DUO for...

Duo Security is now part of Cisco.

Federal Access

Former U.S. Federal CIO Tony Scott recommends implementing strong authentication for all agencies and all users.

THE CHALLENGE:
Fulfilling NIST Compliance

Federal agencies are rapidly adopting the cloud to support the Federal Modernizing Government Technology (MGT) Act. At the same time, agencies must deploy two-factor authentication to meet former Federal CIO Tony Scott's recommendation, and to comply with the requirements outlined in the National Institute of Standards and Technology (NIST) 800-53/63/171 and the updated NIST Cybersecurity Framework (CSF 1.1).

Duo provides federal agencies easy and effective secure access and authentication to help bridge the gap from current network architectures to modern "trusted endpoint" based architectures. Based on NIST guidance in SP-800-63-3, Duo can be used as an alternative to CAC/PIV or PIV-D solutions in cases where they can't be used or are not supported.

DUO IS FEDERAL-READY

NIST

GSA

AWS GovCloud (US)

section 508 compliance

FIPS

SEWP V

"The flexibility provided by Duo, the overall ROI and the API capability makes for a very robust product that is easily deployed and managed. Those features alone put it light years ahead of the competition."

IT Manager
Federal Government

Duo for Federal Access

THE SOLUTION:

Duo's Trusted Access

Duo's trusted access solution aligns with NIST 800-53/63/171 requirements in three ways:

01

Scale to All Users

Easily integrate Duo with hundreds of applications. Duo has out-of-the-box integrations with local Windows logon, Linux and Unix console, remote access VPNs, and cloud applications, such as Office 365, Salesforce, Box, and Google.

For end users, Duo offers simple one-tap, push notification-based authentication. Duo also offers OTP-based hard and soft tokens and YubiKeys that meet FIPS 140-2 requirements.

02

Visibility Into Devices

Get visibility into all end-user devices running Windows, MacOS, iOS or Android – without requiring agents. Pinpoint devices running out-of-date OSs, browsers, Flash and Java. Identify devices with unwanted security postures, such as jailbroken/rooted devices or devices without encryption enabled. Create security policies for application access based on these factors and others, such as user location and network type.

03

Complement Your PIV/CAC Solution

Strengthen access security into applications when users have a Common Access Card (CAC) or Personal Identity Verification (PIV), solutions which many agencies have already deployed.

Duo works alongside CAC/PIV and PIV-D solutions and can also be used as an alternative to them in cases where CAC/PIV are not ideal or supported, such as modern auth support in cloud infrastructure or other systems that might not support certificate-based authentication (CBA).

"

Duo has increased the level of security in the business to the point that IT can sleep well at night knowing the business has the best two-factor authentication protecting the environment."

Charles Basile
IT Administrator
Teledyne Technologies