The Self-Service Setup Checklist

Automating provisioning through IT self-service is possible. Self-service and role-based access control (RBAC) will not only kill the access request ticket, it will increase both security and compliance. Here's how to get started.

□ 01. Find the Apps

Self-service starts with app awareness. Employees often use non-approved apps, and it's up to IT to find them. From Dropbox to Notion, Clockwise to Postman, IT teams must gather a list of apps – sanctioned or not. Tools like Google OAuth [1] and Lumos can audit app usage and uncover which apps are hiding in the background.

□ 02. Centralize Requests

A company AppStore is a centralized channel that allows employees to request apps, permissions, internal tools, or even developer resources without IT help. But first, IT teams must pick which apps are on the AppStore. Once defined, the AppStore becomes a one-stop-shop for all approved apps. You can start defining your AppStore within a Confluence page or Lumos.

□ 03. Create Approval Workflows

Once the AppStore is in place, IT teams must decide who can approve requests for apps. This creates clarity whether to notify a manager or app admin for an access request. You can either define approvers on a central Confluence page and, then, let employees request apps through your ITSM. Or, you can use Lumos to make approvers accept or reject requests through Slack, auto-create the requested access and log everything for compliance purposes. No IT ticket needed.

[1] https://support.google.com/a/answer/6124308?hl=en

□ 04. Define Visibility

In an advanced self-service tool like Lumos, IT can set which roles should see which apps. For example, only sales needs to be able to request a sales tool like Outreach. Role-based visibility removes the clutter – and ticket requests.

□ 05. Pick Direct App Assignment or Group-Based Assignment

With most SSO providers [2], you can assign the user directly to the app or assign them to a group that adds them to the right app. For example, you can either assign the salesperson to Salesforce or assign them to the group "Salesforce_Admin" within your SSO provider, which then assigns the person to the right group within Salesforce. Make it clear for which apps IT should assign users to apps directly or via groups.

□ 06. Focus on Compliance

IT must define the audit process for access requests in the event of an auditor request. You can use an ITSM for this. Or, a self-service app like Lumos that creates an audit log plus – if wanted – opens and closes an IT ticket within your ITSM for the access request.

□ 07. Educate the User

A central onboarding hub, or knowledge base, can arm employees and approvers with the tools they need to use the AppStore. Lumos, for example, has a Slack-native app that makes it easy for employees to request apps where they spend most of their time.

[2] https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-migrate-users#an-example

Employees shouldn't be admins for hundreds of web apps with excessive permissions. But then again, nobody wants to be stuck in IT ticket queues for days to get the right access. With Lumos, you make your company more productive and compliant with self-service app requests, access reviews, and license removals. Learn more at Lumos.com