# Security for DocuSign eSignature

## Security is in DocuSign's DNA, and like all of our products, DocuSign eSignature is researched, designed, and developed with security as a top priority.

This document outlines the security technologies, policies, and practices that protect your documents and data within DocuSign eSignature, including information that enables you to configure security in accordance with the specific risk management and compliance requirements of your organization. For security details common to all DocuSign products, visit product security on the Trust Center.

### Physical and logical security

DocuSign maintains around-the-clock onsite security with strict physical access control that complies with industry-recognized standards, such as SOC 1, SOC 2, and ISO 27001.

We also use world-class security software and hardware to protect the physical integrity of DocuSign eSignature and all associated computer systems and networks that process customer data. We do this through a centralized management system that controls access to the production environment through a global two-factor authentication process.

This isolated production environment is protected by industry-leading network management systems, anti-virus software, and malware detectors. The anti-virus software is integrated with processes that automatically generate alerts to DocuSign's cyber incident response team if potentially harmful code is detected.

### Security testing and vulnerability management

The quality and integrity of DocuSign eSignature is ensured by a formal product development lifecycle that includes secure coding practices in accordance with OWASP. Rigorous automated and manual code reviews are designed to pinpoint security weaknesses. We also perform internal and external vulnerability scans and penetration tests against the DocuSign eSignature production environment. Any identified weaknesses from these industry-compliant tests are remedied in a commercially reasonable manner and in a timeframe commensurate with their severity.

### Security monitoring

We monitor DocuSign eSignature from both an operational and a security perspective. Intrusion prevention and detection events are logged, and tailored alerts are sent to our operations and security teams to ensure that DocuSign eSignature can be used without security exposure from any location by those authorized to access it.

## Storage, encryption, and disposal

To ensure your data stays protected, DocuSign follows industry best practices to:

- Logically separate individual customer data
- Encrypt customer data—all data access and transfer activities use HTTPS and other secure protocols, such as SSL, SSH, IPsec, SFTP, or secure channel signing and sealing
- Support only recognized cipher suites
- Encrypt all documents with AES 256-bit encryption or the most recent FIPS-approved methods
- Provide non-repudiation for all documents generated and signed using DocuSign via a Certificate of Completion
- Maintain a data disposal and re-use policy for managing data assets
- Implement processes for equipment management and secure media disposal

## Business continuity and disaster recovery

DocuSign maintains written business continuity and disaster recovery plans that ensure the continuing availability of DocuSign eSignature. The continuity plan includes crisis management, business recovery, and infrastructure elements, and we test both plans on an annual basis in accordance with ISO 27001 controls.

## Configurable security features

DocuSign eSignature offers the following customer-configurable features:

- *Multi-factor authentication* provides an additional level of assurance that only those authorized to access DocuSign eSignature and associated documents can access them
- *Role-based authorization* for all business transaction types enables you to designate access to specific individuals

## Whitelists for DocuSign eSignature service

DocuSign customers should configure their spam filters and other software to allow for the following whitelisted domains to be accepted. They should also explicitly allow Internet addresses advertised by DocuSign eSignature. It's important to keep up-to-date with our current IP address ranges.

### Domains

We recommend whitelisting all subdomains under the following domains:

- .docusign.com
- .docusign.net

### Akamai CDN

To enhance network performance and security, DocuSign eSignature uses Akamai CDN for static content distribution. DocuSign browser applications use outgoing connections to docucdn-a.akamaihd.net.

DocuSign

**DocuSign endpoint IP addresses**

If customers only need to whitelist the DocuSign endpoint, the following IP addresses apply:

*North America-based and demo accounts (current and continuing):*

**NEW 64.207.216.1 through 64.207.219.254

162.248.184.1 through 162.248.187.254

34.212.7.28

34.213.201.254

34.213.254.17

34.215.124.54

34.215.142.185

34.215.203.190

35.164.40.59

35.167.67.7

52.25.145.215

52.27.85.20

52.34.155.26

52.41.95.219

*European Union-based accounts (current and continuing):*

185.81.100.1 through 185.81.103.254

**DocuSign email IP addresses**

If customers need to whitelist DocuSign's email IP addresses, the following apply:

*North America-based and demo accounts (current and continuing):*

**NEW 64.207.216.1 through 64.207.219.254

162.248.184.1 through 162.248.187.254

34.212.7.28

34.213.201.254

34.213.254.17

34.215.124.54

34.215.142.185

34.215.203.190

35.164.40.59

35.167.67.7

52.25.145.215

52.27.85.20

52.34.155.26

52.41.95.219

52.25.139.174

54.244.242.160

54.244.242.186

54.244.242.190

54.244.242.214

*European Union-based accounts (current and continuing):*

185.81.100.1 through 185.81.103.254

54.93.78.134

54.93.137.237

54.93.151.48

54.93.154.157

54.93.162.246

## Support for Sender Policy Framework (SPF) record checking

To flag and quarantine malicious spam on mail servers, enable both Sender Policy Framework (SPF) lookup functionality and Domain-based Message Authentication, Reporting & Conformance (DMARC). The combination of these technologies helps protect against malware spam attacks. Learn more about SPF at http://www.openspf.org/ and DMARC at http://www.dmarc.org/.

Follow Us:

### About DocuSign

DocuSign is changing how business gets done by empowering anyone to transact anytime, anywhere, on any device with trust and confidence. DocuSign keeps life moving forward.

For U.S. inquiries: toll free 866.219.4318 | docusign.com

For EMEA inquiries: phone +44 203 714 4800 | email emea@docusign.com | docusign.co.uk

For Australia and NZ inquiries: toll free: Sales: 1 800 255 982 - Support: 1 800 083 139 | docusign.com.au



eSignature Security_ DSRS030119PSSPUBGLB