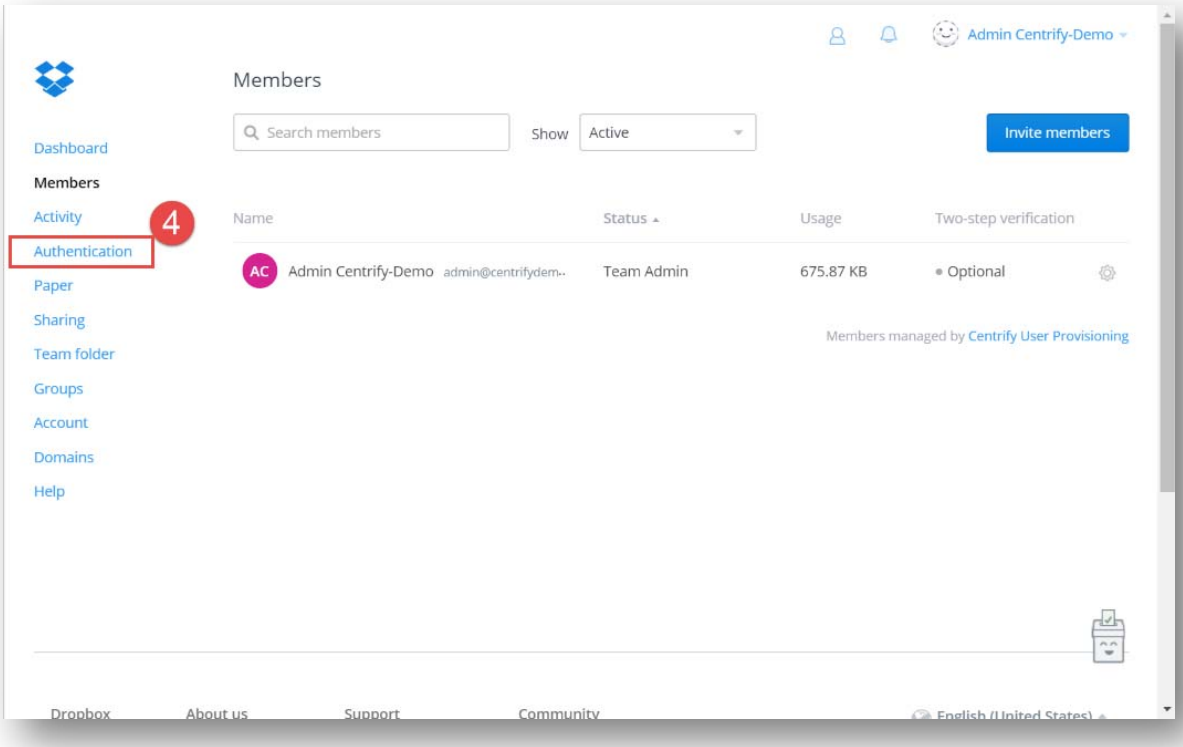
- When you require SSO for Dropbox, two-step verification is automatically disabled to avoid overlapping settings.

To configure Dropbox for SSO:

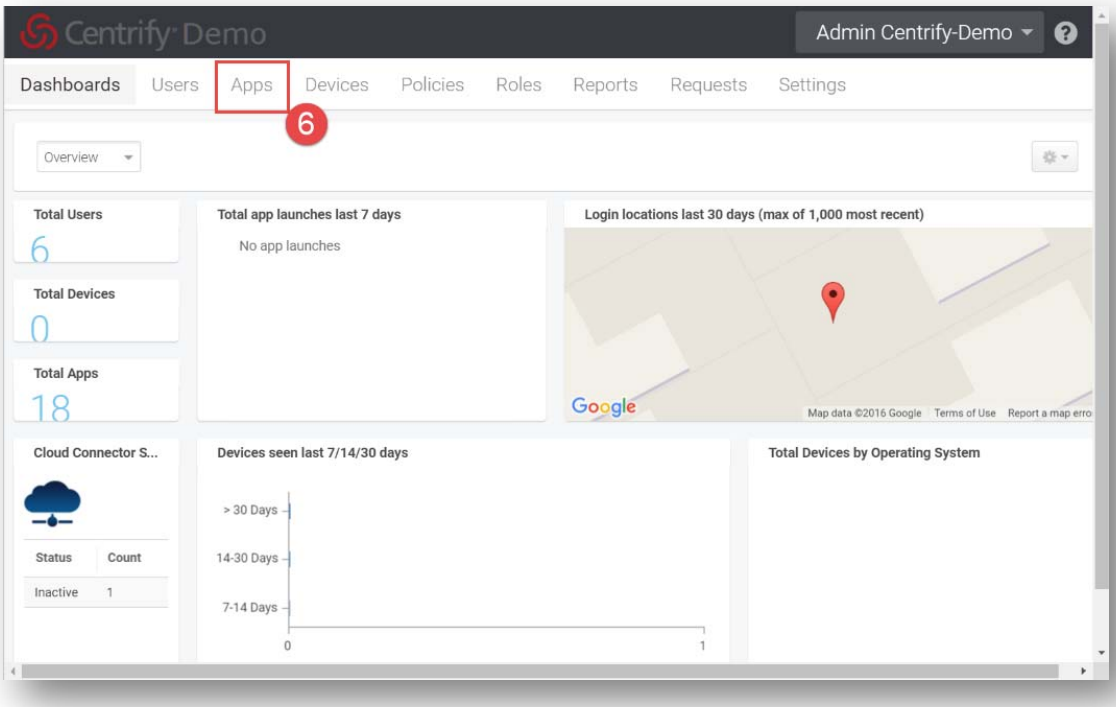
1. In your web browser, go to https://www.dropbox.com and https://cloud.centrify.com/manage
2. In the Dropbox browser click **Sign in**, enter your administrative user name and password, and click **Sign in.**
3. Click **Admin Console.**



