

Duo for Compliance

Complex regulations and security frameworks can make it challenging to select security products that address all of the needs and requirements to be compliant. This quick guide will help you understand how Duo editions can help your business with compliance requirements and regulatory framework guidelines.

The Challenge

Risk and Compliance teams within organizations need to work closely with Security teams to ensure that the security practices being implemented follow recommended best practices, align with compliance requirements, and adhere to data privacy regulations.

If these teams are not in alignment, it can result in heavy financial and reputational penalties. Teams need to work together to find the right solutions that can increase security and assist with compliance without impacting user productivity.

The Solution

Duo provides organizations with best-in-class security technology and a trusted partnership that can help build and maintain a well-rounded security program. We believe that by focusing on security fundamentals and best practices, you can easily achieve compliance.

We focus on protecting your employees with strong phishing and push fatigue resistant multi-factor authentication. In addition to protecting your employees, we provide the ability to ensure only trusted and managed devices have access to your data.

Built with a focus on security and usability, Duo's solutions can help organizations establish security practices that provide a great user experience while aligning with certain areas of compliance guidelines.




Duo offers different editions that provide flexible solutions for organizations to address security projects and requirements. Duo helps you meet components of compliance and regulatory requirements with a secure, easy-to-use platform that provides the foundation for a zero-trust security approach for your workforce.

Meet Compliance Requirements

Every security best practices guide and regulation asks for MFA and device visibility

<p>Meet MFA requirements outlined in PCI-DSS 3.2 Section 8.3</p> 	<p>Helps meet NIST 800-63, 800-53, and 800-171 access security requirements</p> 	<p>Meet DEA's EPCS requirements when approving e-prescriptions</p> 	<p>Aligned with GDPR data protection laws in Europe</p> 	<p>Meet FFIEC requirements for financial applications</p> 	<p>Get visibility into personal devices used to access PHI</p> 	<p>Aligned with guidelines for identification and authentication</p> 
---	---	--	---	---	--	--

Avoid Consequences

 Damages, Lawsuits, and Fines	 Lost IP, Business, and Reputation	 Privacy Violations
---	---	--

Duo Helps You Follow Best Practices

Overarching security frameworks like ISO 27001 and NIST provide recommendations for security best practices, which inform many compliance guidelines that span across multiple industries and verticals.

Foundational Frameworks	HOW DUO EDITIONS HELP		
	Duo Essentials	Duo Advantage	Duo Premier
<p>ISO 27001(2022) International Organization for Standardization 5.15, 5.16, 5.33, 5.34, 8.3, 8.4, 8.5, 8.15, 8.18, 8.21, 8.26, 8.31, 8.32, 8.33</p>	<ul style="list-style-type: none"> Syncs with existing identity access management (IAM) solutions Provides a layer of strong authentication Automates user provisioning and de-provisioning of authentication factors Reports on event logs recording user activities Allows only trusted endpoints to access specific applications 	<ul style="list-style-type: none"> Includes everything from Duo Essentials Enforces adaptive access policies for role-based access Controls access to systems and applications with a secure log-on procedure, where required by the access control policy Limits access to source code to verified users 	<ul style="list-style-type: none"> Includes everything from Duo Essentials and Duo Advantage Provides secure access to internal applications without exposing them to external risk Enables limited access for external third-parties to specific applications and systems
<p>SOC2 Systems and Organization Controls Report 2017 Trust Services Criteria (TSC) Reference Number: CC6.1, CC6.2, CC6.3, CC6.6, CC6.7, CC7.1</p>	<ul style="list-style-type: none"> Provides automatic provisioning and deprovisioning of MFA tokens Integrates with a SIEM for fraudulent push authentication reported by users Provides visibility of endpoints accessing business applications 	<ul style="list-style-type: none"> Implements the concepts of least privilege to establish role-based access policies to applications Restricts access from devices that are out of date and provides users with self-remediation options 	<ul style="list-style-type: none"> Restricts access to known devices and locations Provides secure external access that can be tracked and limited to protect internal resources Establishes trust in BYOD in environments with agentless an approach

Duo Helps Address Areas of Compliance Guidelines

Risk and Compliance teams will often work with Security teams to ensure their security strategy is in line with the compliance requirements to avoid potential financial penalties.

