okta

WEBINAR

Okta Privileged Access

Safe harbor

This presentation contains “forward-looking statements” within the meaning of the “safe harbor” provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, long-term financial targets, product development, business strategy and plans, market trends and market size, opportunities, positioning and expected benefits that will be derived from the acquisition of Auth0, Inc. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as “expect,” “anticipate,” “should,” “believe,” “hope,” “target,” “project,” “goals,” “estimate,” “potential,” “predict,” “may,” “will,” “might,” “could,” “intend,” “shall” and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may fail to successfully integrate any new business, including Auth0, Inc.; we may fail to realize anticipated benefits of any combined operations with Auth0, Inc.; we may experience unanticipated costs of integrating Auth0, Inc.; the potential impact of the acquisition on relationships with third parties, including employees, customers, partners and competitors; we may be unable to retain key personnel; global economic conditions could worsen; a network or data security incident that allows unauthorized access to our network or data or our customers’ data could damage our reputation and cause us to incur significant costs; we could experience interruptions or performance problems associated with our technology, including a service outage; the impact of COVID-19 and variants of concern, related public health measures and any associated economic downturn on our business and results of operations may be more than we expect; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any unreleased products, features or functionality referenced in this presentation are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.

Infrastructure and privileged accounts are a top attack vector for threat actors

+80%

of breaches affect servers

74%

of all breaches include the human element through error, privilege misuse, use of stolen credentials, or social engineering

#1

Servers are the number one source of “initial access” during a hack

The volume and complexity of privileged resources and accounts has exploded with cloud adoption

Critical Resources

- Secrets
- Databases
- CI/CD tools
- IaaS (AWS, GCP, Azure)
- Servers

Critical Accounts

- Administrator Accounts (e.g. local admin on your laptop; Salesforce admin, Okta admin)
- Service Accounts

This proliferation of resources + accounts makes it difficult to fully adopt modern, zero trust security. We must ensure:

The **right people**

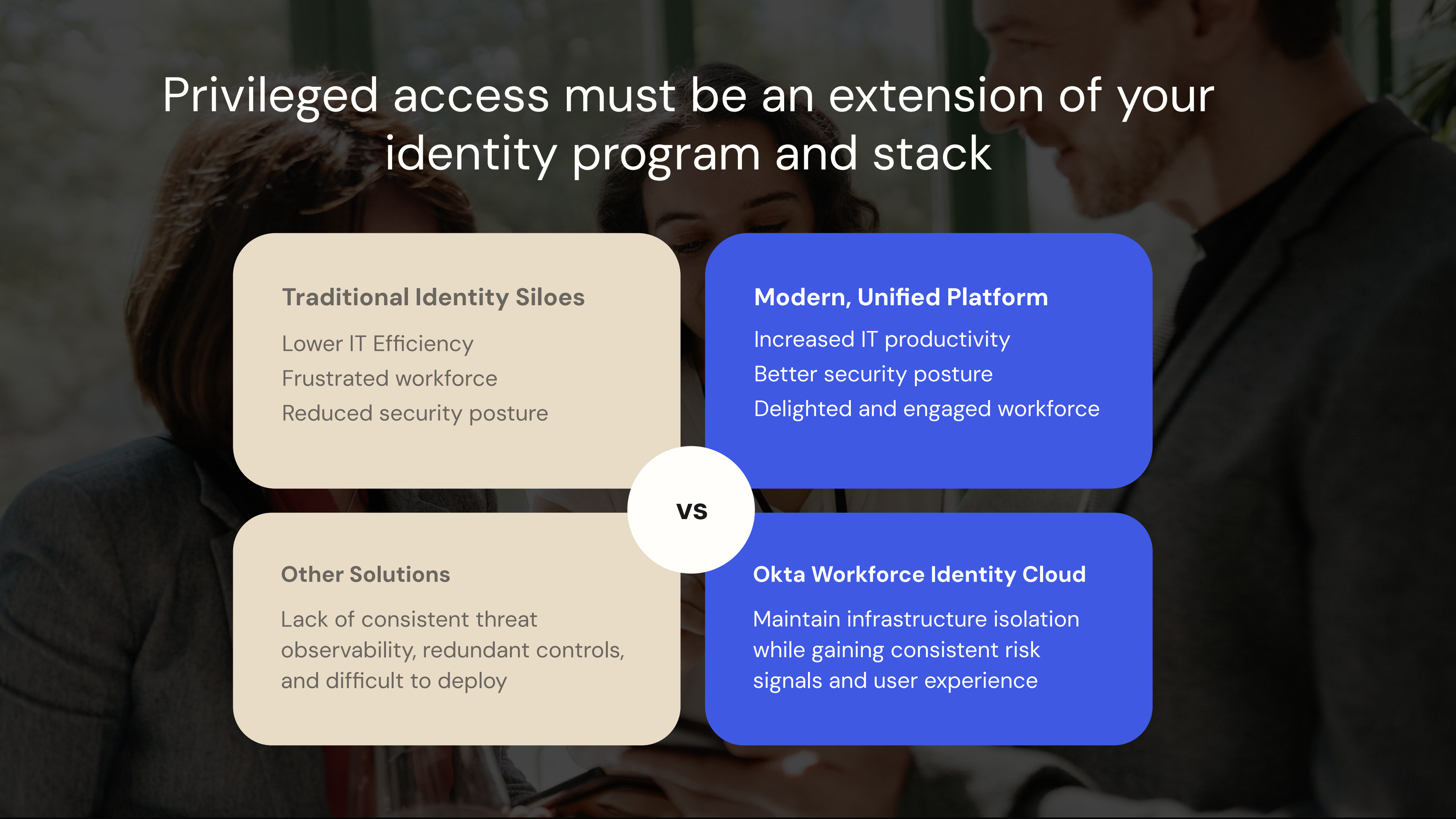
Have access to **the right resources**

At the **right time**, with **zero standing privileges** across *every* resource and account

In the **right context**

Re-**assessed continuously**

… All while making it **easy and cost effective** for both Admins and Users to manage and use



Privileged access must be an extension of your identity program and stack

Traditional Identity Siloes

Lower IT Efficiency

Frustrated workforce

Reduced security posture

Other Solutions

Lack of consistent threat observability, redundant controls, and difficult to deploy

vs

Modern, Unified Platform

Increased IT productivity

Better security posture

Delighted and engaged workforce

Okta Workforce Identity Cloud

Maintain infrastructure isolation while gaining consistent risk signals and user experience

Okta Workforce Identity Cloud: a unified solution for every one, and every identity need

Employees | Contractors | Business Partners

OKTA INTEGRATION NETWORK | Connect everything

Access Management

Any resource. Any device. Anywhere.
One secure passwordless experience.

Identity Governance

The right level of access, from a user's first day to their last.

Privileged Access

Least privilege for everything. No matter who they are, or what device they use.

PLATFORM | 99.99% Uptime

Directories
Connect in and manage all of your people

Insights + Reporting
All the data

Extensibility
Pro code or no code tools across Okta APIs + SDKs

Risk Signals
Connect in signals across your stack

Okta Privileged Access powers security, efficiency gains

Eliminate Standing Access to Privileged Accounts

Eliminate all standing access to privileged accounts on servers. power scheduled rotation of privileged account passwords, and monitor for out-of-band password changes to privileged accounts.

Raise the Security Bar for Privileged Accounts

Layer JIT privileged access policies with risk signals from across Okta's ecosystem, for example native signals from Okta as well as from partners in the EDR, MDM, and SASE spaces.

Meet Regulatory and Cybersecurity Insurance Requirements

More easily adhere to and demonstrate for auditors how your organization meets requirements for regulations and controls such as PCI-DSS, SOX, GDPR and NIST.

Simple, Great Employee Experience

Offer your workforce a seamless SSO experience for everything from apps to servers – or go one step further with Okta FastPass' phishing- resistant, passwordless login.

INTRODUCING

Okta Privileged Access:
A modern solution to enforce least privilege

Critical Capabilities

- JIT access for Infrastructure
- Access Requests for privileged resources
- Vault and Secure Privileged Accounts
- Audit & Session Recording
- Generic Secrets Management
- Manage Cloud Infrastructure

Okta Privileged Access

Secure Server Access

What is it?

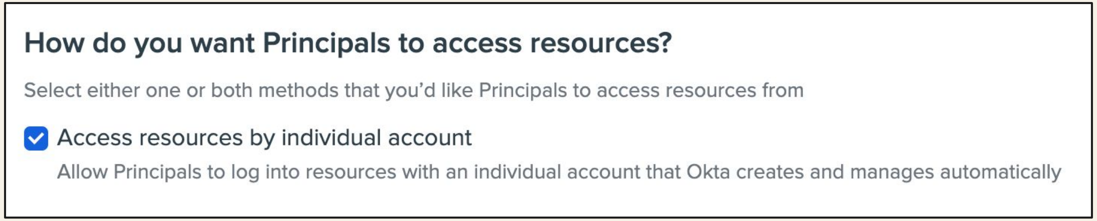
Modern server access using short-lived certificates secures and streamlines user access.

Benefits

Secure privileged access to servers

Eliminate Passwords and SSH Keys

Eliminate manual account administration

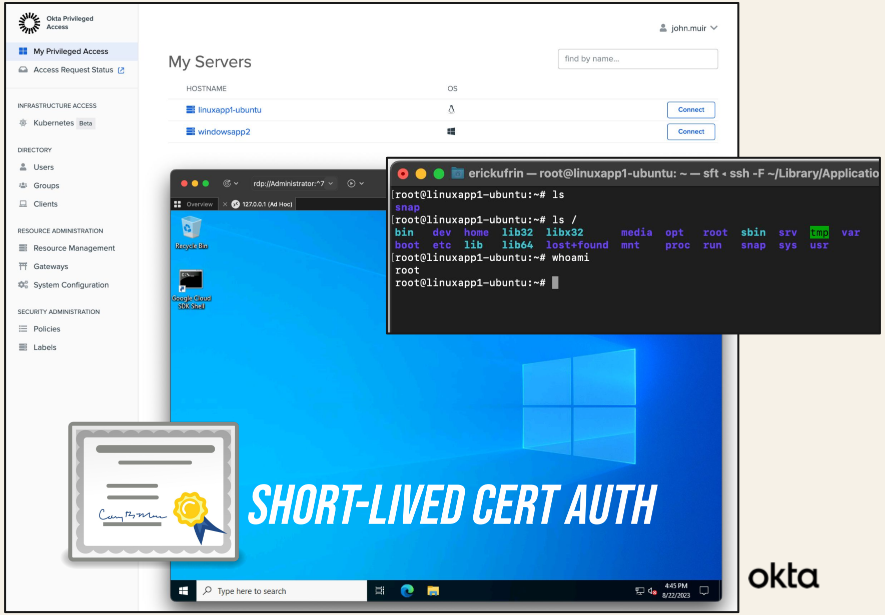


How do you want Principals to access resources?

Select either one or both methods that you'd like Principals to access resources from

☑ Access resources by individual account

Allow Principals to log into resources with an individual account that Okta creates and manages automatically



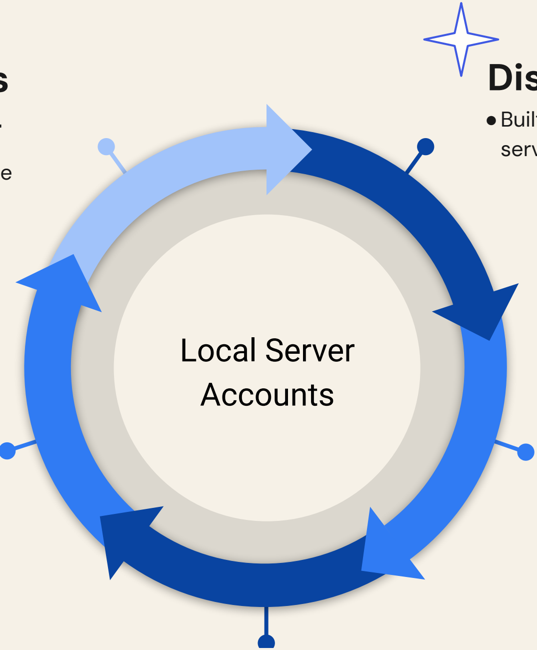
My Servers

HOSTNAME	OS	
linuxapp1-ubuntu	🐧	Connect
windowsapp2	⊞	Connect

erickufrin — root@linuxapp1-ubuntu: ~ — sft ◂ ssh -F ~/Library/Applicatio

```
root@linuxapp1-ubuntu:~# ls
snap
root@linuxapp1-ubuntu:~# ls /
bin   dev  home  lib32  libx32      media  opt   root  sbin  srv  tmp  var
boot  etc  lib   lib64  lost+found  mnt    proc  run   snap  sys  usr
root@linuxapp1-ubuntu:~# whoami
root
root@linuxapp1-ubuntu:~# 
```