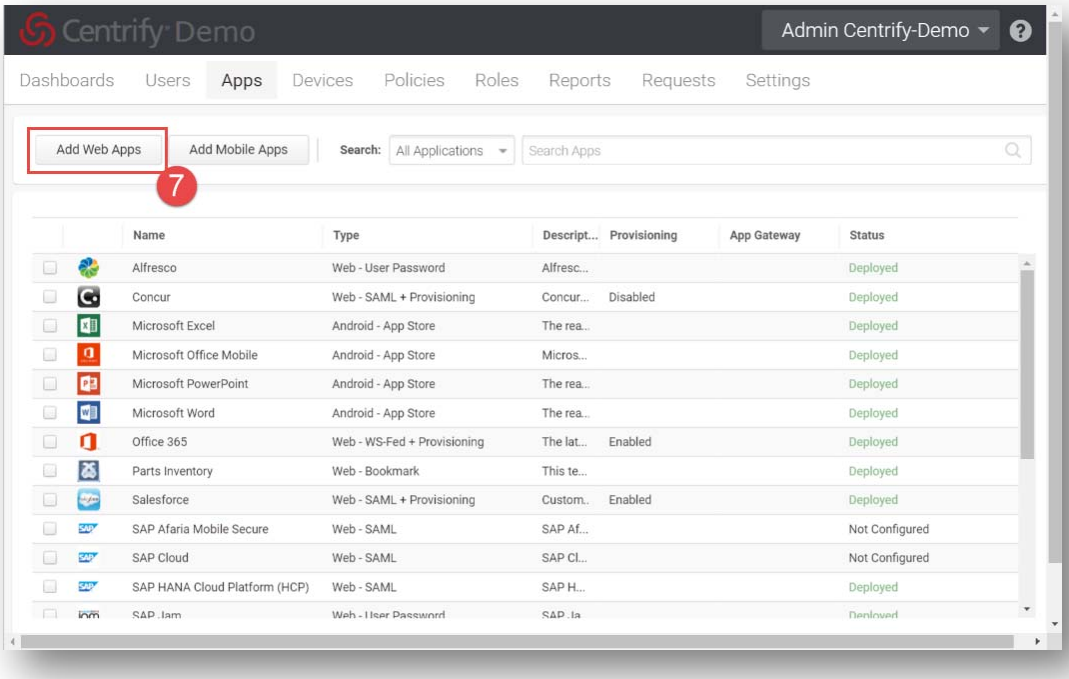
4. Click **Authentication.**



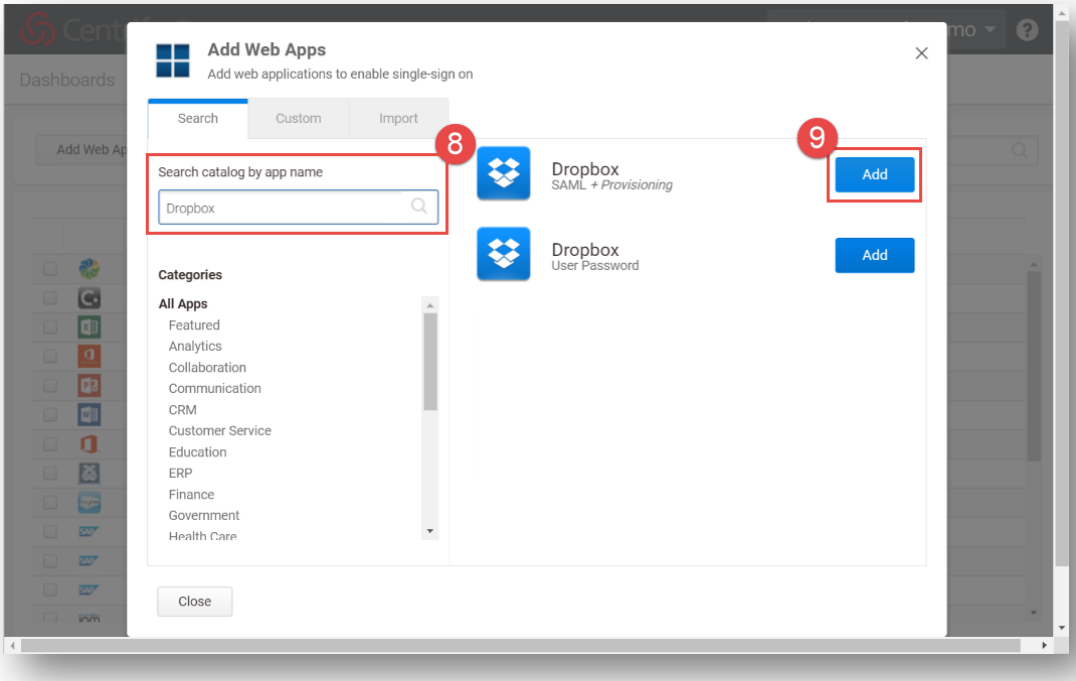
5. In the Centrify browser enter your **administrative username and password and sign in**.
6. Click on **Apps.**



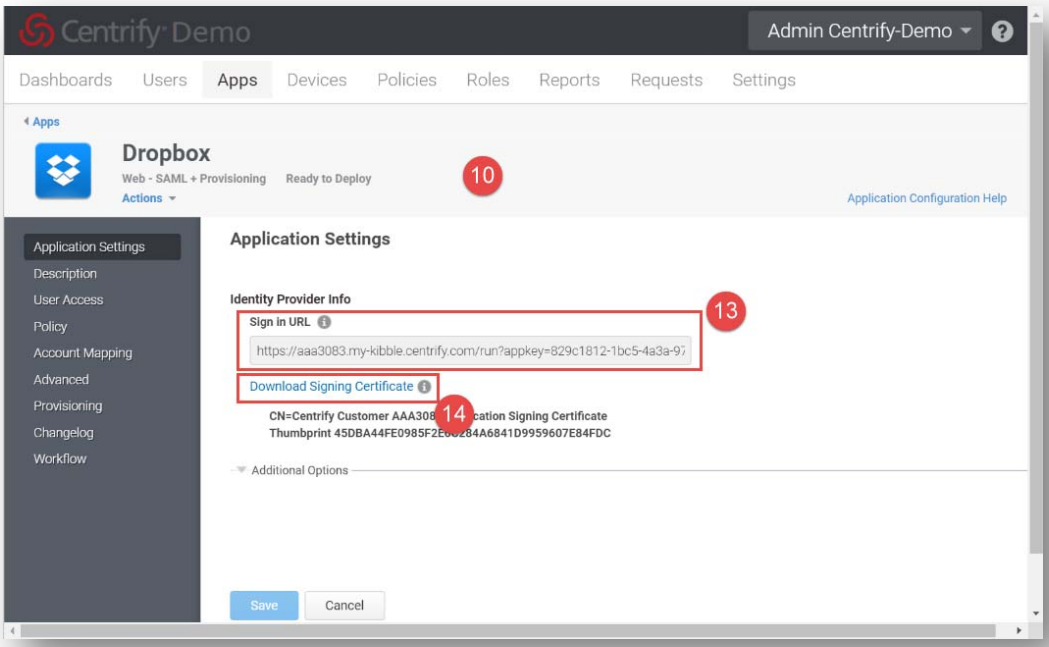
7. Click on **Add Web Apps.**



8. Search for **Dropbox.**
9. Click on **Add** for **Dropbox SAML + *Provisioning*.**

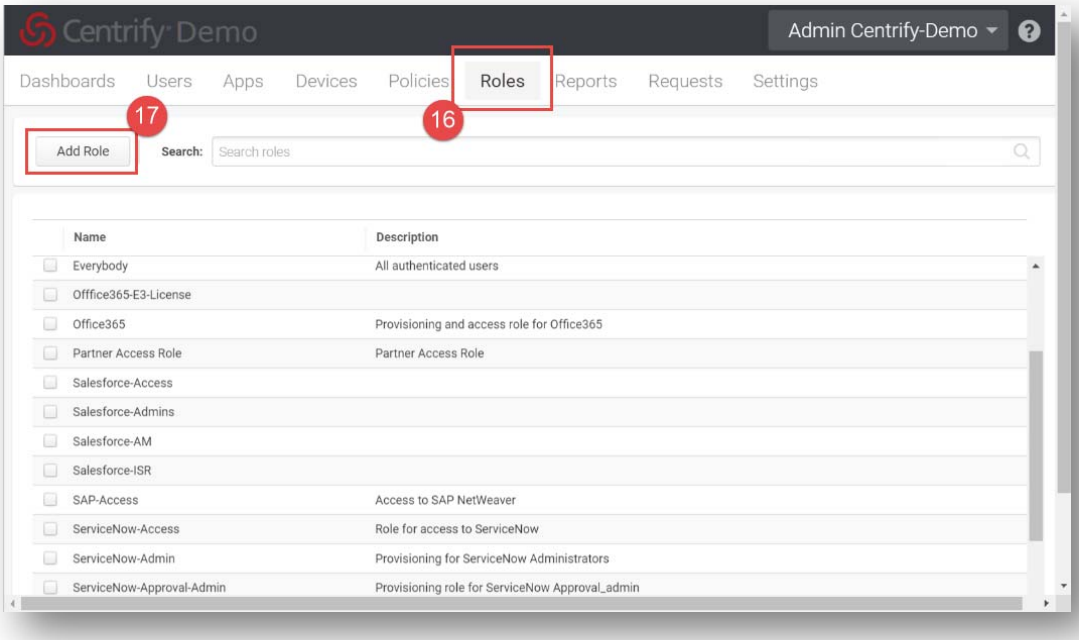


10. Confirm any dialog prompt and close the Add Web Apps dialog window. The Dropbox configuration window will open automatically.

