Datasheet August 2024

Okta Guide to Tackling Admin Sprawl

Adopting security best practices for privileged access

Members of the modern workforce often hold more and higher access and permissions than they need to perform their job – without realizing the threat this could pose to the organization's security posture. This phenomenon (not limited to administrative accounts) is caused by several factors, like admins granting excessive permissions as a result of misconfiguration or convenience, or users retaining permissions that are no longer necessary.

Increasingly, risks based on inconsistent access controls can have implications for not only organizational security, but also cost and compliance. According to Gartner's report on Best Practices for Optimizing IGA, nearly 75% of cloud security failures now result from mismanaged identities, access, and privileges, up from 50% in 2020. If left unaddressed, admin sprawl can lead to threat actors targeting unused or unmonitored user accounts, with the objective of unlocking initial access or elevated permissions.

The notion of privileged access, or the separation of administrative roles and responsibilities from non-administrative ones, is an important part of access management. To reduce cybersecurity and compliance risks — while also avoiding unnecessarily over-provisioning licenses — orgs should enforce least privilege, ensuring only the right users are assigned to the roles and permissions they need, at the right time.

> "Identity has become the key to modern security. Controlling the identity sprawl while enabling business is a challenge that legacy solutions could not resolve. Identity Security Posture Management uniquely provides us with ongoing visibility and reduces identity risks with a quick time-to-value and a data-driven approach."
>
> **Matthew Sharp**
> CISO at Xactly

[1] Example of footnote.

The problem with admin sprawl

At Okta, we have found that across all orgs using our Workforce Identity Cloud (WIC) services in 2024, 25% of super admins had not performed **any** kind of admin activity in the previous 45 days (which is a metric that maps to Control 5.3 of Center for Internet Security (CIS) Controls v8.0)[1]. This is an important issue for a few reasons:

- Critical/material **business impact** in case of an account takeover.
- The over-provisioning of permissions leads to **weakened security posture**, from inconsistent access controls.
- Excessive permissions can proliferate, leaving teams more **vulnerable to an attack** (i.e. over-permissioned accounts granting excessive access to other accounts).

While the activity across super admins accounts may appear high in contrast with industry average, the actual admin activity being performed only comprises 'least privilege' actions, or those which would not require the super admin role. This principle refers to the act of only granting users or entities access to the data or resources needed to complete a particular task. That includes user management actions (like viewing, creating, deleting users), group actions (like creating groups and adding/removing users), mobile policies, org security, and more.

It is increasingly important for permissions to be aligned with the right users and, ideally, be aligned to specific timeframes, as this allows organizations to maintain compliance with regulations like SOC 2, NIST-800, and SOX.

Admin Activity

A user's level of access to permissions, systems, and resources depends on the scope of their role, function, and assigned permissions. There are two unique types of admin activity this could include.

Access to Okta admin console

Okta's administrator console makes it simple to secure or manage users and their access, with pre-built app integrations to setup and configuration tools.

Use of API tokens

API tokens can be used to configure policies or restrictions on which user can connect to Okta and where they connect from. This does not include 1-time generated tokens.

[1] Note that it is not likely for organizations to achieve 100% utilization across their privileged users—nor is it recommended, since some buffer is needed for users who need 'break glass' permissions in rare cases.

A framework for reining in admin access

There is no hard rule around how many users should have admin permissions. This can vary across organizations based on a number of factors, including their org size. By examining some real-world Okta Workforce Identity Cloud (WIC) deployments, we have established a framework for managing admin sprawl before it becomes an issue.

The following framework is only a starting point. To help organizations align with these recommendations and improve their admin management, we recommend:

01 **Assess current admin utilization**
Run a recurring access certification campaign to review custom or standard administrator permissions. This will help uncover accounts with unnecessary admin permissions. Revoke admin rights from users who have not performed any admin activity in the last 45 days.

02 **Downsize the number of admins**
Based on the graph, identify the target number of admins for your organization's size. For organizations on the stricter side, in the chart below, aim for the 33rd percentile value (in light green) to minimize risk; for more permissive organizations (in yellow), consider the 66th percentile value to allow flexibility. You may also gradually reduce the number of super admins by reallocating non-essential admin permissions to standard user roles.

03 **Implement role-based access control (RBAC)**
Define and assign roles with specific permissions that align closely with job functions. Ensure that only those with a legitimate need have admin access, adhering to the principle of least privilege.

04 **Automate monitoring and measurement**
Use tools to regularly monitor admin activity and enforce policies. Set up alerts for unusual admin activities or when the number of admins exceeds the recommended range. Schedule periodic reviews to reassess admin needs and adjust access levels accordingly.

05 **Training and awareness**
Conduct training sessions for admins to ensure they understand the responsibilities and risks associated with their roles. Promote awareness of best practices to maintain security and compliance.

Implementing these steps can help your organization effectively manage and control admin sprawl, and help ensure a balanced and secure admin environment.

The graph below represents a range of existing super admins across Okta customer deployments (Y-axis) and how this trends across organizations varies by size (X-axis).