Securing Local Server Privileged Accounts



Discovery

- Built-in discovery of server local accounts

Vaulting

- Select which accounts to secure and vault

Scheduled Rotation

- Scheduling and password complexity
- Logging

Policy-Based Access

- Access Request
- MFA
- Session Recording

Continuous Monitoring

- Detect and auto-remediate
- Okta System Log

Okta Privileged Access

Server Account Vaulting

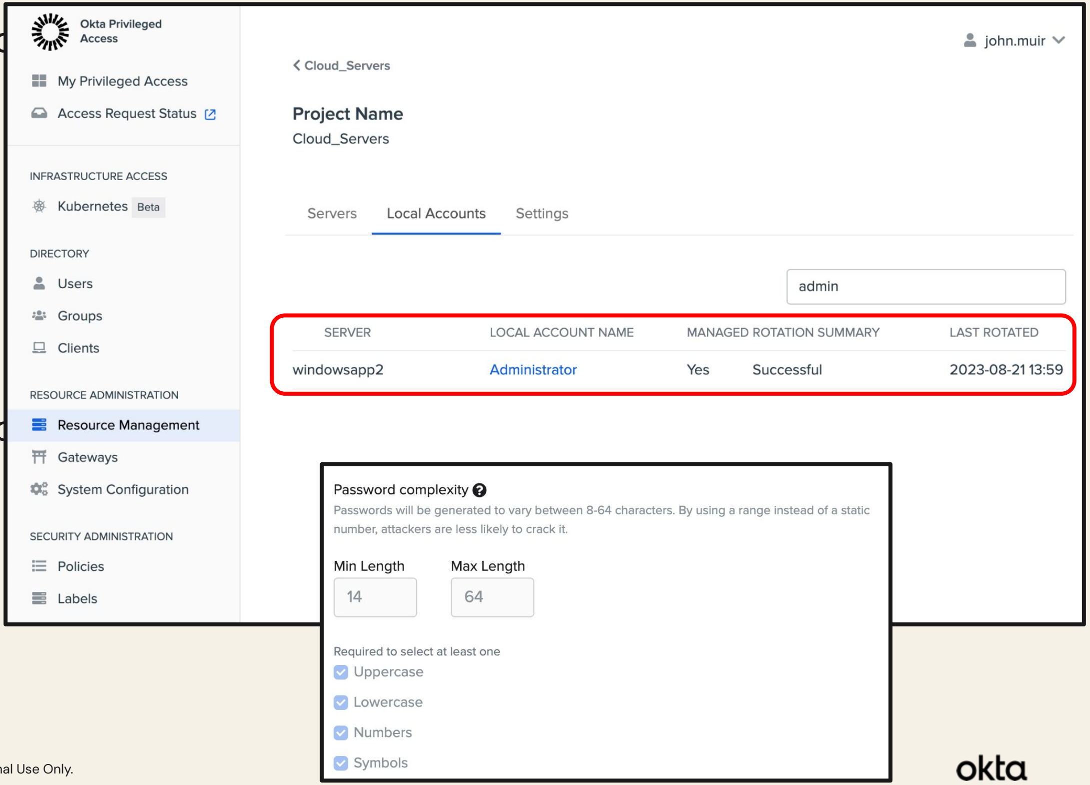
What is it?

Discovery of local accounts and automatec of passwords.

Benefits

Secure privileged account passwords

Detect and remediate out-of-band passwo changes



Project Name
Cloud_Servers

admin

SERVER	LOCAL ACCOUNT NAME	MANAGED	ROTATION SUMMARY	LAST ROTATED
windowsapp2	Administrator	Yes	Successful	2023-08-21 13:59

Password complexity

Passwords will be generated to vary between 8-64 characters. By using a range instead of a static number, attackers are less likely to crack it.

Min Length: 14

Max Length: 64

Required to select at least one

☑ Uppercase

☑ Lowercase

☑ Numbers

☑ Symbols

Okta Privileged Access

Gateway, Recording, Audit

What is it?

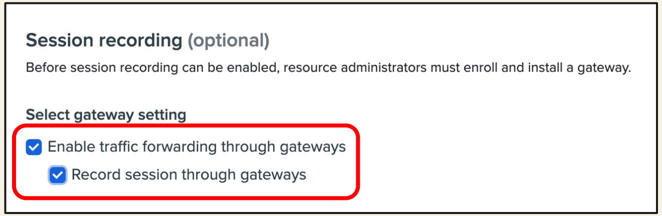
Gateway is a transparent proxy for SSH and RDP. Administrators can optionally record sessions.

Okta System Log provides a single location to review all Events related to Privileged Access.

Benefits

Tamper-proof session logs are stored on the Gateway for later review

Session and Event data help with security detection & response as well as compliance objectives



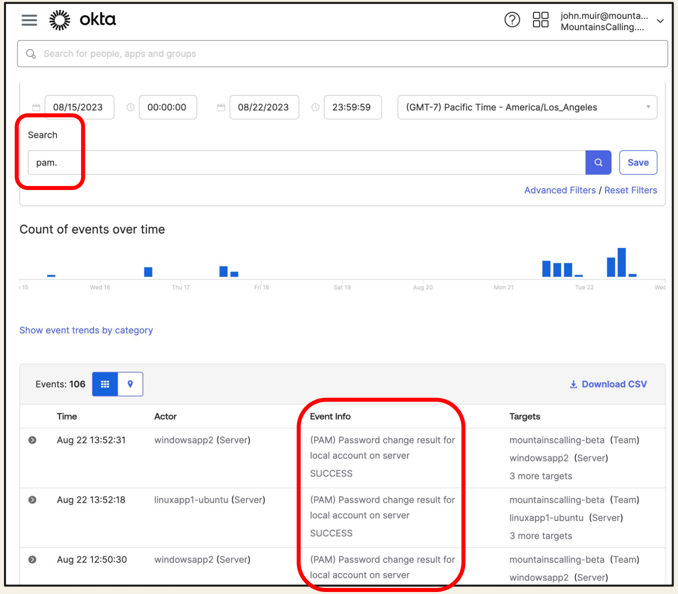
Session recording (optional)

Before session recording can be enabled, resource administrators must enroll and install a gateway.

Select gateway setting

☑ Enable traffic forwarding through gateways

☑ Record session through gateways



08/15/2023 00:00:00 08/22/2023 23:59:59 (GMT-7) Pacific Time - America/Los_Angeles

Search: pam.

Count of events over time

Events: 106

Time	Actor	Event Info	Targets
Aug 22 13:52:31	windowsapp2 (Server)	(PAM) Password change result for local account on server SUCCESS	mountainscalling-beta (Team) windowsapp2 (Server) 3 more targets
Aug 22 13:52:18	linuxapp1-ubuntu (Server)	(PAM) Password change result for local account on server SUCCESS	mountainscalling-beta (Team) linuxapp1-ubuntu (Server) 3 more targets
Aug 22 12:50:30	windowsapp2 (Server)	(PAM) Password change result for local account on server	mountainscalling-beta (Team) windowsapp2 (Server)

Access Request Integration

What is it?

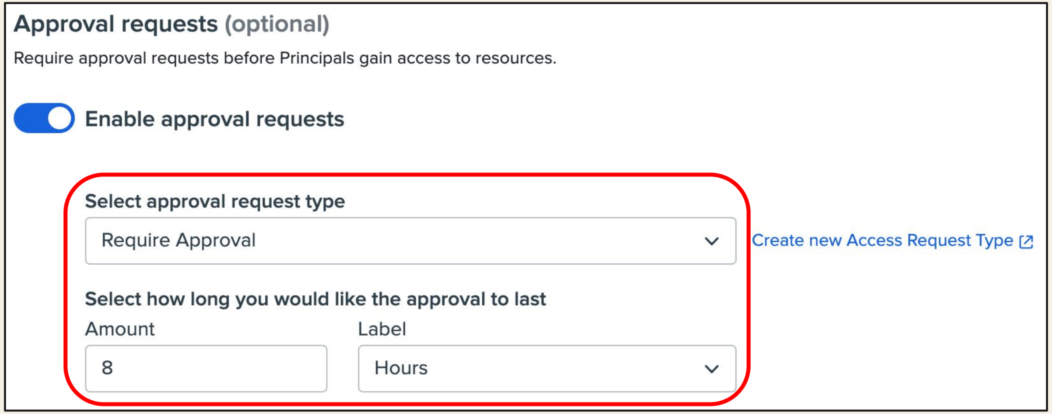
Require human approval workflows before resources can be accessed.

Supports Slack, MS Teams, Web Inbox

Benefits

Protect critical or sensitive access with "two rules" or other human review workflows

Control the length of time access can be used



Approval requests (optional)

Require approval requests before Principals gain access to resources.

Enable approval requests

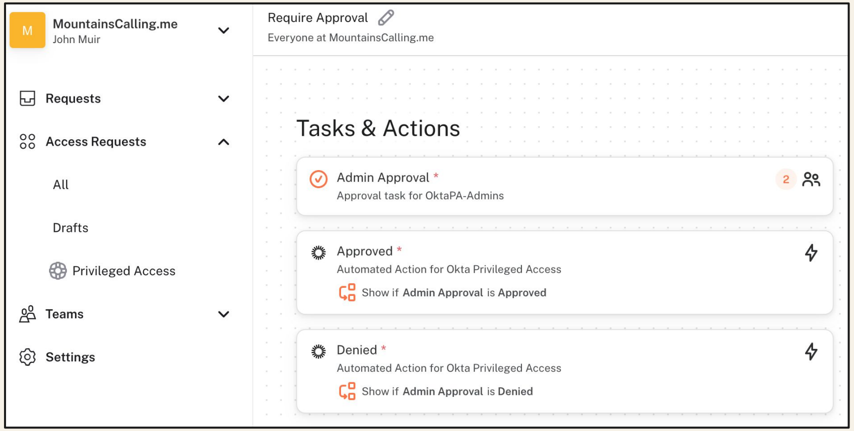
Select approval request type: Require Approval

Create new Access Request Type

Select how long you would like the approval to last

Amount: 8

Label: Hours



MountainsCalling.me
John Muir

Require Approval
Everyone at MountainsCalling.me

Tasks & Actions

Admin Approval *
Approval task for OktaPA-Admins
2

Approved *
Automated Action for Okta Privileged Access
Show if **Admin Approval** is **Approved**

Denied *
Automated Action for Okta Privileged Access
Show if **Admin Approval** is **Denied**

