Moving Beyond User Names & Passwords

An Overview of Okta's Multifactor Authentication Capability

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Contents

1 Moving Beyond User Names and Passwords
1 Enter Multifactor Authentication
1 MFA For On Premises and Cloud Apps
2 The Okta Solution
2 Fully Integrated with the Okta Service
2 Works with your VPN
2 Flexible, Secure Verification Options
2 Security Question
2 Soft Token
2 Text Message
3 Centralized Policy Management
3 Easy for Administrators and Users
3 Extensible to Third-Party MFA Solutions
4 Conclusion
4 About Okta

Moving Beyond User Names and Passwords

Typical web applications are protected with single-factor authentication: a user name and password. These credentials, in addition to being difficult to manage, leave sensitive data and applications vulnerable to a variety of common attacks. Attackers are using increasingly prevalent and sophisticated techniques to steal passwords to consumer, banking, and enterprise applications. Individual users are vulnerable to password theft via highly targeted spear phishing attacks, while large groups of users can be compromised by an attack on a specific vendor holding their credentials. These credentials are then sold individually or in bulk on the black market to any criminal organization that might want them.

Examples of recent large-scale password thefts include attacks on Sony and LastPass. In June 2011, the Sony website was broken into and hackers "compromised over 1,000,000 users' personal information, including passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts".[1] In LastPass's case, the May 2011 breach potentially exposed user names and passwords to a wide swath of web applications.[2]

The effect of a stolen password is magnified by the fact that users frequently reuse passwords across multiple applications. This means that a stolen Facebook or nytimes.com password may compromise users' Salesforce.com or Active Directory accounts. A recent study by the Internet security company BitDefender revealed that "75 percent of social networking user name and password samples collected online were identical to those used for email accounts".[3]

As enterprises adopt more cloud applications, addressing this threat will become critical. Unlike older on-premises applications, cloud applications are accessible to anyone on the public Internet. And while enterprise cloud software vendors like Salesforce.com and Workday go to considerable measures to ensure they run a highly available and secure service, their login screens are equally as available to attackers as to legitimate users.

Moreover, today's cloud applications do not easily integrate with existing enterprise products used to monitor dangerous security events, which can make password breaches of enterprise cloud apps difficult if not impossible for most IT organizations to detect.

Enter Multifactor Authentication

Multifactor authentication (MFA) is designed to protect against the range of attacks that rely on stealing user credentials. Organizations can use a variety of techniques, but all work by requiring the user to provide something in addition to their primary password— something the user is, has, or knows—before they can be authenticated to the protected service. With MFA in place, even if a user's password is stolen, his account is safe from unauthorized access.

MFA For On Premises and Cloud Apps

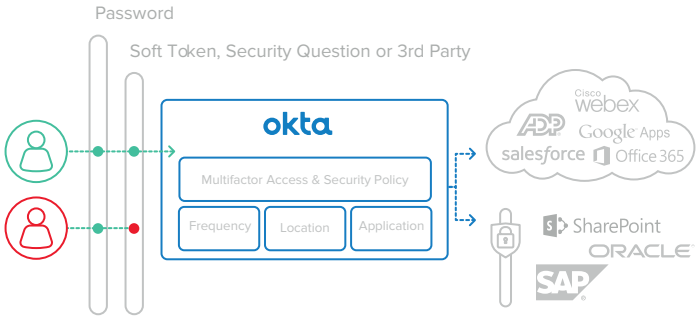
Multifactor authentication has been in use for decades, most commonly by enterprises adding protection to their VPN gateways and other sensitive resources. This was particularly helpful because VPN gateways provided a single point of entry to on-premises applications that generally just required a user name and password to access.

Today, as key business systems migrate to the public cloud, critical data is as likely to be stored in the cloud as it is behind the firewall and every organization has a mix of on premises and cloud applications to protect. Most cloud based applications leverage their own siloed identity store and security model to protect this data, making it difficult if not impossible for IT organization to enforce uniform control policies across all of their applications as they did with MFA on a VPN for on premises apps. Adding MFA one app at a time is simply not practical, as it would require administrators and users to juggle dozens of factor types across as many applications. What organizations need is a unified access gateway that applies equally to VPNs and on-premises and cloud-based applications.

The Okta Solution

Okta is an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. The Okta service provides directory services, single sign-on, strong authentication, provisioning, workflow, and built in reporting. Okta's s secure, flexible multifactor authentication comes included as part of the core identity and access management service. Designed to protect against today's phishing attacks, stolen passwords, and shared credentials, Okta's MFA solution provides both the highest security and simplest administration possible. Okta's native multifactor options can be centrally administered in an integrated fashion, or Okta integrates with existing third-party multifactor solutions such as Verisign VIP or RSA. Okta also provides options to easily replace or integrate with existing strong authentication solutions, such as RADIUS.

Fully Integrated with the Okta Service



Okta provides multifactor authentication as a core feature of the Okta identity management service if organizations don't already have their own solution. Okta builds all MFA functionality with the same focus on flexibility, security, and ease of use that we apply to all other aspects of our product, and it comes bundled with the Okta solution.

