OTAVA

DATA SHEET

TWO-FACTOR AUTHENTICATION

Security and convenience in one application

Get the best of both worlds with Otava's Two-Factor Authentication. Validating user identity before allowing access to important tools and data is a critical security safeguard many organizations miss. 2FA is an optimal security measure that protects against cybercrime and unauthorized access for clients connecting to networks or applications from a remote location. By linking the second authentication factor to a personal device, you can achieve improved security and greatly reduce your risk of compromise. 2FA is not only required to meet PCI compliance, but it's generally recommended as a best practice for a strong cybersecurity posture that regular business applications including VPN access, Active Directory, Remote Desktop and others can take advantage of.

You're a good fit for Otava Two-Factor Authentication if...

- **You're concerned about security and access vulnerabilities towards business-critical networks, applications or processes.**
- **You have sensitive or proprietary data that can be accessed remotely, or you're concerned about password security.**
- **You need to meet Payment Card Industry Data Security Standards (PCI DSS).**
- **You work with sensitive healthcare information. Since 2006, the HHS has recommended Two-Factor Authentication as a best practice for HIPAA compliance.**
- **You've embraced mobile or remote workforce options and want to validate the identity of people requesting access.**
- **You want to reduce IT overhead for help desk support and need secure method for employees to self-reset passwords.**

Why Otava Two-Factor Authentication

Simple, secure remote network access:

Two-Factor Authentication provides an extra layer of protection ensuring user identity and guards against unauthorized entry, because it requires the use of one form of authorization (username/password) and a second (differing) form of identity validation to gain access to a network remotely.

Mobile-based authentication:

The addition of a simple, mobile-device based authentication method allows you to complete a secondary authentication of your choice to achieve network access.

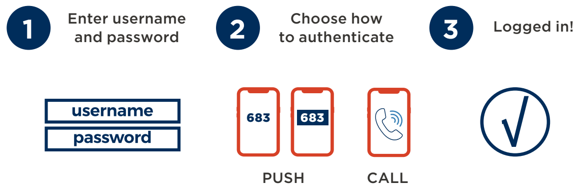
Choose your authentication method:

Push Notifications: Quickly view login or transaction details and tap "Approve" on your iOS or Android device.

Smartphone Passcodes: Easily generate login passcodes: A mobile application is available for free on all smartphone platforms.

Text Message: Login passcodes sent via text messages. Works on all mobile devices with SMS support.

Phone Call: Simply answer a phone call and press a key to authenticate.



EXPECT EXCEPTIONAL

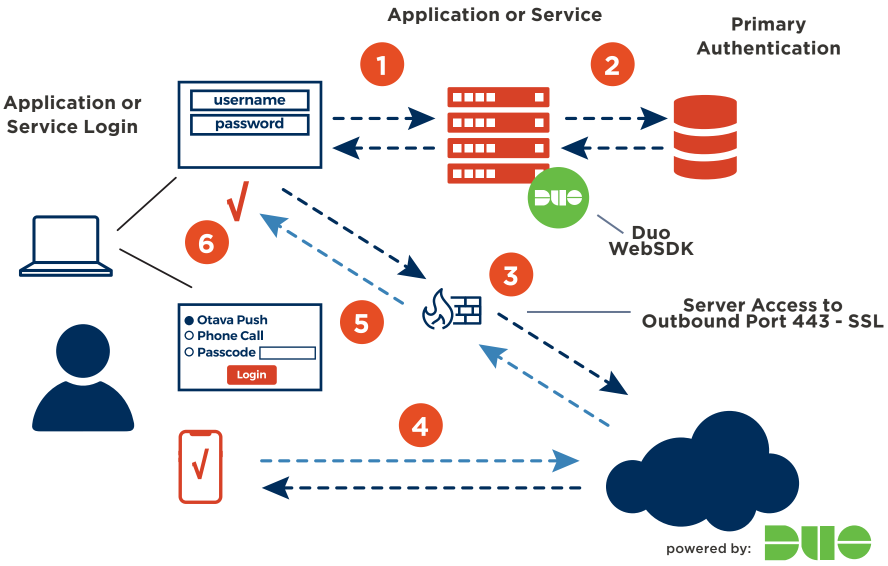
Otava Two-Factor Authentication Meets Compliance

PCI DSS

If you need to meet PCI DSS (Payment Card Industry Data Security Standards) compliance because you collect, store or process credit cardholder data, then you need to use Two-Factor Authentication. PCI requirement 8.3 mandates:

> **"Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties."**

How Otava Two-Factor Authentication Works



HIPAA

While not required, two-factor authentication is a best practice to meet HIPAA compliance. The HIPAA security Rule §164.312(d) requires a covered entity to identify methods available for authentication:

> **"Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems."**

HIPAA
100% Compliant

PCI DSS
100% Compliant

ISO 27001
100% Compliant

SSAE 16/SOC 1
Type II

SOC 2
Type II

Otava Two-Factor Authentication Benefits

- Ease of integration and installation
- Can be controlled and implemented by the client
- Inexpensive and adds a significantly higher level of security
- Meets regulatory requirements for sensitive data protection
- Supports most types of smartphones, features and landlines
- Increased device visibility improves overall security
- Eliminates vulnerability of single password security
- Increased protection for employee credentials
- Enhanced security for remote worker VPN access
- Protection for Active Directory identity authentication
- Strong SSL encryption assures security of all authentications
- Two-Factor Authentication powered by Duo Security-Cisco

OTAVA
EXPECT EXCEPTIONAL

OTAVA provides secure, compliant hybrid cloud solutions for service providers, channel partners and enterprise clients. By actively aggregating best-of-breed cloud companies and investing in people, tools, and processes, Otava's global footprint continues to expand. The company provides its customers with a clear path to transformation through its highly effective solutions and broad portfolio of hybrid cloud, data protection, disaster recovery, security and colocation services, all championed by its exceptional support team. Learn more at www.otava.com.

READY TO ENHANCE YOUR CYBERSECURITY STANCE?
Call to talk to a specialist.

OTAVA.com (877) 740-5028 solutions@otava.com