Compliance Guidelines	HOW DUO EDITIONS HELP		
	Duo Essentials	Duo Advantage	Duo Premier
<p>EPCS Electronic Prescriptions for Controlled Substances (75 FR 16236, March 31, 2010) [Docket No. DEA218, RIN 1117AA61]</p>	<ul style="list-style-type: none"> Protects individual /institutional practitioners from misuse of their credentials by insiders, as well as from external threats. Meets cryptographic requirements and is verified by a DEA accredited auditor 	<ul style="list-style-type: none"> Includes everything from Duo Essentials Ensures that only authorized practitioners are able to gain access and digitally sign for controlled substance distribution with granular access policies based on role 	<ul style="list-style-type: none"> Includes everything from Duo Essentials and Duo Advantage Permits access only to known/trusted devices accessing systems for e-prescribing Enforces security controls and encryption on BYOD devices
<p>FFIEC Federal Financial Institutions Examination Council Version Sept 2016 Title: II.C.5, II.C.7, II.C.7(a), II.C.7(e), II.C.10(d), II.C.13(e), II.C.15(b), II.C.15(c), II.C.15(d), II.D, III.C</p>	<ul style="list-style-type: none"> Provides controls to require multi-factor authentication for access to local workstations Provide a detailed view of the security posture of the devices that are connecting to sensitive applications Implements a robust authentication method consistent with the criticality and sensitivity of the application. 	<ul style="list-style-type: none"> Enforces access policies based on group membership for sensitive applications Provides guidance for devices up-to-date and remediation through self-service Blocks access for unauthorized devices connecting to applications 	<ul style="list-style-type: none"> Restricts remote access to authorized network areas and applications Ensures seamless and secure remote access to sensitive applications Ensures BYOD devices connecting to sensitive information are reported and meet the latest security criteria before granting access.
<p>GBLA Gramm-Leach-Bliley Act FIL222001 Title: V Subtitle A Section 501(3)</p>	<ul style="list-style-type: none"> Provides MFA to strengthen secure password policy 	<ul style="list-style-type: none"> Ensures devices and browsers accessing sensitive application are patched and updated Verifies that protected screen lock is enabled on mobile devices Makes sure device encryption is enabled on mobile devices 	<ul style="list-style-type: none"> VPN-less remote access to private applications (hosted on-premises or multi-cloud environments) Secure access to internal web applications Secure remote access to applications hosted in Amazon WebServices (AWS), Azure, and Google Cloud Platform (GCP)
<p>HIPAA Health Insurance Portability and Accountability Act CFR 45 revised October 1, 2007 Standard: 164.304, 164.308(a)(1), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(4)(ii)(B), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(d)</p>	<ul style="list-style-type: none"> Implements strong authentication requirements that protect electronic protected health information (ePHI) from unauthorized access Provides visibility into endpoints accessing systems that contain PHI Provides emergency access options in the event of a lost or stolen authentication method 	<ul style="list-style-type: none"> Implements access controls to reduce risks and vulnerabilities Enforces access policies to ensure that ePHI is not available or disclosed to unauthorized persons Enforces access restrictions based on group membership to applications containing ePHI Prompts users for self-remediation on devices that don't meet security controls 	<ul style="list-style-type: none"> Enables secure BYOD access to ePHI by establishing devices meet minimum security requirements Establishes security protections for remote access to protected applications containing sensitive ePHI
<p>NERC North American Electric Reliability Corporation CIP005 Table R2 Part 2.3, CIP007 Table R5 5.1, CIP0102 Table R2 2.1</p>	<ul style="list-style-type: none"> Enforces multi-factor authentication for user access 	<ul style="list-style-type: none"> Offers user training for user security and audit reporting Blocks access from unknown sources 	<ul style="list-style-type: none"> Enforces controls for remote access to protected resources Restricts access to managed devices
<p>PCI DSS Payment Card Industry Data Security Standard Version 4.0 Requirements: 8.3, 8.4, 8.5</p>	<ul style="list-style-type: none"> Provides strong MFA capabilities to protect access into the cardholder data environment 	<ul style="list-style-type: none"> Restricts access to systems and applications containing cardholder data to verified users and healthy devices 	<ul style="list-style-type: none"> Validates user identities and establishes trust in devices Reduces the risk of accessing the cardholder data environment from outside the network

Duo Helps Provide Technical Controls for Data Privacy

With additional requirements around data privacy impacting businesses with presence, there is added complexity for organizations as they strive to implement security solutions to protect operations while rolling out new technologies and keeping employees productive.

