Duo for...

Duo Security is now part of Cisco.

Continuous Diagnostics and Mitigation

Duo helps federal agencies and other public sector organizations ensure secure access to the right applications.

Fulfilling DHS CDM Phase 2 with Duo

Duo Security, now part of Cisco, is a trusted vendor for the U.S. Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program under Phase 2.

Duo **helps federal agencies** and other public sector organizations ensure their users have access only to the applications and services that are appropriate for their role in the organization, whether on the network or in the cloud.

Duo satisfies NIST's Digital Identity Guidelines (NIST 800-63-3b) and DFARS/FARS (NIST SP 800-171).

"Duo is the most successful end-user facing solution I've ever been involved in deploying."

Lance Honer, Manager of Cybersecurity, Day & Zimmermann

DUO IS FEDERAL-READY

FedRAMP

GSA

NIST

section 508 compliance

FIPS 140-2 CRYPTOGRAPHY

SEWP Approved SEWP V Federal Government IT Provider

for DHS CDM

Duo Secure Access

Duo offers a cloud-based, user-centric zero-trust security platform for all users, all devices and all applications. It provides multi-factor authentication (MFA) and access authorization features to help organizations implement strong access controls in their environment.

Every time a user attempts authentication to a protected application or resource, Duo checks device health and security posture, and allows access only when all requirements have been satisfied. It works with both bring your own devices (BYOD) and managed devices.

Duo and CDM

The intent of CDM is to identify and continuously monitor the status of users, networked devices and systems, and mitigate identified risk. CDM Phase 2 addresses the general question "who is on the network?" Duo offers strong capabilities to address CDM Phase 2's four new tool functional areas (TFA).

TRU (Trust)

Duo ensures trust by providing strong MFA and rich access control policies to ensure a user is who they say they are and have access only to the applications and services that are appropriate for their role in the organization.

CRED (Credential)

Duo ensures account credentials with MFA and access controls. In order to maintain secure separation between first and second factors of authentication, Duo does not manage or handle passwords – these always remain with the identity provider (such as Microsoft's Active Directory).

BEH (Behavior)

Duo supports appropriate behavior by enabling organizations to enforce knowledge-based access requirements – restricting access to specific resources or applications until an end user meets training and knowledge management requirements.

PRIV (Privilege)

Duo prevents access beyond what is needed to meet the business mission by managing access through a rich policy engine. This enables organizations to manage access privileges across a broad set of applications and resources, whether on the network or in the cloud.

FedRAMP Authorized Designation

Duo's cloud-based Duo Federal MFA and Duo Federal Access products offer federal agencies and other public sector organizations an alternative to traditional card and token-based authentication methods with two-factor authentication (2FA) technology, among other capabilities.

Duo's Federal Editions are FedRAMP Authorized, FIPS compliant and tailored to meet the strict security requirements of federal agencies and public sector organizations.