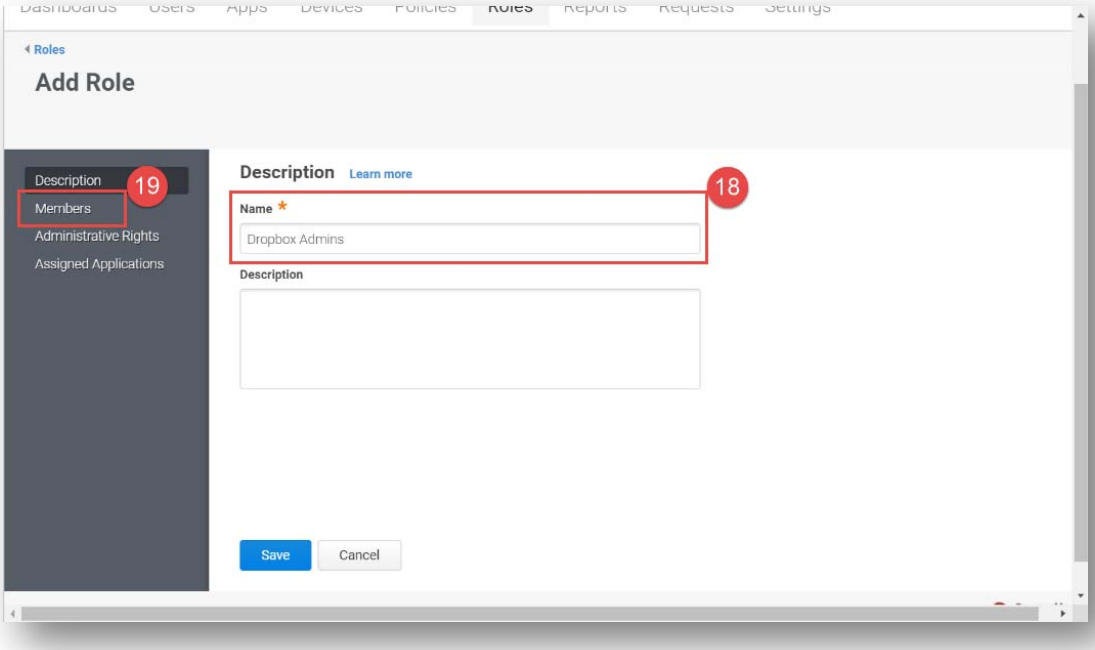


11. Back in the **Dropbox** browser window select **Enable Single Sign On.**
12. Select either **Optional** or **Required** based on your requirements.
13. **Copy** the **Sign in URL** from the Centrify App dialog into the Sign in URL field.
14. Download the Signing Certificate from the Centrify App dialog and upload the Certificate to Dropbox.
15. Click Save changes.

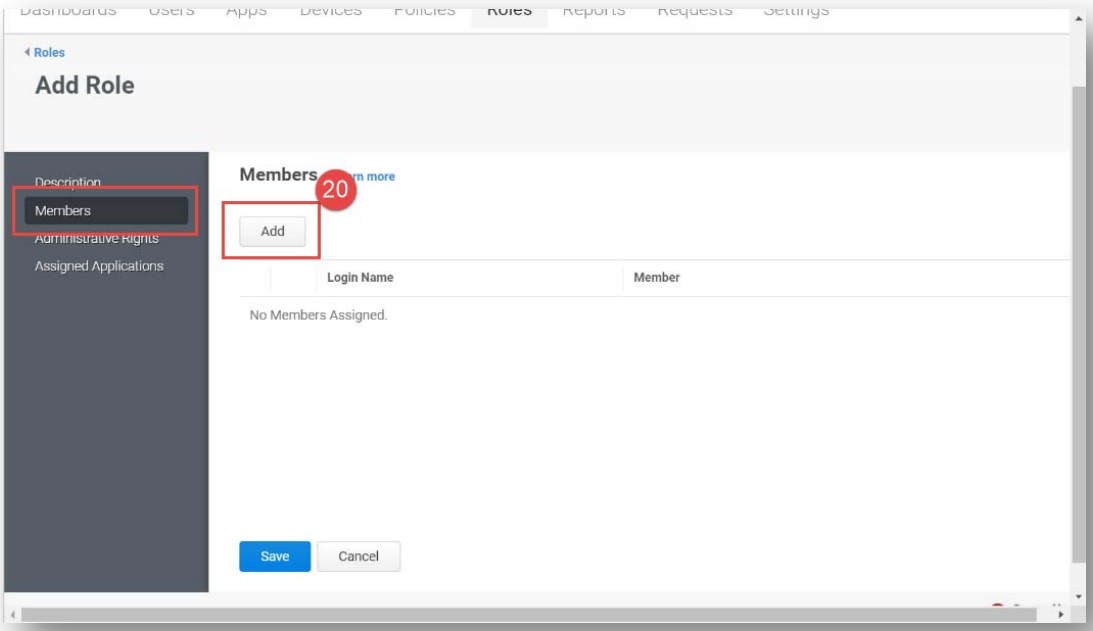
16. Back in the Centrify Cloud Manager click on **Roles.**
17. Click on **Add Role.**



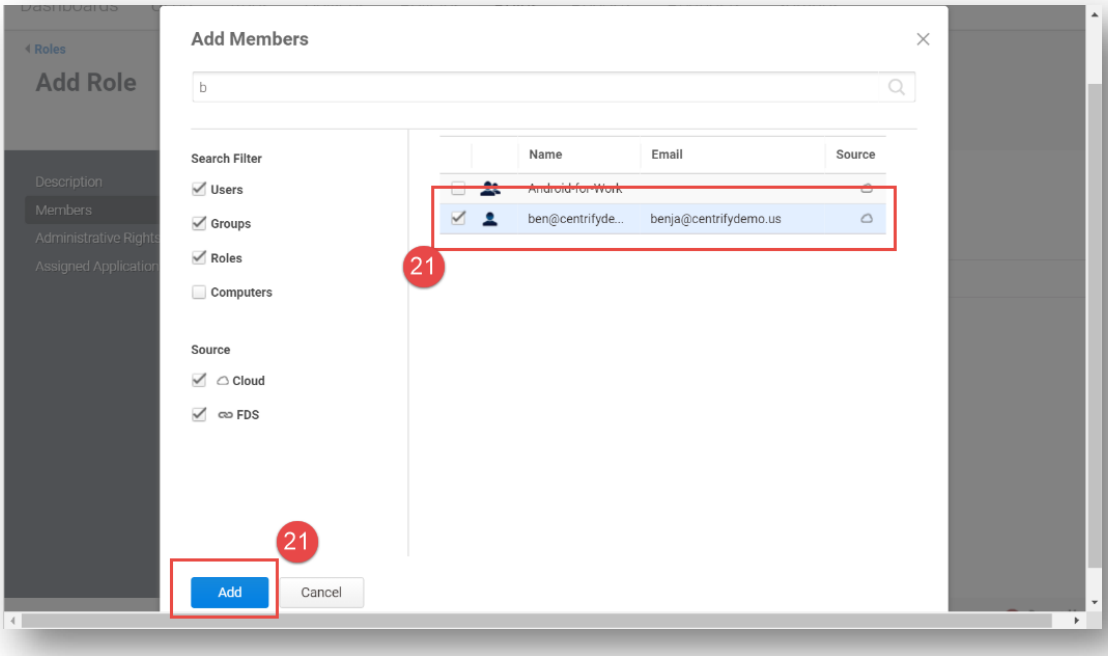
18. Enter a **Role name**. For best practice it is suggested to create Centrify Roles that correspond to the Dropbox groups configured. This will make it easier to automatically provision users into Dropbox.
19. Click on **Members.**



