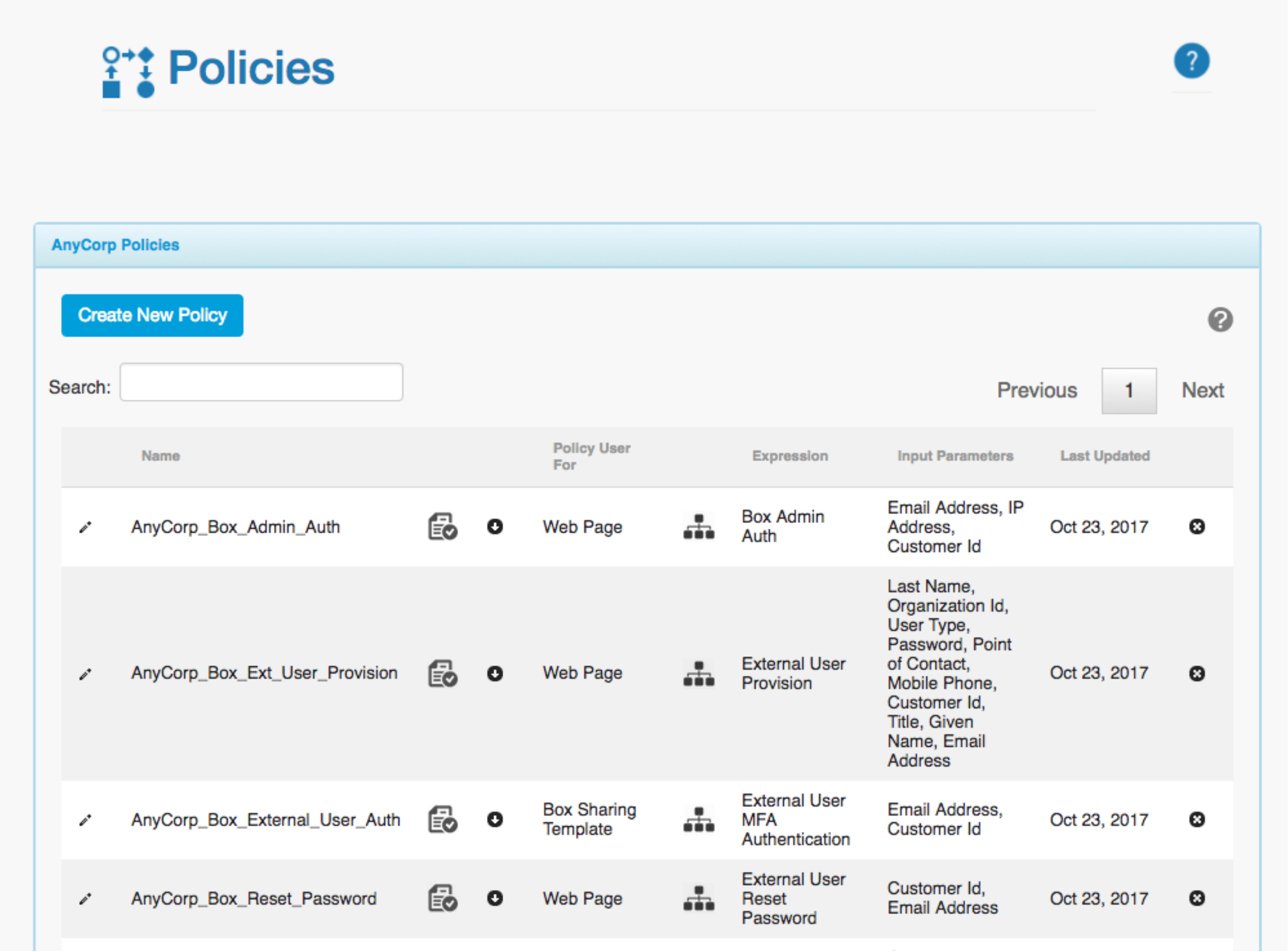
In the Policies tab the RA for Box external user lifecycle management policies are configured. The Resilient Access product includes a powerful policy workflow engine that can be configured to create flexible and adaptive access policies that can range from multi-factor authentication to role based authorization to meeting governance and compliance policies.



| Name | | | Policy User For | | Expression | Input Parameters | Last Updated | |
|---|---|---|---|---|---|---|---|---|
| AnyCorp_Box_Admin_Auth | | | Web Page | | Box Admin Auth | Email Address, IP Address, Customer Id | Oct 23, 2017 | |
| AnyCorp_Box_Ext_User_Provision | | | Web Page | | External User Provision | Last Name, Organization Id, User Type, Password, Point of Contact, Mobile Phone, Customer Id, Title, Given Name, Email Address | Oct 23, 2017 | |
| AnyCorp_Box_External_User_Auth | | | Box Sharing Template | | External User MFA Authentication | Email Address, Customer Id | Oct 23, 2017 | |
| AnyCorp_Box_Reset_Password | | | Web Page | | External User Reset Password | Customer Id, Email Address | Oct 23, 2017 | |

For the RA for Box product the system is pre-configured with  a set of policies for external user lifecycle management. These policies can be tailored to meet a customer's specific requirements by modifying the existing pre-configured policies. The pre-configured policies are:

## User Provisioning

This policy executes after the external user fills out the account registration form from the unique provisioning link they received in an email. The policy provisions the user into the external user database and prompts the user to go through an account activation workflow that includes

- Setting up their password recovery security questions
- SMS authentication to verify the phone number entered is the user's mobile phone
- Provides the option for setting up Google Authenticator as a second factor authentication method
- Activates the user's account and send a welcome email.

## User Authentication

The user authentication policy executes before access is granted to a shared file or folder. This authentication ensure that only RA for Box provisioned users can gain access to shared content. There are two pre-configured MFA policies for user authentication depending on which Box sharing type the authentication is for.

### Shared Link Authentication

This policy includes the following components

- Authorization Check - When shared links are sent from the RA for Box system, the software tracks which shared links are sent to which user. This is the basis for an authorization check to ensure the user is attempting to access a shared link that was specifically sent to the user rather than a shared link obtained from another RA for Box user.
- Password Lockout Check - A user's account is locked if they have three failed login attempts. This step ensures the account has not been locked out, if the account is locked the user is prompted to visit the account recovery page to reset their password.
- Password Authentication - performs password authentication, allows three retry attempts before registering a failed login.
- Choice of SMS or Google Authenticator as a second factor authentication method.
- Box Authorization - Performs Box API authentication to access the Box shared content.

### User Group Authentication

This policy includes the following components:

- Password Lockout Check
- Password Authentication
- Choice of SMS or Google Authenticator
- Box Authorization - Performs Box API authentication to access the User group shared folder that contains the folders that were shared with the user group.

### Password Reset

This policy is executed from the Account recovery page by clicking on the *Reset Password* button. It includes the following components:

- Security Question Check - prompts answers for the security questions configured during account registration
- Choice of SMS or Google Authenticator
- Prompt to set the new password and confirm password

### Account Activation

The account can be suspended or locked out for various reasons including lockout due to reaching the failed logins limit, failed activation during account registration and suspended by admin action. A suspended account can be activated from the Account recovery page by clicking the *Activate Account* button. This policy includes the following components:

- Email Authentication - prompts the user to enter a six digit code that is sent to their email account
- SMS Authentication - sends a text message to the user's registered mobile phone
- Google Authenticator Setup - Provides the option to setup Google Authenticator for 2nd factor authentication.
- Activates the user's account