- Dark green indicates the median value of super admins per org size.
- Light green represents the 33rd percentile for organizations on the stricter side.
- Yellow represents the 66th percentile for organizations on the more permissive side.

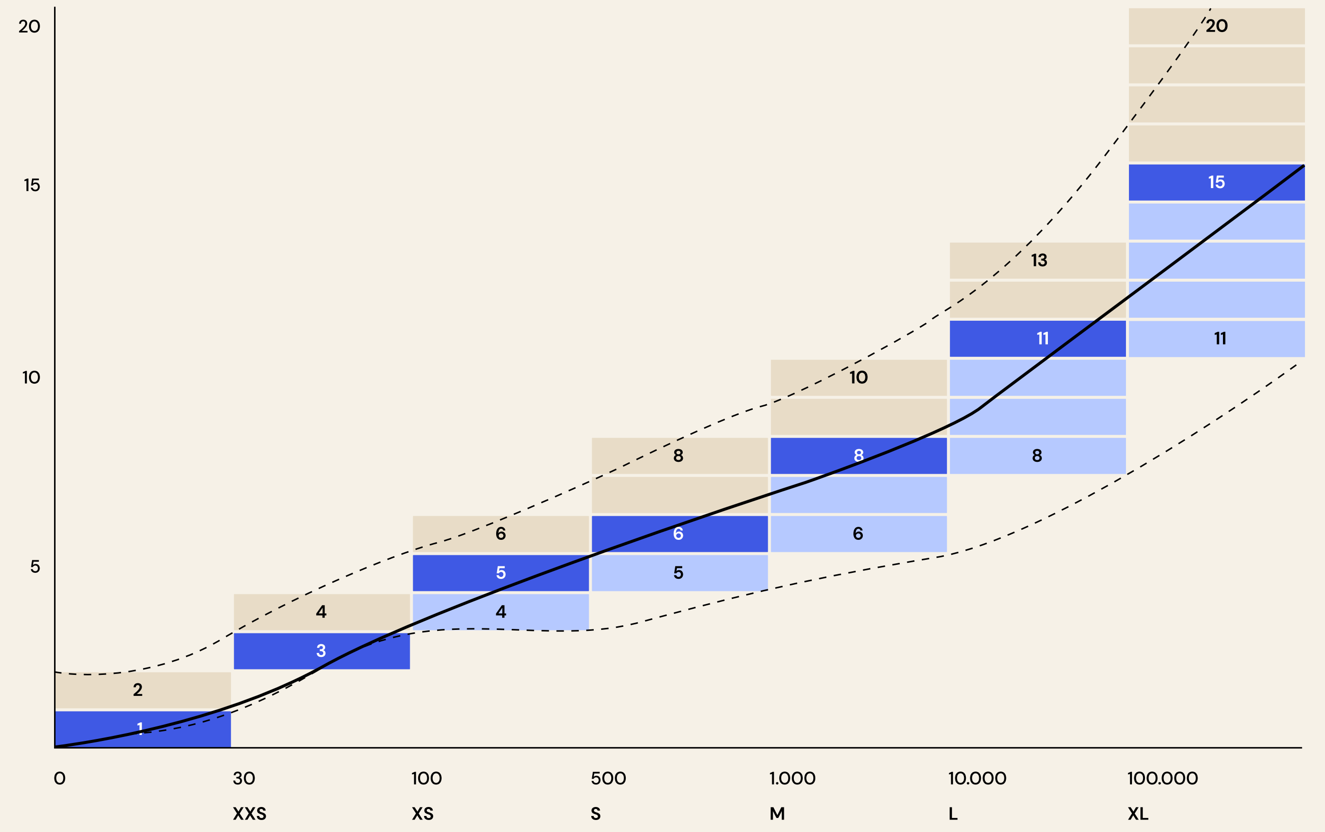

Figure 1 - Existing number of super admins according to org size

The data in the above graph serves as a guide to understanding how organizations rank compared to their peer groups by size and level of permissiveness related to admin rights. For example, companies with employee counts between 500 and 1000 are operating with around 5-8 super admins. To balance operational efficiency and security exposure, organizations need to tighten their exposure.

	Existing			Suggested max
	More strict	Median	More permissive	
XXS (30-99)	3	3	4	5
XS (100-499)	4	5	6	
S (500-999)	5	6	8	
M (1.000-9.999)	6	8	10	10
L (10.000-99.999)	8	11	13	
XL (100.000+)	11	15	20	

Figure 2 - Target number of super admins according to org size

Managing admin sprawl is a crucial part of maintaining security, cost efficiency, and compliance within any organization. As illustrated by these findings and recommendations, taking proactive steps to assess and optimize admin utilization, implementing role-based access controls, and building a culture of continuous monitoring and training can significantly reduce the risks associated with excessive permissions and access.

About Okta
Okta is the leading independent Identity provider. We enable organizations to securely connect the right people to the right technologies at the right time. We provide simple and secure access to people and organizations everywhere, giving them confidence to reach their full potential. Okta Identity Security Posture Management (ISPM) enables organizations to proactively defend against identity breaches—helping them identify vulnerabilities, prioritize risks, and streamline remediation.
To learn more, visit okta.com.