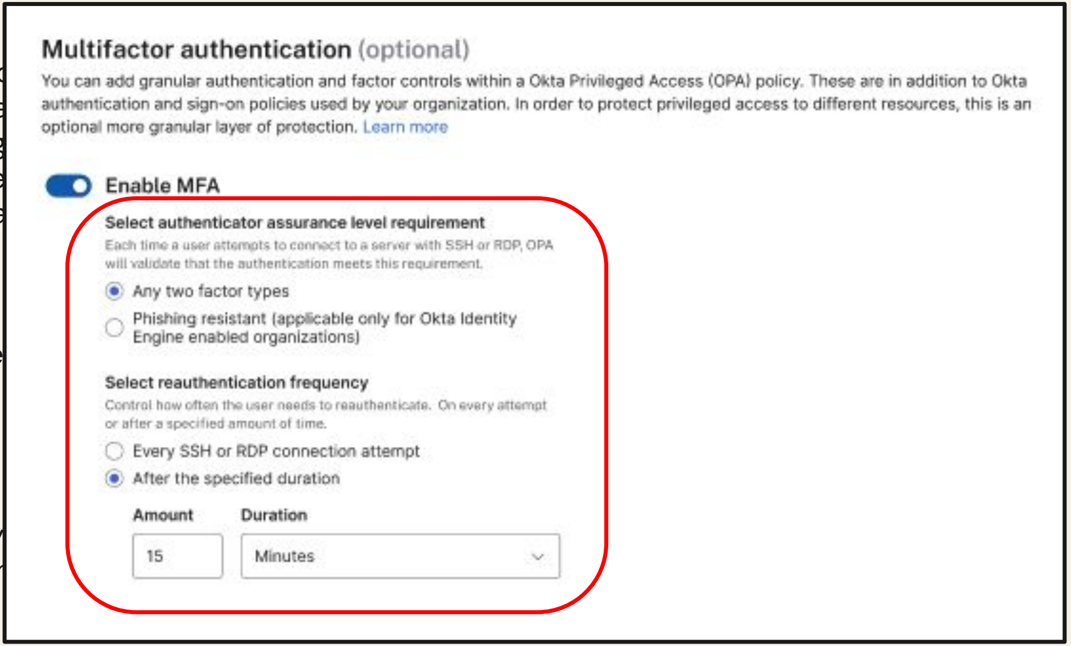
Granular MFA support in PAM access policy

What is it?
Today, Okta customers use sign-on policies and rules t secure and flexible way to control how users authentica sign in to their accounts. However, the existing Okta sig policies are not granular enough to, for example, require end-user use MFA on every SSH or RDP connection to a privileged server.

The Okta PA policy adds support for more granular 'per-connection' MFA requirements for SSH and RDP se access.

Benefits

Help customers achieve stronger security outcomes by re-verifying user identity before granting access to high privileged resources



Multifactor authentication (optional)

You can add granular authentication and factor controls within a Okta Privileged Access (OPA) policy. These are in addition to Okta authentication and sign-on policies used by your organization. In order to protect privileged access to different resources, this is an optional more granular layer of protection. Learn more

Enable MFA

Select authenticator assurance level requirement

Each time a user attempts to connect to a server with SSH or RDP, OPA will validate that the authentication meets this requirement.

● Any two factor types

○ Phishing resistant (applicable only for Okta Identity Engine enabled organizations)

Select reauthentication frequency

Control how often the user needs to reauthenticate. On every attempt or after a specified amount of time.

