**Using Sync Password**

Notes:

This feature pushes end users' Okta password to the end user's Active Directory object. This push occurs during initial Okta set up, Okta log on, or whenever a users' Okta password changes. Passwords will also be synced from AD to Okta.

If an Okta user is pushed to Active Directory after the user has already activated their Okta account, the Active Directory user object will be in a "User must change password at next logon" state. In this scenario, the user must first log onto Okta in order for the password to be pushed from Okta to AD.

The following table details the settings and components required for Sync Password uses cases.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Use Case** | **Enable DelAuth in Okta AD Settings?** | **Install Password Sync Agent? †** | **Enable Sync Password in Okta AD Settings?** | **Enable Sync Password in App? ‡** |
| Active Directory Environments | ↓ | ↓ | ↓ | ↓ |
| Allow users’ to sign in to Okta using their Active Directory credentials. | Yes | No | No | No |
| Make users' Okta credentials the same as their AD credentials and push AD passwords to provisioning-enabled apps | Yes | Yes | No | Yes |
| Sync an Okta users’ password down to AD, when Okta is provisioning an on-premises AD environment | No | No | Yes | No |
| Sync Okta passwords to AD | No | No | Yes | No |
| Sync Okta passwords to AD and push passwords to provisioning-enabled apps | No | No | Yes | Yes |

† In this use case, the Password Sync Agent must be installed and configured on all domain controllers in each domain in your forest, and the Okta username format must be either UPN or SAM Account Name.

‡ This option is available only in the provisioning settings of eligible SWA apps.

For more information, see the Password Synchronization Overview guide.

**Active Directory environments**

**Sync AD passwords to provisioning-enabled apps**

This feature pushes users' AD password to provisioning-enabled SWA apps during initial Okta set up and/or whenever users' AD password changes. It requires the Okta AD Password Sync Agent. The agent automatically pushes users' AD passwords from your Domain Controllers to the Okta service. Passwords are synced from your Domain Controller to Okta whenever a user's password is changed. The agent must be installed on all Domain Controllers and Delegated Authentication must be enabled on your Okta organization.

**Requirements**

* The org must be AD-mastered.
* The Active Directory Agent must be installed and configured in each domain in your forest.
* The Active Directory Password Sync Agent must be installed and configured on all domain controllers in each domain in your forest.
* Delegated Authentication must be enabled.
* Okta username format must be either UPN or SAM Account Name.

**Procedure**

1. Install and configure the Active Directory Agent on at least one domain controller in each domain in your forest. For details, see Install and configure the Okta Active Directory (AD) agent.
2. Install and configure the Active Directory Password Sync Agent on all domain controllers in each domain in your forest. For details, see Install and Configure the Active Directory Password Sync Agent.
3. Make sure that Delegated Authentication is enabled in Security > Delegated Authentication > Active Directory.Note: If your org is using the feature Instance-Level Delegated Authentication, del auth settings are configured in Directory > Directory Integrations > Active Directory > Settings.
4. Make sure that the Okta username format is UPN or SAM Account Name (samAccountName) in Directory > Directory Integrations > AD > Settings.
5. Go to the Applications menu.
6. Click a provisioning-enabled app to view its page.
7. Click the Provisioning tab, and in Provisioning Settings make sure that Enable provisioning featuresis enabled.
8. Scroll to the Sync Password section and select Enable.
9. For Password type, select Sync Okta Password.You must select Sync Okta Password in this use case because Delegated Authentication is enabled, which will make users' Okta password synonymous with their AD password.
10. Click Save.

**Sync Okta passwords to AD**

This feature pushes users' Okta password to Active Directory during initial Okta set up and/or whenever users' Okta password changes.

Note: If you also want to push users' Okta passwords to provisioning-enabled apps, see Sync Okta passwords to AD and to provisioning-enabled apps.

**Requirements**

* For use with Okta-mastered orgs in Active Directory environments
* The Okta service account must have permission to Reset user passwords and force password change at next logon via the Delegation of Control Wizard. For details, see Okta Service Account Options.
* Delegated Authentication must be disabled
* The Active Directory Password Sync Agent is not installed

**Procedure**

1. Make sure that Delegated Authentication is disabled in Security > Delegated Authentication > Active Directory.Note: If your org is using the feature Instance-Level Delegated Authentication, del auth settings are configured in Directory > Directory Integrations > Active Directory > Settings.
2. Go to Directory > Directory Integrations.
3. Click the Active Directory link.
4. Click the Settings tab.
5. Scroll to the Sync Password section and select Enable.
6. Click Save Settings.

**Sync Okta passwords to AD and to provisioning-enabled apps**

This feature pushes users' Okta password to Active Directory and provisioning-enabled apps during initial Okta set up and/or whenever users' Okta password changes.

**Requirements**

* For use with Okta-mastered orgs in Active Directory environments
* The Okta service account must have permission to Reset user passwords and force password change at next logon via the Delegation of Control Wizard. For details, see Okta Service Account Options.
* Requires enabling the Sync Password setting in two different areas of the product
* Delegated Authentication must be disabled
* The Active Directory Password Sync Agent is not installed

Important: The first time end users try to access the app after the admin performs this procedure, they must do so via the chiclet on their Okta dashboard in order to complete the syncing operation. Trying to access the app in any other way in the first post-procedure instance may fail.