20. Click on **Add.**

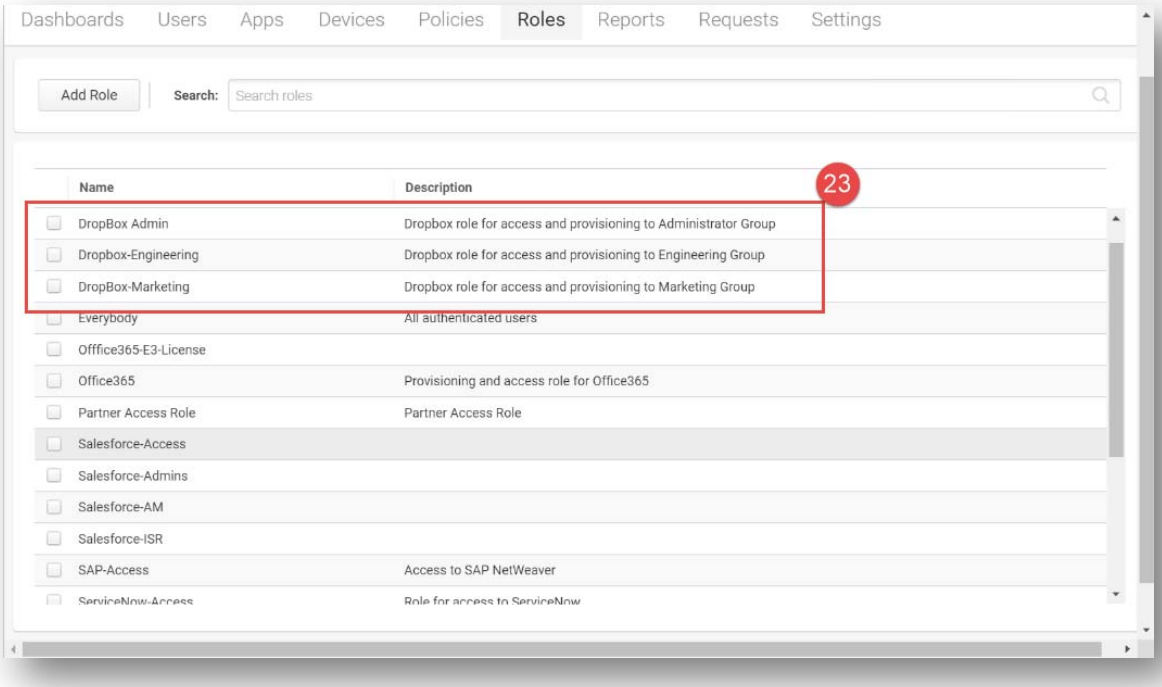


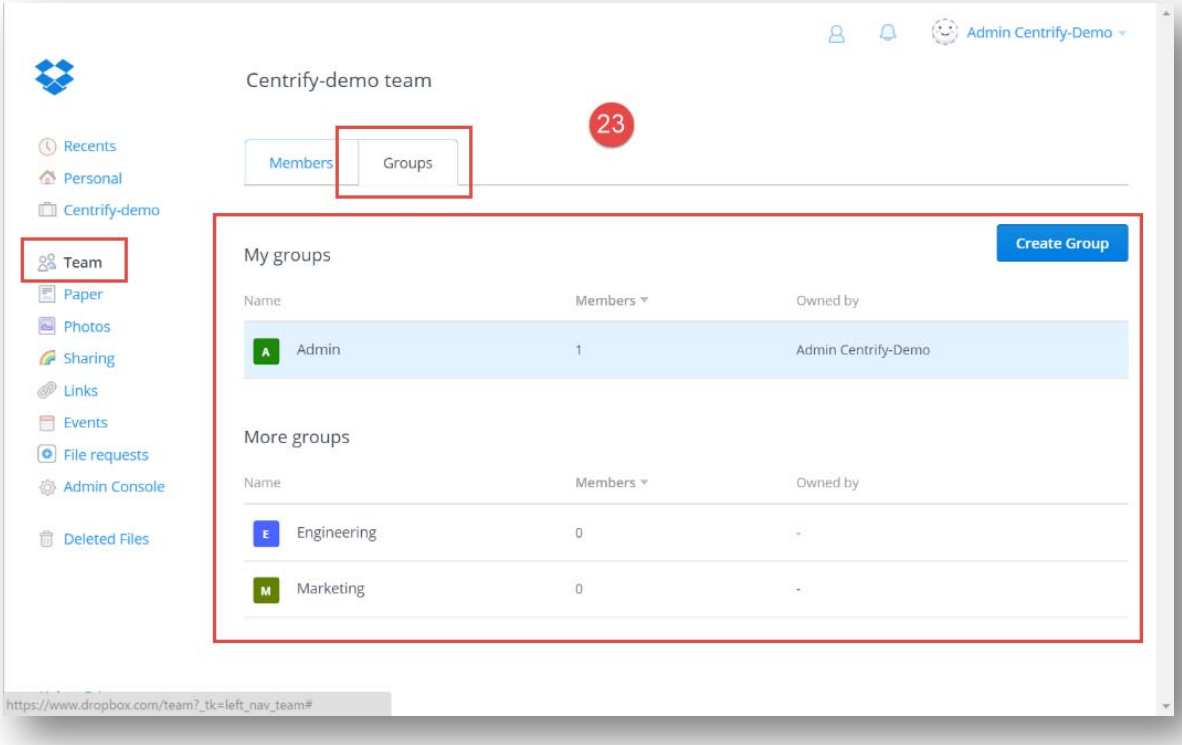
21. In the Add Members dialog select the individuals you want to add to the Role just created and click on **Add.**



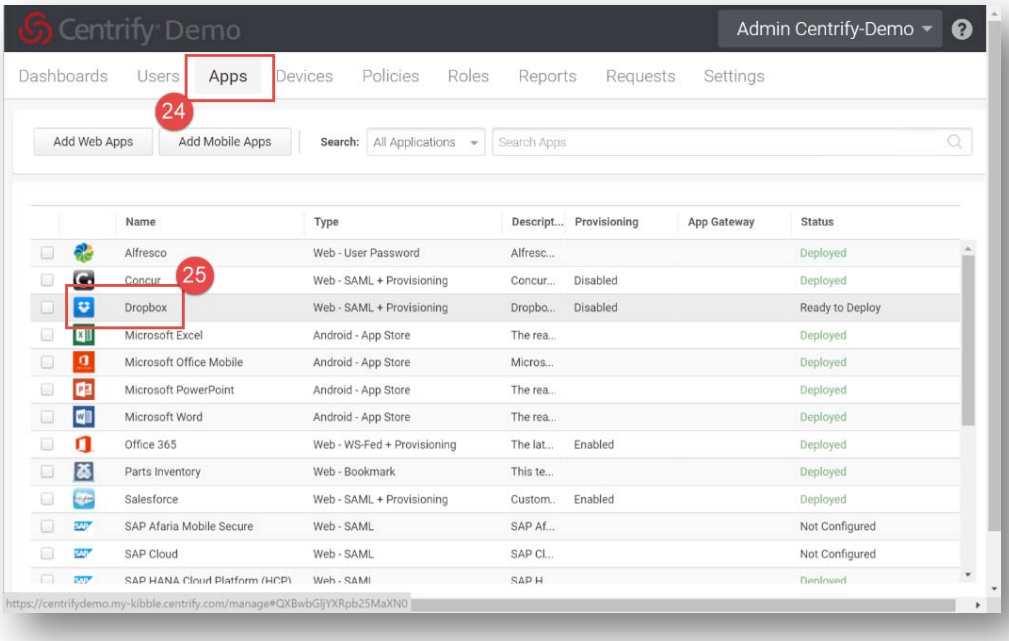
22. Repeat steps 20 and 21 until you added all individuals to the group.

