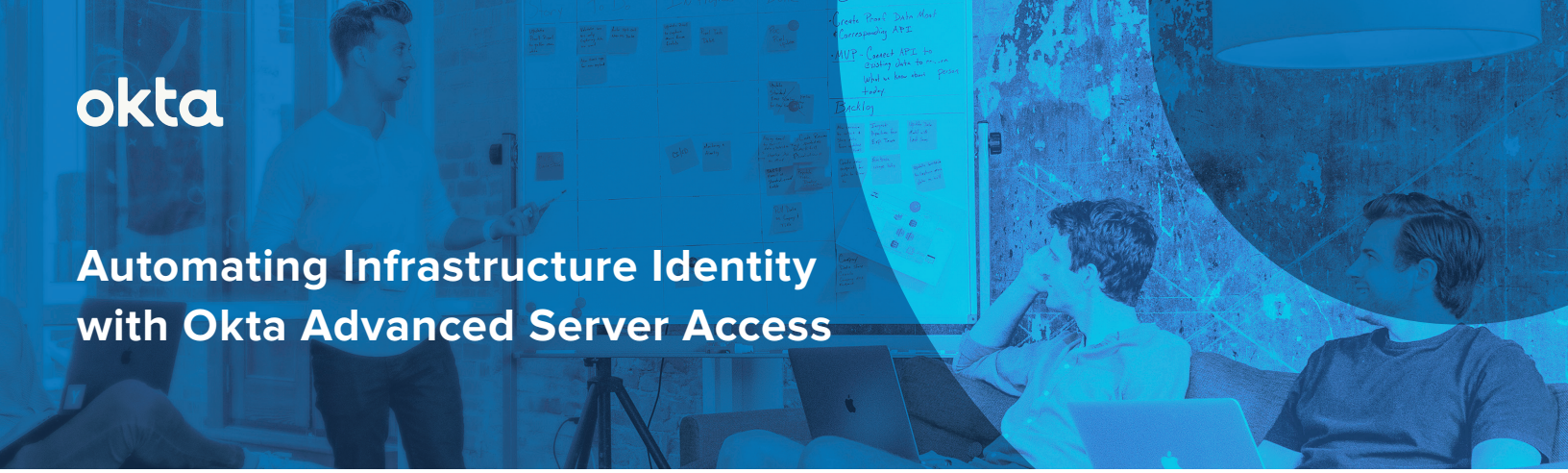


# Automating Infrastructure Identity with Okta Advanced Server Access

## It's a New World

Today's ever-evolving business environment has accelerated to the point where to survive, every company must become a technology company. Market realities have changed dramatically, requiring companies to adapt at tremendous speeds. Customers are demanding new ways to purchase goods and services. Partners are looking for new ways to work closely without the need for around-the-world flights. And the way employees work together has changed almost overnight. With the pace of change increasing ever faster, even the most successful companies are struggling to keep up, let alone stay ahead.

To meet these challenges, companies are expediting many strategic IT and security initiatives that give their employees, customers, and partners the capabilities needed to do business in the current climate. Migration to the cloud has accelerated, as companies seek the flexibility and lower cost of moving to cloud-based compute, storage, and networking services. To expedite the delivery of new services while scaling quickly to meet increasing customer demand, software suppliers are turning to Infrastructure-as-a-Service (IaaS) provided by cloud service providers such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure.

While increasing a company's velocity, these strategic initiatives share a common barrier to faster implementation: security. The primary job of today's Chief Information Security Officer (CISO) is to enable their company to move faster without increasing security risk. According to the 2020 Cloud Threat Report by Oracle and KPMG[1], 92% of IT professionals surveyed described a "gap" between their desired level of cloud usage and their company's ability to deliver cloud access securely. In the same survey, 59% of respondents admitted to having privileged cloud account credentials stolen through spear-phishing attacks. And as cloud use grows, the need for cloud-based services to comply with increasingly strict security regulations increases the burden on today's CSO.

## Okta Advanced Server Access: Solving a Common Problem with an Elegant Solution

Given the complexity of cloud security along with the urgency to scale faster, the need to control and manage access to company resources has never been higher. But addressing each point of vulnerability with a different security application only increases complexity and the subsequent burden on IT resources, slowing down your operation rather than speeding it up.

To meet today's security requirements, companies need a single access authentication process that guarantees that the right person can access the right resources at the right time. This principle of Least Privilege Access is a foundational layer in building a Zero Trust Security Model.

**Okta Advanced Server Access** (Okta ASA) expands Okta's industry-leading identity and access management platform to include server access and administration across any hybrid or multi-cloud infrastructure. By leveraging the Okta Identity Cloud, Okta ASA creates a single, unified Integrated Access Management (IAM) system that brings all of a company's servers alongside its applications under a single, secure umbrella of identity-based authorization and management.

Designed for scalability, Okta ASA leverages automation to streamline time-consuming manual tasks such as onboarding and offboarding admin users, freeing up

[1] https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf

precious IT resources to launch the new services their customers, partners, and employees require. Okta ASA gives even the largest companies the security, speed, and ease of use they need to manage access with the highest security level.

Okta ASA also simplifies the increasingly complex compliance requirements. As a SaaS, Okta ASA provides simple internal processes for tracking and managing SysAdmin user accounts and credentials, controlling command-level sudo privileges, as well as capturing server audit logs—all common requirements for compliance standards such as SOC2, PCI-DSS, and FedRAMP.

## Enabling Zero Trust Server Access and Authentication

Static SSH keys and passwords are the weakest links in the access security chain. Okta replaces this outdated key-based system with a dynamic, ephemeral one-time access token that ties directly to the user's Least Privilege Access profile in the central Okta Identity database.

**Okta ASA Secure Log-in Process:**

1. Users log in to a server directly from their local SSH or RDP tools—integrated with the Client Application.
2. Okta authenticates the user and device, then authorizes the request against the respective role-based access controls.
3. A built-in client application mints a temporary client certificate scoped tightly to the individual request.
4. The Client uses the certificate to initiate a secure SSH or RDP session with the target server.
5. The login event is captured via the server agent and sent to the audit log or 3rd party SIEM service.

The central difference between Okta ASA and existing solutions is that instead of being based on keys, Okta ASA relies on identity, roles, and access privileges on a per-server basis. This process not only creates a single point of control for all servers but eliminates the risk of a break-in based on lost or stolen keys, shared accounts, or other unintentional consequences of "credential sprawl."

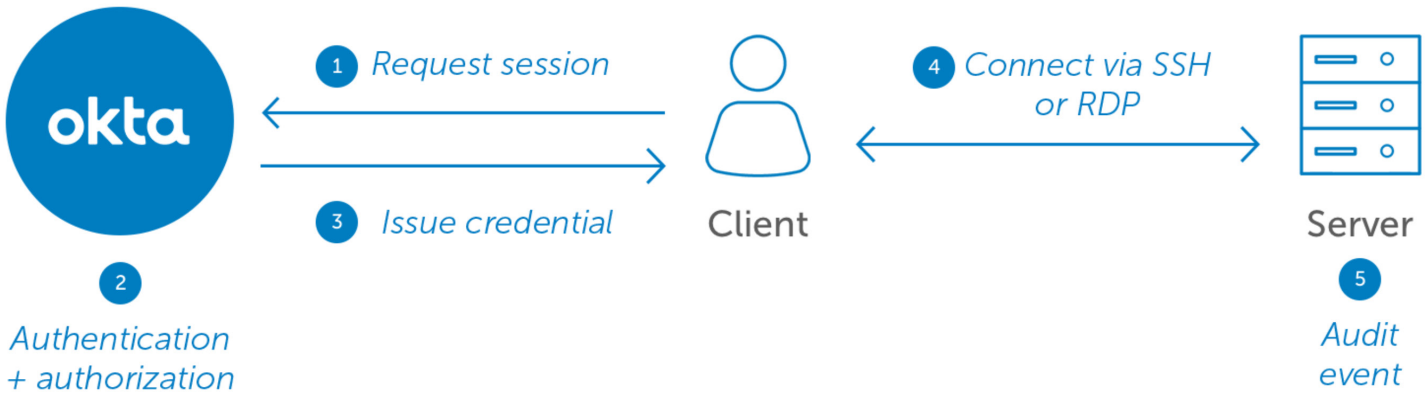
## Okta ASA Addresses Today's Challenges with Today's Technology

Okta designed Advanced Server Access to address today's business needs. Alternatives to adopting an integrated access management system cannot meet the speed and scalability requirements of today's business world. With more dynamic infrastructure environments, where resources are constantly spinning up and down, securing control of administrative accounts and credentials is near impossible without establishing a strong link with core identity.

Privileged Access Management (PAM) vendors track those with special credentials but lack a centralized control plane, where access and permissions are a function of the user's role. Without a clear link to identity, onboarding, and even more importantly, offboarding, of server admin users is a manual process, which can leave doors open for malefactors to enter. Okta ASA automates the onboarding and offboarding process for all users, simplifying this critical task, and removing human error opportunities.

Also, as many companies are learning, migrating to the cloud is not a simple process. Each cloud vendor uses its own access/authentication system. This practice not only gives the IT group yet another set of credentials to manage but increases the risk of

**Zero Trust Okta Authentication Model**



Okta ASA not only provides increased security for the critical data on your company's servers, but also accelerates your move to the cloud-native world:

- Designed for the cloud, Okta ASA simplifies the transition to any cloud-based architecture. Its unified identity and access controls cross any hybrid or multi-cloud environment.
- Backed by the Okta ephemeral client certificate architecture, Okta ASA replaces static SSH keys and passwords and eliminates "credential sprawl."
- Built for DevOps automation, Okta ASA speeds server admin onboarding and offboarding at scale. Local server accounts and policies are automatically provisioned and de-provisioned to downstream servers from the Okta Identity Cloud as the source of truth.
- Compliance is built into the Okta ASA Software-as-a-Service, reducing the in-house compliance burden for access and authentication systems.
- Okta ASA works out of the box with your existing SSH and RDP tools. Okta ASA is easy to configure, thus delivering a seamless user experience.

vendor lock-in. Okta ASA frees a company to move from one cloud vendor to another without having to change authentication systems, having been built to work out of the box with Amazon Web Services, Google Cloud Platform, and Microsoft Azure. This integration allows the security team to create a single umbrella of authentication that covers on-premise and multiple off-premise or hybrid clouds, thus vastly simplifying the access/authentication process as companies scale their cloud operations.

## Conclusion

The need to adapt quickly, and to "do more with less," have become requisite to survival, let alone continued growth. Gone are the days when strategic initiatives such as moving to the cloud, or enabling a secure, distributed workforce, or even BYOD, could be put off until the next fiscal period. With Okta ASA, the barriers to accelerating your company's "velocity" are very often within your control.