Data Privacy Controls	HOW DUO EDITIONS HELP		
	Duo Essentials	Duo Advantage	Duo Premier
<p>PIPEDA Personal Information Protection and Electronic Documents Act Guidelines for Identification and Authentication</p>	<ul style="list-style-type: none"> Provides strong authentication options for users accessing protected systems 	<ul style="list-style-type: none"> Includes everything from Duo Essentials Provides the ability to elevate or relax authentication requirements based on application sensitivity with access controls Restricts access from unknown locations or devices 	<ul style="list-style-type: none"> Includes everything from Duo Essentials and Duo Advantage Restricts remote access to applications containing sensitive information Provides technical controls to deliver external access while protecting internal systems
<p>GDPR EU General Data Protection Regulation, Regulation (EU) 2016/679 Article 5 Section 1(f) and 2, Article 24 Section 1, Article 32 Section 1(b) and 2</p>	<ul style="list-style-type: none"> Prevents unauthorized access to sensitive information Delivers detailed logs of access events 	<ul style="list-style-type: none"> Provides granular policy controls to manage and restrict access 	<ul style="list-style-type: none"> Provides visibility into which corporate-managed and unmanaged devices are accessing company applications and data
<p>CCPA California Consumer Protection Act Section 1798.150. (a) (1)</p>	<ul style="list-style-type: none"> Verifies users' identities with strong two-factor authentication before granting access to applications that may contain personal information 	<ul style="list-style-type: none"> Ensures only trusted and authorized users and healthy devices can access critical business applications and the data they store 	<ul style="list-style-type: none"> Ensures that only healthy, trusted devices gain access to sensitive resources and can block unauthorized devices

Duo Helps Meet Federal Compliance Regulations

The Federal government has very specific and strict compliance standards. Duo works with Federal and Public Sector organizations to meet security compliance standards. If you have questions about Cisco's compliance, go to the Customer Information Clearinghouse and make a request through our Trust Portal.

Compliance Guidelines	HOW DUO EDITIONS HELP	
	Duo Federal MFA	Duo Federal Access
<p>Products from Duo Security follow guidance as provide by NIST in attempts to comply with 800-53 and 800-63 Federal Edition has achieved FedRAMP level: Moderate National Institute of Standards and Technology (NIST) 800-171 Rev2 SP 800-63 B guidance NIST 800-53 Control: IA2, IA3, IA5, IA6, MA4, SC7, SC11, 800-63 Control: AL2 AL3 NIST 800-171 Control: 3.11, 3.12, 3.1.8, 3.1.11, 3.1.12, 3.1.14, 3.1.15, 3.1.18, 3.1.20, 3.3.1, 3.3.2, 3.3.8, 3.4.2, 3.5.2, 3.5.3, 3.5.7, 3.7.5 Authenticator Assurance Level (AAL) 2</p>	<ul style="list-style-type: none"> Uniquely identifies and authenticates users Meets NIST digital identity guidelines Limits system access to authorized users Provides inventory of all endpoints accessing protected applications Provides local access protections online/offline for DFARS requirements 	<ul style="list-style-type: none"> Includes everything from Federal MFA Limits applications that authorized users are permitted to access Grants access only to healthy and compliant devices Adds a layer of authentication for privileged accounts Provides Asset Management, Risk Assessment, Access Control, Data Security, Protective Technology, and Continuous Monitoring
<p>CMMC 2.0 NIST 800-171 Cybersecurity Maturity Model Certification (CMCC) for third-party contractors</p>	<ul style="list-style-type: none"> Provides defense contractors strong MFA across multiple domains including Access Control (AC), Identification and Authentication (IA) and Audit and Accountability (AU) as well as Media Protection (MP) 	<ul style="list-style-type: none"> Protects every application, is easy to deploy, removes telephony, is end-to-end FIPS capable, and allows actions to be logged and traceable to a specific user
<p>CJIS Criminal Justice Information Services Version 5.9 Section: 5.5.2.3, 5.5.6.1, 5.5.6.2, 5.6, 5.13.4.1, 5.13.7.1, 5.13.7.2, 5.15 *Can also be achieved with non-FedRAMP editions</p>	<ul style="list-style-type: none"> Supports multiple ways to authenticate Provides automated method of authentication methods Provides methods for users to report fraudulent access attempts 	<ul style="list-style-type: none"> Ensures end users have up-to-date security patches on their devices Provides guidance for self-service remediation for systems that are out of date Meets the MFA requirement for PAM, Gen users, device policy etc.
<p>FIPS 140-2 and FIPS 140-3 Federal Information Processing Standards Control: 1402 Iv13</p>	<ul style="list-style-type: none"> Is FIPS compliant with validated cryptographic modules in the Federal Editions Zero-touch implementation for FIPS 140-2 and FIPS 140-3 compliant mobile authentication; no configuration required by administrators 	

This resource highlights how Duo's editions address specific areas within the various frameworks, compliance requirements, and data privacy guidelines. Duo should be considered an integral component within overarching security strategies with its agnostic approach. It integrates with and complements other key security solutions in the market to empower organizations to meet compliance requirements.