23. Repeat steps 17 through 22 until you created all the Groups corresponding to your Dropbox Groups.



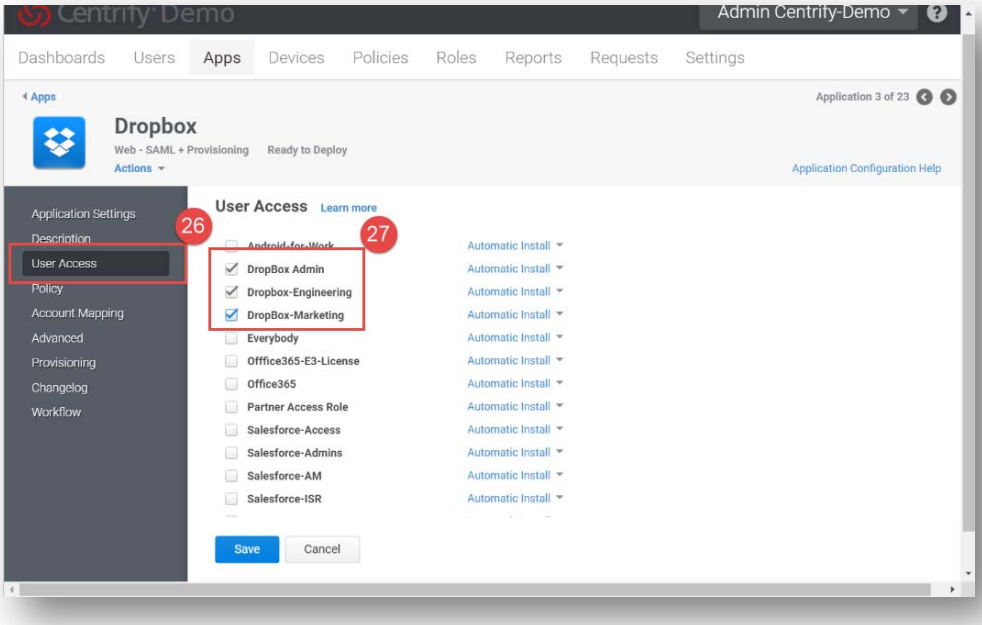


24. Click on **Apps.**
25. Click on **Dropbox.**



26. Within the Application configuration dialog click on **User Access.**
27. Select all the **Dropbox roles** that are **granted to access Dropbox.**

- When assigning an application to a role, select either **Automatic Install** or **Optional Install**:
- Select **Automatic Install** for applications that you want to appear automatically for users.
- If you select **Optional Install**, the application doesn't automatically appear in the user portal and users have the option to add the application.



Introduction and overview of Dropbox provisioning

For Dropbox, the overall workflow of configuring provisioning is as follows. You must have a Dropbox for Business account in order to enable provisioning.

Configuring Dropbox for automatic user provisioning (an overview):

1. In Cloud Manager, you configure the Dropbox application for automatic user provisioning:
2. In the Dropbox application in Cloud Manager, you enable provisioning and authorize the Cloud Manager to provision users for your account.
3. You add the role mappings and specify how to handle updates to existing Dropbox user accounts.
4. Make sure that provisioning is working as desired.
5. Run preview synchronizations in Cloud Manager, review the synchronization reports, and review the list of users in Dropbox. Make changes as needed to get the desired provisioning results.
6. Configure the Dropbox application provisioning for Live mode.

Preparing your Dropbox account for provisioning

- Here are a couple other things to know about Dropbox provisioning:
- When the OAuth access token for provisioning expires, a notice is displayed on the provisioning page of Dropbox and included in directory synchronization emails. When this happens, you need to re-authorize Centrify to continue provisioning users for the Dropbox accounts.
- Dropbox provisioning can update existing user accounts only if the user is already active.
- Users activate their Dropbox accounts; administrators cannot activate a user account. Users click a link in an email invitation to activate their account. You can check the status of users in Dropbox by opening the Admin Console and going to the Members page.
- Dropbox provisioning supports user creation and user deletion.
- The current version of Dropbox provisioning APIs doesn’t support user activation nor user licensing, and the APIs support a subset of available user attributes.
- Provisioned users are assigned as “user” or “admin” in Dropbox.
- When a user is deprovisioned, the user is removed as a team member in the Dropbox account.The user’s files are deleted and not transferred to another member.

Configuring Dropbox in Cloud Manager for automatic provisioning

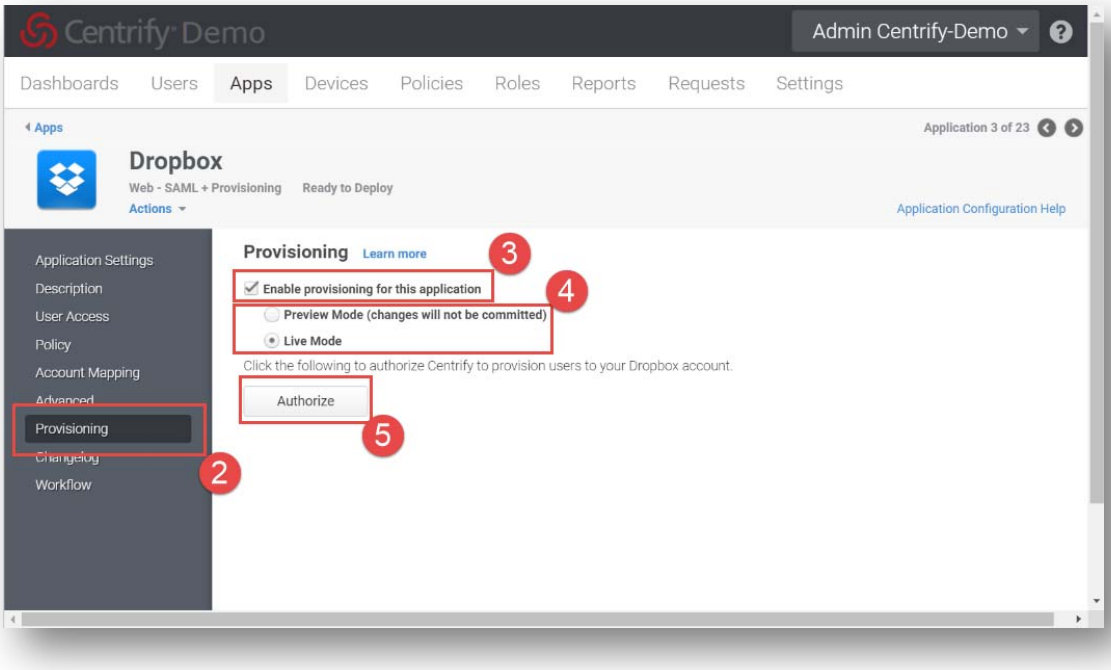
This section describes how to authorize Cloud Manager to provision users into your Dropbox account.

To configure Dropbox in Cloud Manager for automatic provisioning:

1. In Cloud Manager, add, configure, and deploy the Dropbox SAML application. For details, see the previous chapter
2. Click the Provisioning tab.
3. On the application's **Provisioning** tab.
4. Select **Enable provisioning** for this application.
5. Select either **Preview Mode** or **Live Mode**.

