CITRIX SYSTEMS, INC.

Citrix Cloud Services: Customer Content and Log Handling

October 12, 2018

Table of Contents

Overview

This document describes the types of Customer Content and Logs that Citrix Cloud services collect.[1] The audience for this information is Security Officers, Compliance Officers, and Information Auditors and others whose role includes the handling of cloud data in their organization. This document only applies to Citrix Cloud platform regions, Citrix Virtual Apps and Desktops, Citrix Endpoint Management, Smart Tools and Citrix Content Collaboration services. Details for other services will be included in a future version of this document. This information is subject to change without notice.

The following terms are used in this document:

Customer Content means any data uploaded to Customer's account for storage or data in Customer's computing environment to which Citrix is provided access in order to perform Services.

Log means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.

Personal Data means any information relating to an identified or identifiable natural person (as further defined in Article 4 of the EU General Data Protection Regulation) to which Citrix is provided access in order to provide the Services described in this document.

Customer Content and Logs can include Personal Data, including but are not limited to proper names, user IDs, phone numbers, email and IP addresses.

How Citrix handles Customer Content stored on its systems

Customers determine the Customer Content that they choose to load to a Citrix-managed service and Citrix processes that data as a data processor for its Customers. Citrix does not have access to Customer Content that might contain Personal Data (for example, Microsoft Office files, databases, and so on) except as requested for support or troubleshooting, other than as described under "Per-service information" beginning on page 4.

Geographic location

Citrix Cloud services are available across multiple regions (for example, EU, US or Asia Pacific South). However, a customer's cloud account can only be homed in one region. Once the customer chooses a region, the account cannot be moved between regions.

Logs may be replicated and accessed globally to support the Services, including auditing for performance of the Services, support or troubleshooting, and to allow for cross-region authentication (for example, when an EU based Administrator needs to access a U.S. based service).

See Citrix Cloud Geographical Considerations for more details.

[1] The Citrix Privacy Policy available at https://www.citrix.com/about/legal/privacy.html describes how Citrix uses and protects personal information that Citrix collects in connection with the operation of its business (e.g., in Marketing, Sales, Finance and Partner operations). By contrast, this document addresses the collection and handling of Customer Content and Logs in connection with the performance of Citrix Cloud services. In this capacity, Citrix acts as a "data processor" for its customers with respect to the handling of Customer Content. Further information may be found in the Citrix Data Processing Agreement available here.

Collected across all Citrix Cloud services

The Citrix Cloud platform collects the following Log data related to Citrix cloud-based services.

Inflight and stored user Log data

- Administrator user name
- Administrator first and last name
- Administrator email address
- Administrator phone number
- Administrator address
- Administrator country
- Administrator password
- End-User principal used to log on by end-users (example: domain\username)
- End-User name
- End-User , first and last name
- Common Active Directory (AD) properties for end-users

Inflight and stored device Log data

- Internet facing IP address used by the administrator to access the service (not stored)
- Active Directory attributes may also be seen inflight

Logging

For administrators, Citrix logs:

- Name (first name, last name, display name)
- Email address

For end-users, Citrix logs:

- Name (first name, last name, display name, and other AD properties containing the name).
- AD properties that typically contain the email address.
- Any AD properties, including custom properties, whose names do not match “email” “telephone” or “address.”

Backup

For all services, all inflight or stored Logs or Customer Content listed in this document may be included in backups. Citrix performs the following types of backups:

- Online backups may be made to any of the following depending on the service: Azure Blob storage, AWS S3, AWS Elastic Block Store, and Azure SQL.
- One-way replication of data between Microsoft Azure and Amazon AWS.
- Offline or offsite backups are not made for any service.

Backups may contain any of the data discussed in this document and may be stored in different regions for redundancy.

Third party services that may store or process Logs on behalf of Citrix

Citrix may choose, when appropriate, to store or process Logs within the services listed below. These third-party services are subject to change, and not all third party services are utilized by all Citrix Cloud services. Unless otherwise noted, these services are US-based.