○ Every SSH or RDP connection attempt

● After the specified duration

Amount	Duration
15	Minutes

Live DEMO

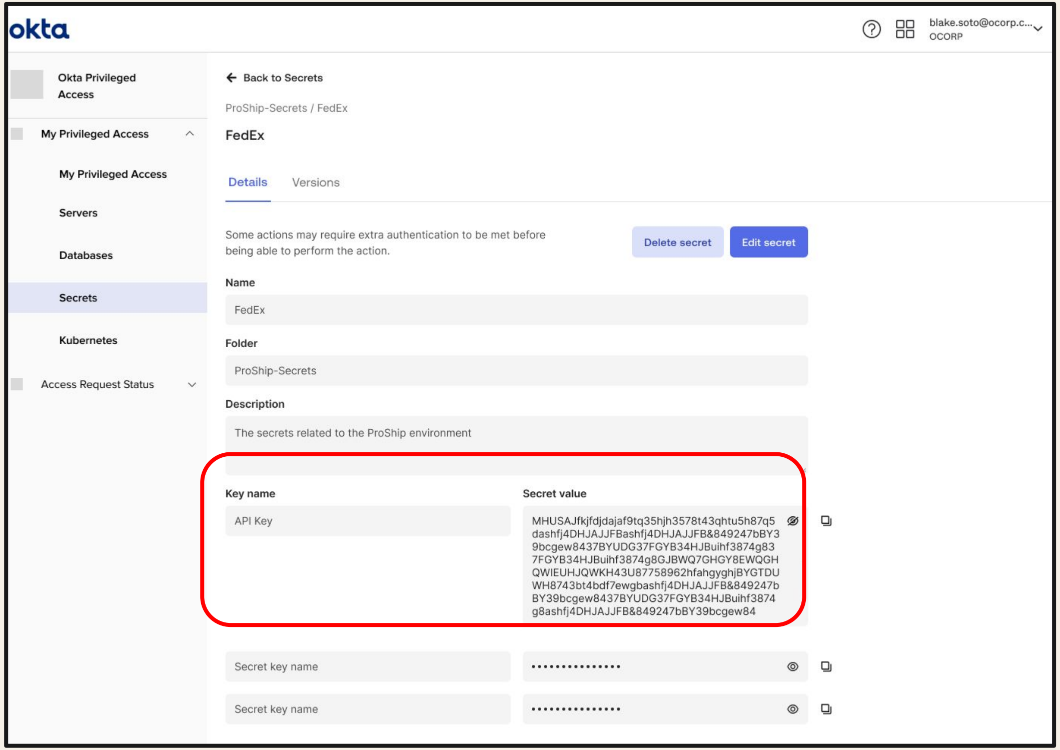
Okta Privileged Access

Secrets Vault

What is it?
Okta Privileged Access Secrets Vault feature will enable customers to protect Secrets (any string). The Secrets Vault feature will provide a durable, secure place to store secrets within their organization. This feature will deliver ease-of-use for end users as well as provide controls and governance layers that administrators require to satisfy security requirements and compliance regulations.

Benefits

Secure organizational ***secrets***, these private bits of information that if left exposed could cause irreparable harm to the organization



ProShip-Secrets / FedEx

FedEx

Some actions may require extra authentication to be met before being able to perform the action.

Name: FedEx

Folder: ProShip-Secrets

Description: The secrets related to the ProShip environment

Key name	Secret value
API Key	MHUSAJfkjfdjdajaf9tq35hjh3578t43qhtu5h87q5dashfj4DHJAJJFBashfj4DHJAJJFB&849247bBY39bcgew8437BYUDG37FGYB34HJBuihf3874g837FGYB34HJBuihf3874g8GJBWQ7GHGY8EWQGHQWIEUHJQWKH43U87758962hfahgyghjBYGTDUWH8743bt4bdf7ewgbashfj4DHJAJJFB&849247bBY39bcgew8437BYUDG37FGYB34HJBuihf3874g8ashfj4DHJAJJFB&849247bBY39bcgew84
Secret key name	•••••••••••••••
Secret key name	•••••••••••••••

Live DEMO

Okta Privileged Access

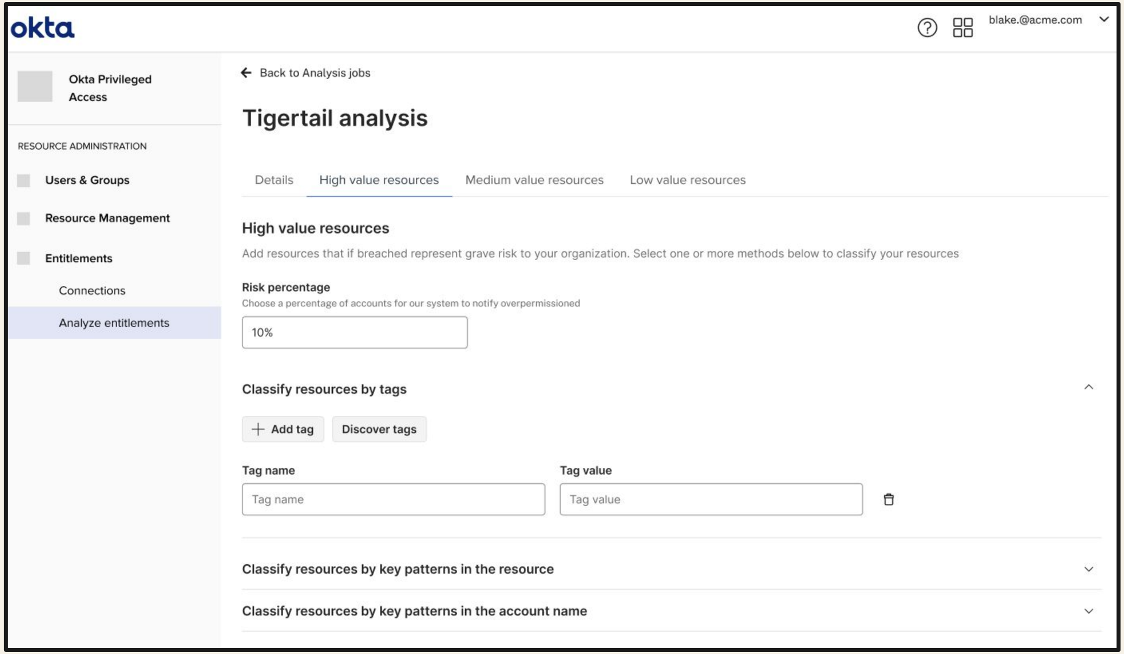
Privileged Entitlements Discovery and Analysis

What is it?