Works with your VPN

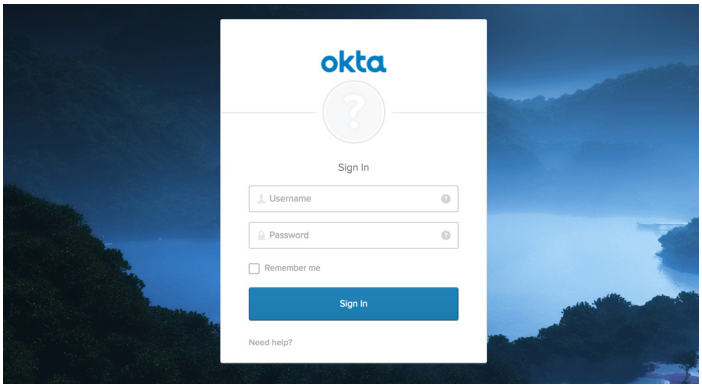
Okta's Single Sign-On and MFA solution works with any SAML-enabled SSL VPN, including Juniper SA and Cisco ASA. This enables comprehensive, seamless authentication across all enterprise applications accessed from the public Internet, whether cloud-based, in the DMZ, or protected by a VPN.

Flexible, Secure Verification Options

Organizations can choose from a variety of second factor options, balancing the needs of their user base, the sensitivity of the applications they are protecting, and overall ease of use.

Security Question

Security questions offer added protection by requiring users to provide additional information beyond simple user name and password. This option requires no additional devices and minimal user configuration.



Soft Token

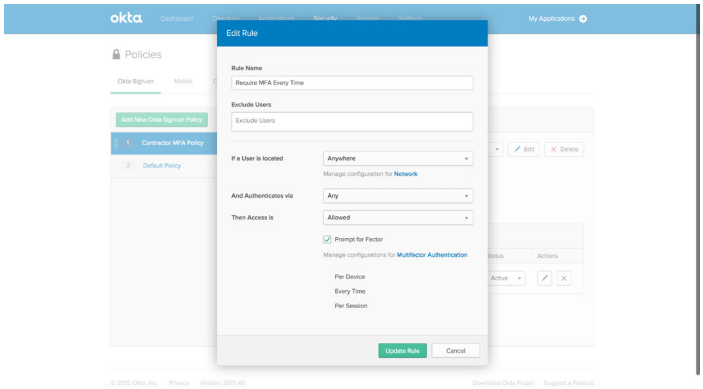
Okta's soft token is designed for absolute simplicity for the user, and comprehensive security for the Okta administrator. The app can be installed directly from both the Android and Apple App Stores, or directly from Okta for BlackBerry users. It self-configures using the device's integrated camera. Once installed, users simply read a six-digit number, generated using the industry standard Time-Based One-Time Password algorithm, from their phone screen to access protected resources.

Text Message

For those users who need something stronger than a security question but don't have a smartphone, Okta's MFA also offers a text message option which will work with any SMS enabled cell phone. Like the other MFA options it is built into the service, not additional third party services required – it just works.

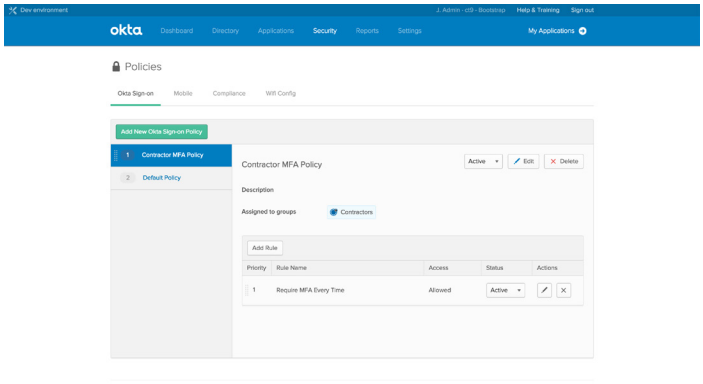
Centralized Policy Management

One Okta policy controls access to all applications, whether cloud-based or on-premises. Policies can control how often and when to ask users for additional verification. Frequency can range from every login to once per device.



Okta provides multiple options for MFA

Extra verification can be required for all apps or individual apps, and separate policies can be established for internal and external users.



App specific MFA enables flexible policies

Easy for Administrators and Users

Okta's multifactor authentication solution is easy to use for both administrators and users. As an Okta service, it is fully cloud delivered—no on-premises software or hardware is required. It can be enabled with just two clicks in the Okta administrative interface. Users are fully empowered to self-administer their tokens on their smartphones, subject to the policies administrators define. No clumsy hard tokens or complex SSL certificates are required.

Extensible to Third-Party MFA Solutions

In addition to native Okta MFA support, Okta also integrates with a variety of existing MFA solutions such as Versign VIP and RSA. By leveraging the same extensible architecture that enables Okta to provide a set of pre- integrated applications, customers can also leverage existing MFA products in conjunction with the Okta service.

Conclusion

Okta provides a unified multifactor authentication solution for your cloud and on premises applications with an architecture designed for both higher levels of security and ease of use for users and administrators. It is an integral part of the core Okta service and comes bundled with every edition of the Okta service. With Okta's multifactor authentication, a single policy and token can be used to secure any application managed by the service. It works with cloud-based applications, SSL VPNs, and on-premises web apps. Enabling Okta with MFA protects business-critical data from the most prevalent attacks on the Internet today.

About Okta

Okta is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security policies. It integrates directly with an organization's existing directories and identity systems, as well as 4,000+ applications. Because Okta runs on an integrated platform, organizations can implement the service quickly at large scale and low total cost. More than 2,500 customers, including Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International and Western Union, trust Okta to help their organizations work faster, boost revenue and stay secure.

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.

1. See http://www.informationweek.com/news/security/attacks/229900111

2. See http://www.pcworld.com/article/227223/lastpass_online_password_manager_may_have_been_hacked.html

3. See http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email

4. See http://tools.ietf.org/id/draft-mraihi-totp-timebased-06.txt