Third Party Service	Purpose
Alert Logic	Security monitoring
Amazon Web Services	Storage and diagnostics
Chef	Code automation
Crashlytics	Traffic/event analysis
Dome9	Connectivity monitoring
Fabric	Traffic/event analysis
Google Analytics	Traffic/event analysis
Google Tag Manager	Script management
LaunchDarkly	Traffic/event analysis
Microsoft Azure	Storage and diagnostics
Mix Panel	Traffic/event analysis
New Relic	Connectivity monitoring, logging and analytics
Pager Duty	Internal communication tool
Pendo	In-app communications, analytics
Qualys	Security monitoring
SalesForce	Customer service management, authentication, and communications
SendGrid	Email service provider
Slack	Internal communication tool
Splunk (Separate US and EU instances)	Connectivity monitoring, logging and analytics
Uservoice	Optional discussion board

Per-service information

This section describes Customer Content and Logs stored by each Citrix Cloud service, in addition to that detailed above for all services.

Citrix Virtual Apps and Desktops

Citrix Virtual Apps and Desktops service do not collect, inspect or transfer Customer Content files (for example Microsoft Word and Excel files) from the virtual machines that end-users access. End-users' virtual machines are under customer's control.

In addition to the common elements described above, the application and desktop service collects:

Stored data

No Customer Content or Logs are collected in addition to that listed in the section “

Collected across all Citrix Cloud services" earlier in this document.

Inflight data

- End-user password
- Name of client device

Citrix Endpoint Management

Citrix Endpoint Management provides regional control planes for locations in US, EU, and Asia Pacific regions. Within each region there may be multiple locations. Some data such as email address may be used across regions (e.g., for auto discover service).

Inflight and stored data

User data inflight and stored

- Citrix Endpoint Management cookies
- Connection details
- Google enterprise owner email address
- Mobile number (if applicable)

Device data (stored on per region basis – note backups of this data may be stored on other regions)

- Serial Number
- IMEI
- WiFi MAC address
- Bluetooth MAC address
- Memory and storage
- CPU type and speed
- OS version
- IP address
- Screen resolution
- Jailbreak status
- ActiveSync ID

Citrix Content Collaboration

Inflight stored data

User data

- User Password Hash
- Admin Security Question in its databases
- File and folder names in Logs

Customers may also contribute Personal Data as part of database field data (fields for File Name, Folder Name, and Notes are free-form text).

The document preview engine uses Microsoft Office 365 when customers have O365 entitlement. Citrix native preview is used in several capabilities like Feedback, Approval, and view with watermark. Signature and workflow features similarly will be processed through Citrix RightSignature in the US. Any Personal Data contained in file names or file content may be processed by the Office 365, Citrix native preview technologies or Citrix RightSignature.

Regional considerations

Citrix provides separate US and EU instances of the Citrix Content Collaboration control plane; Citrix does not transfer Customer Content between or outside of these regions. See "Content Collaboration locations and Storage Zones" section of Citrix Cloud Geographical Considerations for more details.

Smart Tools

In addition to that identified in the section "

Collected across all Citrix Cloud **services**" on page 4, Smart Tools also collects DNS and names of site components.

Lab Services

Lab services are unsupported, may change over time, and may not necessarily become Citrix Cloud services. For more information, see the Labs section in Citrix Cloud.

Frequently asked questions

Can I opt out from any logging or storage of the Logs mentioned in this document?

No, it is not possible to opt out of logging or storage of Logs. These are required to ensure that our services function optimally.

Are the products detailed in this document compliant with GDPR?

Citrix products and services are designed to facilitate your GDPR compliance by supporting GDPR requirements around data management, access and security. Citrix has performed data protection impact assessments of its products and Citrix strives to provide functionality that will assist your ongoing compliance efforts. Citrix offers a Data Protection Addendum, including EU Standard Contractual Clauses (Processor), which are available here.

What about other Citrix Cloud services not mentioned in this document?

Additional services in Citrix Cloud will be included in future revisions of this document.