To define least privileged permissions, customers need to understand what resources within their IaaS should be treated as privileged. This feature will help customers find the set of resources in their IaaS applications that represent high risk to their organization if breached, then help them create entitlements in those applications to grant least privileged access to them.

Benefits

Streamline the process of removing standing access to privileged resources in IaaS applications and implementing a just in time access model.



Tigertail analysis

High value resources

Add resources that if breached represent grave risk to your organization. Select one or more methods below to classify your resources

Risk percentage

Choose a percentage of accounts for our system to notify overpermissioned

10%

Classify resources by tags

Tag name

Tag name

Tag value

Tag value

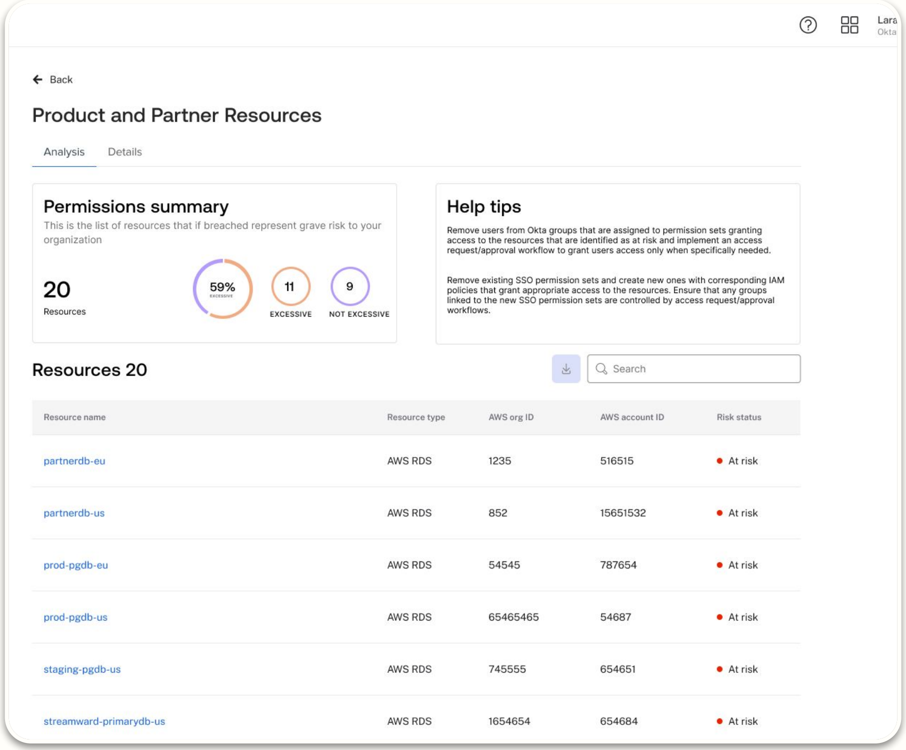
Classify resources by key patterns in the resource

Classify resources by key patterns in the account name

Entitlement Support for Cloud Infrastructure: Discovery and Analysis

Customer Benefits

- Visibility: Quickly discover and analyze existing IaaS entitlements
- Right-Size IaaS Access: Aligns with native IaaS IAM policies for risk-aware access control
- Unified Platform: Integration with Okta Workflows and Access Requests



Product and Partner Resources

Permissions summary

This is the list of resources that if breached represent grave risk to your organization

20 Resources

59% EXCESSIVE

11 EXCESSIVE

9 NOT EXCESSIVE

Help tips

Remove users from Okta groups that are assigned to permission sets granting access to the resources that are identified as at risk and implement an access request/approval workflow to grant users access only when specifically needed.

Remove existing SSO permission sets and create new ones with corresponding IAM policies that grant appropriate access to the resources. Ensure that any groups linked to the new SSO permission sets are controlled by access request/approval workflows.

Resources 20

Resource name	Resource type	AWS org ID	AWS account ID	Risk status
partnerdb-eu	AWS RDS	1235	516515	● At risk
partnerdb-us	AWS RDS	852	15651532	● At risk
prod-pgdb-eu	AWS RDS	54545	787654	● At risk
prod-pgdb-us	AWS RDS	65465465	54687	● At risk
staging-pgdb-us	AWS RDS	745555	654651	● At risk
streamward-primarydb-us	AWS RDS	1654654	654684	● At risk

Okta Privileged Access

Questions?