- **Preview Mode**: Use Preview Mode when you're initially testing the application provisioning or making configuration changes. The cloud service does a test run to show you what changes it would make but the changes aren't saved.
- **Live Mode**: Use Live mode when you want to use application provisioning in your production system. The cloud service does the provisioning run and saves the changes to both the cloud service and the application's account information.

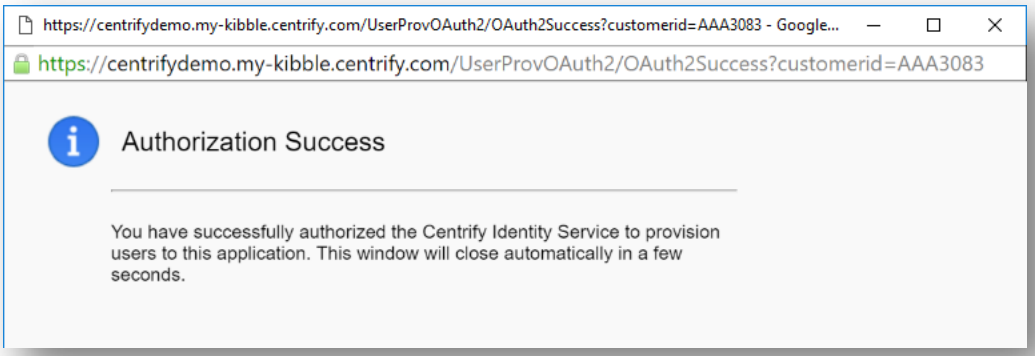
6. Click **Authorize** to authorize the Cloud Manager to provision users for your Dropbox account.



- The Dropbox authorization window appears.

7. If requested, authorize the application for your Dropbox account.

- Once successful, the Authorization Success screen is displayed in the Dropbox authorization window. The window closes automatically in a few seconds and the Provisioning tab displays the Role Mappings section. The Authorize button changes to Re-authorize, indicating that users have already been provisioned to the Dropbox account or that the access token has expired and requires you to re-authorize to continue provisioning users. Next, you're ready to configure Dropbox provisioning based on roles.



Provisioning users for Dropbox based on roles

- Here you specify a Cloud Manager role and specify that users in that role will be matched to existing or new accounts in Dropbox with the roles that you specify.
- When you change any role mappings, the cloud service synchronizes any user account or role mapping changes immediately.

Note: How the cloud service determines duplicate user accounts:

If the user accounts in the cloud service and the target application match for the fields that make a Dropbox user unique, then the cloud service handles the user account updates according to your instructions. In many applications, the user's email address or Active Directory userPrincipalName is the primary field used to identify a user—and in many cases, the userPrincipalName is the email address. You can look at the application's provisioning script to see the fields that the cloud service uses to match user accounts.

To automatically provision users with Dropbox accounts:

1. In the Provisioning page, go to the **Role Mappings** section.
2. Specify how the cloud service handles situations when the cloud service determines that the user already has an account in the target application; **select either Overwrite or Keep**.

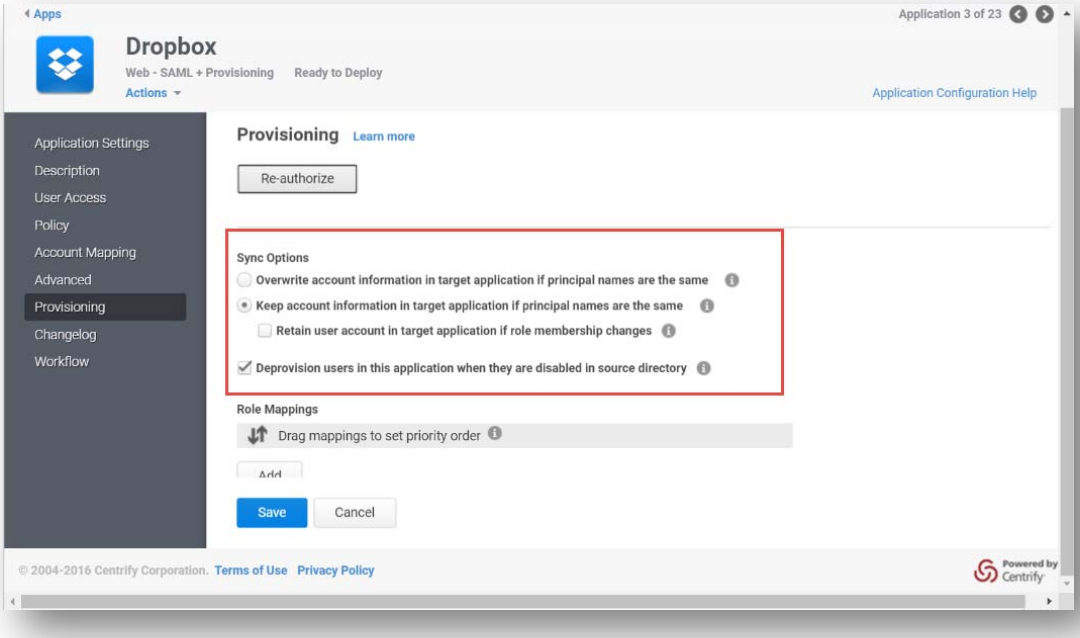
- **Overwrite**: Select Overwrite to update and overwrite the target application user account information with the cloud user account information.

Note: If the target user account has a value for a user attribute that doesn't exist in the cloud user account, then the cloud service leaves that target user account attribute value intact.

Keep: Select Keep to keep the target user account as it is; the cloud service skips and doesn't update the duplicate user account in the application.

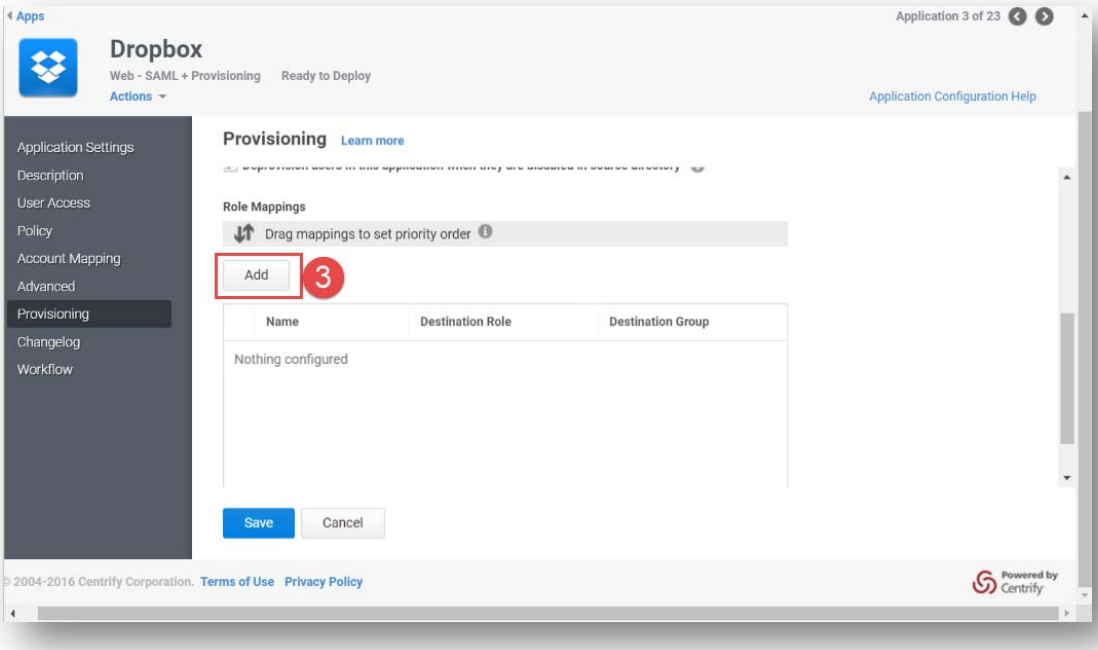
Retain: If you select Keep, you can also select Retain to keep the existing target application user account active when changes in roles or role mappings result in the user no longer being assigned and provisioned to the application. To deprovision users when the user is no longer assigned and provisioned to the application, do not select this option.

- Select **Deprovision users in this application when they are disabled in source directory** to enable the feature.
- When a user is disabled in a source directory, such as Active Directory, a deprovisioning job is created to deprovision the user in the application.



3. To add role mappings and specify which users get provisioned to this application, click **Add**.

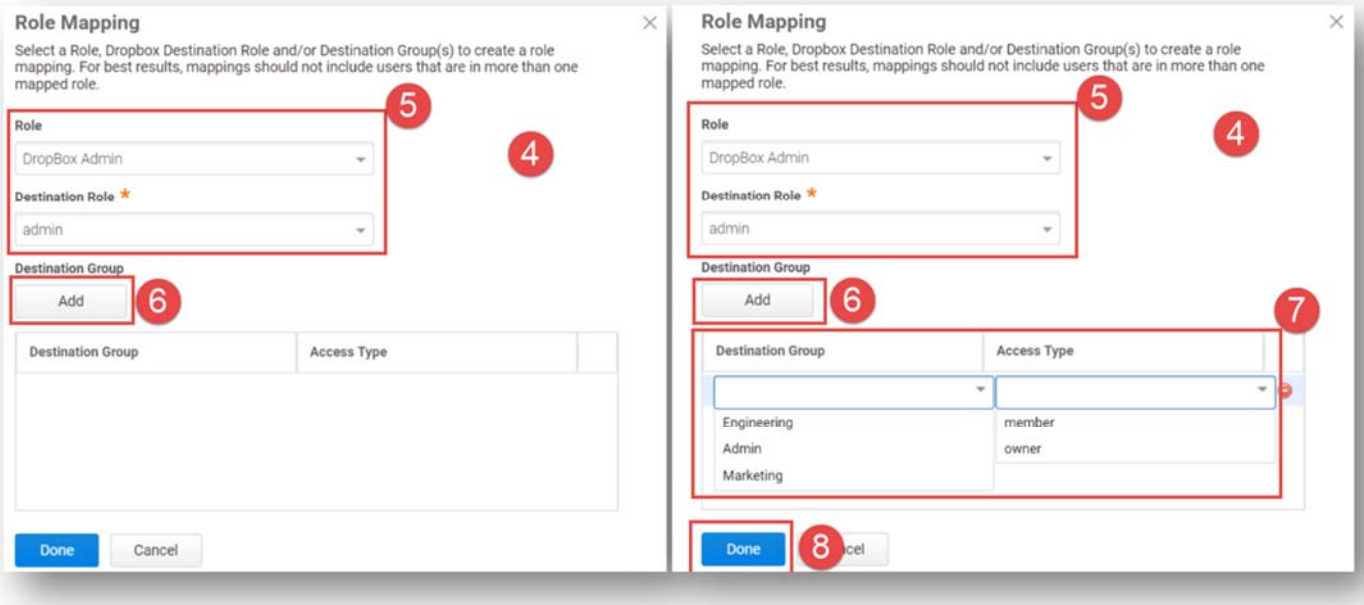
- The Role Mapping dialog box opens.



4. To map user accounts in Cloud Manager to Dropbox user accounts, select a **Cloud Manager role** and a **Dropbox Destination Role** and (optionally) **Dropbox Destination Groups**:
5. Select a **Role** (the ones in Cloud Manager) and a **Destination role** (the ones in Dropbox).
6. Optionally, select a Dropbox **Destination Group**. Click on **Add** under Destination Group
7. Select the appropriate Destination Group and Access Type from the Destination Group and **Access Type** (owner or member) from the list of groups you already created in Dropbox. The Destination Group is used to manage users and their resources in Dropbox and the Access Type sets the permission level for the group. To add more groups to the role click **Add**. One role can be mapped to multiple destination groups in Dropbox.
8. Click **Done** to save the role mapping and return to the Provisioning page.

Tip: If you change your mind, click the red icon to the right of the Dropbox Destination Group to remove the group from the role mapping.

Note: Users can only be added to a destination group if the user has accepted the Dropbox invitation and the account is activated. After the user has activated the account manually in Dropbox, synchronize the Dropbox application from the **Settings> Provisioning** tab in Cloud Manager to associate the user with destination groups. See Synchronizing user accounts with provisioned applications.



9. Continue adding role mappings, as desired.

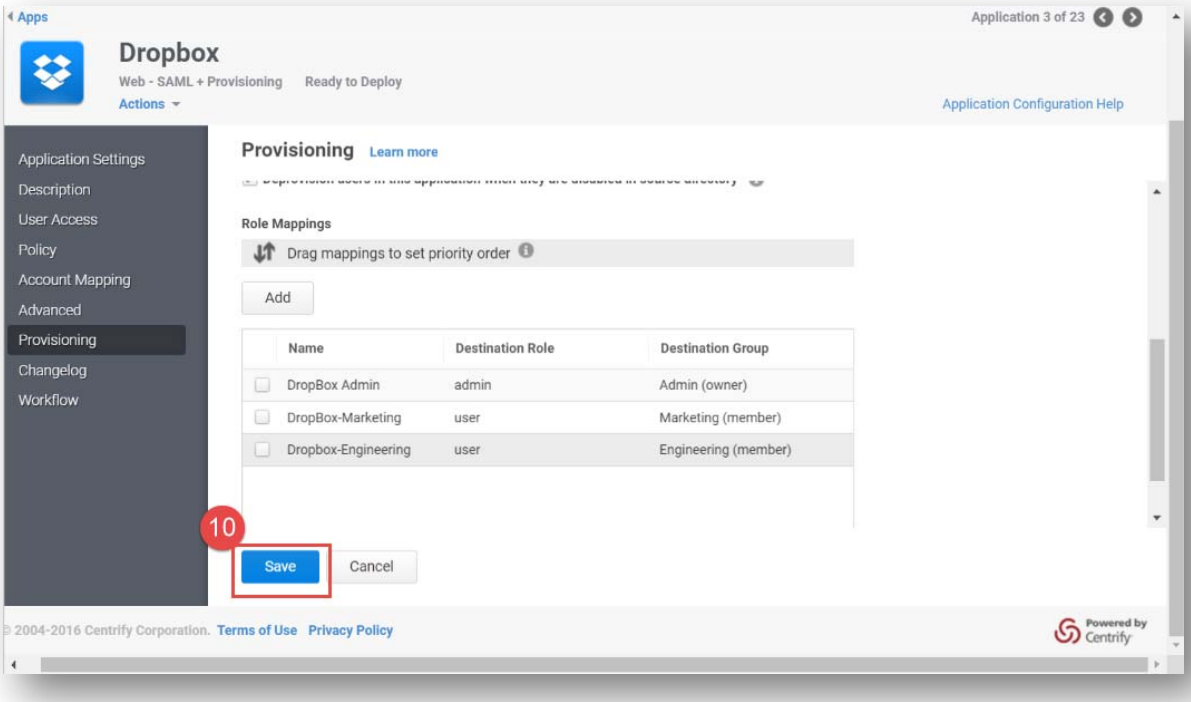
- To change a mapping, select the role mapping and click **Modify**.
- To remove a mapping, select the role mapping and click **Delete**.
- To change the order of the role mappings, select the role mapping that you want to move higher in the list and click **Move Up**.

Tip: Provisioning assigns users access and assignments based on the top-most role mapping. The order in which the roles display in the Role Mappings section matters. The role at the top of the list has priority when provisioning users. For instance, if a user is in multiple roles that you've mapped for provisioning, the cloud service provisions the user based on the role nearer the top of the list. For best results, assign roles where users are only in one role. For more details, see Setting up provisioning.

Note: The provisioning script is intended for advanced users who are familiar with editing server-side JavaScript code.

10. When you're done, click **Save** to save the provisioning details.

- Anytime that you make changes to the provisioning role mapping, the cloud service runs a synchronization automatically. You can also run a preview synchronization or a real synchronization, if desired.



Optional configurations for the Dropbox web application in Cloud Manager

1. On the **Application Settings** page, click **Enable Derived Credentials for this app on enrolled devices (opens in built-in browser)** to use derived credentials on enrolled mobile devices to authenticate with this application.

- For more information, see *Derived Credentials*.

2. On the **Application Settings** page, expand the **Additional Options** section and specify the following settings:

Option	Description
Application ID	Configure this field if you are deploying a mobile application that uses the Centrify mobile SDK, for example mobile applications that are deployed into a Samsung KNOX version 1 container. The cloud service uses the Application ID to provide single sign-on to mobile applications. Note the following: ●The Application ID has to be the same as the text string that is specified as the target in the code of the mobile application written using the mobile SDK. If you change the name of the web application that corresponds to the mobile application, you need to enter the original application name in the Application ID field. ●There can only be one SAML application deployed with the name used by the mobile application. The Application ID is case-sensitive and can be any combination of letters, numbers, spaces, and special characters up to 256 characters.
Show in User app list	Select **Show in User app list** so that this web application displays in the user portal. (By default, this option is selected.) If this web application is only needed in order to provide SAML for a corresponding mobile application, deselect this option. This web application won't display for users in the user portal.
Security Certificate	These settings specify the signing certificate used for secure SSO authentication between the cloud service and the web application. Just be sure to use a matching certificate both in the application settings in the Cloud Manager and in the application itself. Select an option to change the signing certificate. ●**Use existing certificate** When selected the certificate currently in use is displayed. It's not necessary to select this option—it's present to display the current certificate in use. ●**Use the default tenant signing certificate** Select this option to use the cloud service standard certificate. This is the default setting. ●**Use a certificate with a private key (pfx file) from your local storage**

- Select this option to use your organization's own certificate. To use your own certificate, you must click **Browse** to upload an archive file (.p12 or .pfx extension) that contains the certificate along with its private key. If the file has a password, you must enter it when prompted.
- Upload the certificate from your local storage prior to downloading the IdP metadata or the Signing Certificate from the Applications Settings page. If the IdP metadata is available from a URL, be sure to upload the certificate prior to providing the URL to your service provider.

3. On the **Description** page, you can change the name, description, and logo for the application. For some applications, the name cannot be modified.

- The Category field specifies the default grouping for the application in the user portal. Users have the option to create a tag that overrides the default grouping in the user portal.

4. On the **Policy** page, specify additional authentication control for this application.You can select one or both of the following settings:

- **Restrict app to clients within the Corporate IP Range**: Select this option to prevent users outside the company intranet from launching this application. To use this option, you must also specify which IP addresses are considered as your intranet by specifying the Corporate IP Range. To specify the Corporate IP Range, you have to leave the Apps section in Cloud Manager by clicking **Settings** at the top of the page.Then navigate to**Network > Corporate IP Range**, then click **Add** and enter one or more IP addresses or ranges.
- **Require Strong Authentication**: Select this option to force users to authenticate using additional, stronger authentication mechanisms when launching an application. To specify these mechanisms, you have to leave the Apps section in Cloud Manager by clicking **Policies** at the top of the page. Then navigate to **Add Policy Set > User Security Policies > Login Authentication**. Choose **Yes** for **Enable Authentication Policy Controls** and add authentication rules.
- You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require additional authentication methods. For details, see Application access policies with JavaScript.

Note: If you left the Apps section of Cloud Manager to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Cloud Manager.

5. On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts. The options are as follows:

- **Use the following Directory Service field to supply the user name**: Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from the Centrify cloud directory.
- **Everybody shares a single user name**: Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
- **Use Account Mapping Script**: You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:
    - LoginUser.Username = LoginUser.Get('mail')+'.ad';
- The above script instructs the cloud service to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the user's mail attribute value is Adele.Darwin@acme.com then the cloud service uses Adele.Darwin@acme.com.ad. For more information about writing a script to map user accounts, see the SAML application scripting.

6. (Optional) On the **Advanced** page, you can edit the script that generates the SAML assertion, if needed. In most cases, you don't need to edit this script. For more information, see the SAML application scripting.
7. (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.
8. Click **Workflow** to set up a request and approval work flow for this application.

- The Workflow feature is a premium feature and is available only in the Centrify Identity Service App+ Edition. See Configuring Workflow for more information.

9. Click **Save**.

- After configuring the application settings (including the role assignment) and the application's web site, you're ready for users to launch the application from the user portal.

How your users link their computers and mobile devices to Dropbox

- After you've configured your Dropbox account for single sign-on, your users can link computers and mobile devices to their Dropbox account using single sign-on.
- If an existing user has a computer or mobile device currently linked to Dropbox, that link remains intact. There is no need to re-link.
- If the user is new, or if the existing user needs to create a new link or re-link an existing computer or mobile device, the user needs to install the latest version of the Dropbox software and link it to the Dropbox service.

Linking a computer to Dropbox

To link or re-link a computer to Dropbox:

1. Launch the Dropbox application on your computer (not the web application).
2. In Dropbox, enter your email address only to login. (Leave the password field blank).

Note: If Dropbox SSO is configured as Optional, you can log in using either your Dropbox user name and password or your work email address (and then to the user portal). If you use your Dropbox user name and password, Dropbox links your computer directly.

3. Enter your computer name and click **Next**.
4. In the Dropbox application on your computer, click the **Get your link code** to get the Dropbox link code.

- Dropbox opens the user portal in your default web browser and logs you in to Dropbox.
- In the Dropbox web application, the link code displays. Copy this link code and paste it into the Dropbox application running on your computer. After linking, the Dropbox application on the computer stays linked to the account.

Linking a mobile device to Dropbox

To link or re-link a mobile device to Dropbox:

1. Open the Dropbox application on your mobile device (not the web application).
2. Enter your email address (leave the password field blank) and tap **Log in**.

Note: If Dropbox SSO is configured as Optional, you can log in using either your Dropbox user name and password or your work email address (and then to the user portal). If you use your Dropbox user name and password, Dropbox links your device directly.

- Dropbox opens the user portal in your default web browser and logs you in to Dropbox.

3. Your web browser opens to a page that requests your approval for the application to use single sign-on. Tap **Allow**.

- Dropbox then presents a series of configuration screens for you; you're connected to Dropbox and authenticated by way of the user portal.

Contact Centrify

Centrify strengthens enterprise security by managing and securing user identities from cyber threats. As organizations expand IT resources and teams beyond their premises, identity is becoming the new security perimeter. With our platform of integrated software and cloud-based services, Centrify uniquely secures and unifies identity for both privileged and end users across today's hybrid IT world of cloud, mobile and data center. The result is stronger security and compliance, improved business agility and enhanced user productivity through single sign-on. Over 5000 customers, including half of the Fortune 50 and over 80 federal agencies, leverage Centrify to secure identities.

Learn more at www.centrify.com.

Santa Clara, California:	+1 (669) 444-5200	**Email:**	sales@centrify.com
EMEA:	+44 (0) 1344 317950	**Web:**	www.centrify.com
Asia Pacific:	+61 1300 795 789		
Brazil:	+55 11 3958 4876		
Latin America:	+1 305 900 5354		