**Procedure**

1. Make sure that Delegated Authentication is disabled in Security > Delegated Authentication > Active Directory.Note: If your org is using the feature Instance-Level Delegated Authentication, del auth settings are configured in Directory > Directory Integrations > Active Directory > Settings.
2. Go to Directory > Directory Integrations.
3. Click the Active Directory link.
4. Click the Settings tab.
5. Scroll to the Sync Password section and select Enable.
6. Click Save Settings.
7. Go to the Applications menu.
8. Click the desired provisioning-enabled app to view its page.
9. Click the Provisioning tab, and in Provisioning Settings make sure that Enable provisioning featuresis enabled.
10. Scroll to the Sync Password section and select Enable.
11. Configure settings:

* Password Type
* Password typeSync a randomly generated password – This option triggers Okta to push a unique, randomly generated password to each app user at setup. This is designed to prevent theft of a single Okta password from compromising an entire organization. Users receive a notification on their Home page that a random password was generated. To ensure that the Okta randomly generated password complies with the app's minimum password complexity requirements, see Ensure randomly-generated passwords comply with app's password policy.

Note: If you select this option, we recommend that you enable the Reveal Password feature to allow end users to see the password (Applications > Sign On Settings Credential Details). For details, see Revealing the Password of an App.

Sync Okta Password – This option pushes users' Okta password to all app users during initial setup and/or whenever users' Okta password changes.

* **Password cycle:**

Selecting the option Generate a random password whenever the user's Okta password changes ensures that a change in a user's Okta password generates and syncs a new random password to this app as well.

Note: Users may need to update their password on any device where they've installed this app.

**Reset All <App> Passwords**

This option is a security feature that allows you to reset the passwords of all app users.

1. Save

**Expire Okta-Mastered users' password using the Okta Expire Password API**

To prompt Okta-mastered users' to set a new password at next sign in, expire their password using the Okta Expire Password API.

**Requirements**

* For use in orgs with an Active Directory integration
* Delegated Authentication must be disabled
* The Active Directory Password Sync Agent is not installed

**Procedure**

1. Make sure that Delegated Authentication is disabled in Security > Delegated Authentication > Active Directory.Note: If your org is using the feature Instance-Level Delegated Authentication, del auth settings are configured in Directory > Directory Integrations > Active Directory > Settings.
2. Go to Directory > Directory Integrations.
3. Click the Active Directory link.
4. Click the Settings tab.
5. Scroll to the Sync Password section and select Enable.
6. Click Save Settings.
7. Go to Security > Policies > Password.
8. Click the Active Directory Policy.
9. Add a new rule or edit an existing rule: in the The user can setting, select change password.
10. Click Create/Edit Rule.
11. Access the expire\_password endpoint in the Okta User API and change the tempPasswordparameter value to TRUE.

**Ensure randomly-generated passwords comply with app's password policy**

Okta's generated password is 16 characters long with randomly-applied upper/lower case letters and numbers. To ensure a successful sync between Okta and the app, the Okta randomly-generated password should comply with the app's minimum password complexity requirements.

If the Okta randomly-generated password doesn't comply with the app's minimum policy, an error displays on the Okta Tasks page (Dashboard > Tasks). In such cases, Okta can, upon request, change the password policy on an per-app basis to match that app's minimum policy.

**Non-Active Directory Environments**

**Sync Okta passwords or a random password to provisioning-enabled apps**

This feature pushes users' Okta password or a random password to provisioning-enabled apps during initial Okta set up and/or whenever users' Okta password changes.

**Requirements**

**For use in non-Active Directory environments.**

**Procedure**

1. Go to the Applications menu.
2. Click the desired provisioning-enabled app to view its page.
3. Click the Provisioning tab, and under Settings, click To App.
4. Scroll down to the Sync Password section and click the Enable button.
5. Configure settings:

* **Password type:**

Sync a randomly generated password – This option triggers Okta to push a unique, randomly generated password to each app user at setup. This is designed to prevent theft of a single Okta password from compromising an entire organization. Users receive a notification on their Home page that a random password was generated. To ensure that the Okta randomly generated password complies with the app's minimum password complexity requirementse, nsuring Randomly-Generated Passwords Comply with Apps' Password Policy.

Note: If you select this option, we recommend that you enable the Reveal Password feature to allow end users to see the password (Applications > Sign On > Settings > Credential Details). For details, see Revealing the Password of an App.

**Sync Okta Password –** This option pushes users' Okta password to all app users during initial setup.

**Password cycle**

* Selecting the option Generate a random password whenever the user's Okta password changes ensures that a change in a user's Okta password generates and syncs a new random password to this app as well.

Note: Users may need to update their password on any device where they've installed this app.

1. **Reset All <App> Passwords**

This option is a security feature that allows you to reset the passwords of all app users.

1. Save