

Advanced Server Access

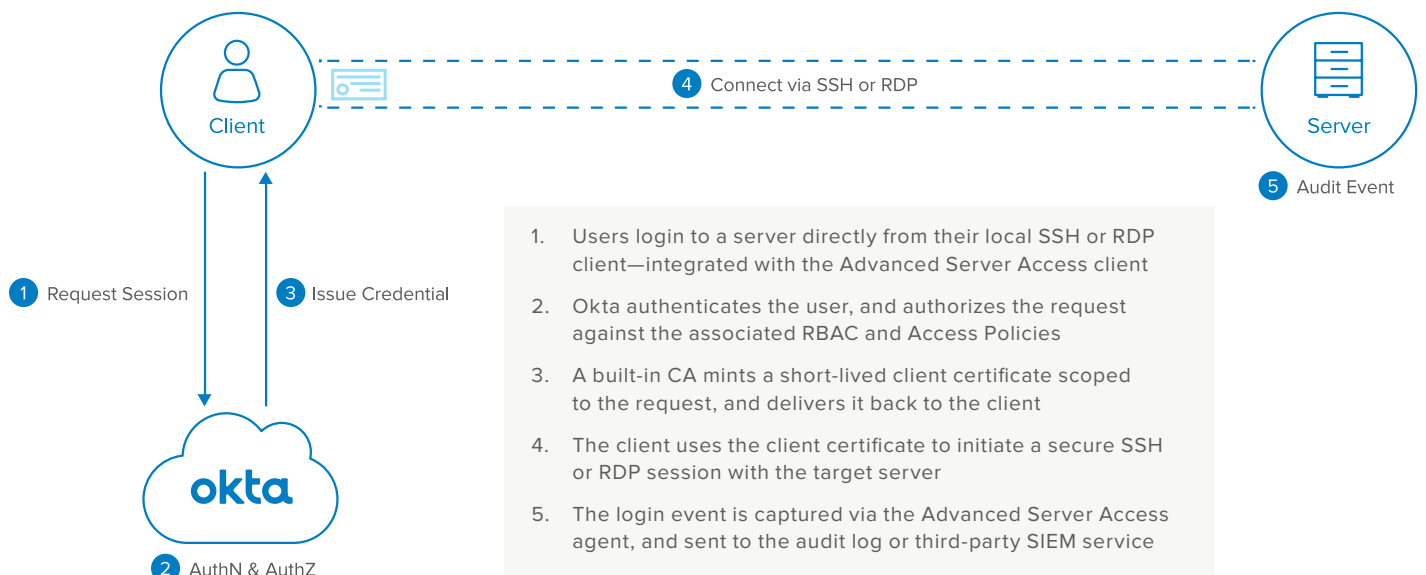
A Zero Trust approach to Linux and Windows

At any level of scale, controlling access to servers is a challenge for IT and Security teams just trying to keep up with credential sprawl. Traditional methods place so much of the emphasis on protecting the “keys to the kingdom,” but have we really seen any fewer breaches year over year, even with so much investment in security? The problem is rooted in the credentials themselves holding the privileges, without any surrounding context about the user or the device. Okta took a fresh identity-led approach to the server access use case and designed a Zero Trust architecture from the ground up capable of making smarter access decisions in real-time.

How Okta Advanced Server Access works

Okta Advanced Server Access replaces traditional SSH Key and RDP Password authentication with a client certificate-backed architecture that mints ephemeral credentials limited in scope to a user on a device at a specific point-in-time. What’s the best way to mitigate the risk of credential theft? It’s to drive their value down to zero by minimizing the attack surface to an individual authorized request.

- Supports mixed environments under the same control plane: on-prem, AWS, Azure, GCP, etc.
- Backed by core Okta Identity, with end-to-end lifecycle management of local machine accounts
- Streamlines familiar SSO and MFA authentication workflows inline with the SSH and RDP protocols



1. Users login to a server directly from their local SSH or RDP client—integrated with the Advanced Server Access client
2. Okta authenticates the user, and authorizes the request against the associated RBAC and Access Policies
3. A built-in CA mints a short-lived client certificate scoped to the request, and delivers it back to the client
4. The client uses the client certificate to initiate a secure SSH or RDP session with the target server
5. The login event is captured via the Advanced Server Access agent, and sent to the audit log or third-party SIEM service

Mitigate the risk of credential theft

No more worrying about how to protect and rotate static credentials

- Okta replaces static keys and passwords commonly used to access servers with single-use ephemeral client certificates
- Through a built-in Certificate Authority, client certificates are minted on-demand only for authenticated and authorized requests
- Each certificate is tightly scoped to the individual request at a point-in-time, significantly minimizing the attack surface

Remove barriers to automation

A cloud-native product designed for highly elastic environments

- Easy to bake server enrollment into your config management of choice—Chef, Puppet, Ansible, Terraform, etc.
- Supports multi-cloud environments with a unified control plane that abstracts each provider's IAM functions
- Every actionable event is exposed as an API, allowing you to build custom workflows to your liking

Centralize access controls to servers

Manage server access under a single control plane, backed by core Okta Identity

- Automate the end-to-end lifecycle of your local server user and group accounts under a single directory
- Deliver seamless SSO and MFA authentication to your SSH and RDP workflows, inline to the protocols
- Introduce contextual access controls based on dynamic user and device posture

Deliver a seamless end user experience

Security controls that even your most technical users will love using

- Works inline with the SSH and RDP protocols, integrated natively with the CLI and GUI tools your team are used to
- Delivered as a SaaS, abstracting the complexities of credential management, privileged user management, and more
- Automation makes it easy to configure dynamic environments, eliminating redundant tasks without compromising security

Extend Core Okta Identity to Your Infrastructure Resources



Universal Directory

Single source of truth for local server user and group accounts



Single Sign-On

Streamlined authentication for SSH and RDP workflows



Adaptive MFA

Inject additional security controls to privileged session auth



Lifecycle Management

Automated provisioning of local server user and group accounts

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables 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 the confidence to reach their full potential. To learn more, visit okta.com.