atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

MULTI-FACTOR AUTHENTICATION SERVICE

Privacy, Security, and Compliance Simplified with Multi-Factor Authentication Service

Verify and authenticate users' identities before granting access to your server environment. Our simple and secure Multi-Factor Authentication Service is the easiest way for users to verify their identity before being granted access to your Linux (SSH) and Windows Servers (RDP).

What is Multi-Factor Authentication Service (MFA Service)?

Multi-Factor Authentication Service (MFA Service) requires two or more methods (also referred to as factors) to verify your identity. These factors can include something you know - like a username and password, plus something you have - like a smartphone app to approve authentication requests.

Why do I need Multi-Factor Authentication Service (MFA Service)?

Multi-Factor Authentication Service (MFA Service) is one of the best ways to protect against remote attacks such as phishing, social engineering, weak or stolen credentials, and other attempts to take over or hijack your accounts.

By integrating Two-Factor Authentication Service with your Linux and/or Windows Servers, attackers are unable to access your accounts without also possessing your physical device (smartphone, etc.) needed to complete the second factor.

Did you know?

- An employee or contractor is responsible for 2 out of 3 insider threat incidents.
- Negligence based insider threats cost on average $3.8 million per year.
- 52% of users re-use their password for multiple logins.

How does the Multi-Factor Authentication Service work?

During the login process, a verification code will be required in addition to a user's username and password. This adds an extra layer of security to their account. Even if someone else obtains their password, it won't be enough for them to sign in with the compromised credentials.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

MULTI-FACTOR AUTHENTICATION SERVICE

Verification Methods

The verification code can be received by text message, phone call, or by using a simple authentication app on your smartphone. Verification codes can even be received when the user's phone has no cell signal.

Administrators can choose from one or more available methods to verify their users:

SMS Passcodes

A passcode sent to your phone via SMS. Simply enter the code into the login prompt.

Phone Callbacks

Simply answer a phone call and press any key to complete the login process.

TOTP Passcodes

Open an authentication app on your smartphone and simply enter the displayed code into the login prompt. These are known as time-based one-time passcodes (TOTP).

Bypass codes

Useful for lost devices or to provide single event access for contractors.

Find Out More?

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at www.atlantic.net, call 888-618-DATA (3282), or email us at sales@atlantic.net.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS