citrix

White Paper

Citrix Cloud Services

Customer Content and Log Handling

September 14, 2020

Table of contents

Abstract

This article describes Citrix's collection and handling of Customer Content and Logs in connection with the performance of the Citrix Cloud services specified below.

The audience for this article is Security Officers, Compliance Officers, and Information Auditors and others whose role includes the management, handling and oversight of cloud data in their organization. This article only applies to Citrix Workspace, Citrix Virtual Apps and Desktops, Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops), Citrix Endpoint Management, Citrix Content Collaboration, Citrix Analytics Service, Citrix Intelligent Traffic Management, and Citrix Application Delivery Management (collectively the "Cloud Services"). Details for other Citrix Cloud services may be included in future versions of this article. For a more detailed description of the Cloud Services and the related legal terms and conditions, customers should refer to their master agreement and applicable Cloud Services order documentation (collectively the "Agreement") as well as online service descriptions at https:// www.citrix.com/buy/licensing/saas-service-descriptions.html and/or product documentation available at https://docs.citrix.com/.

This information is provided "AS-IS" without warranties of any kind (express or implied) and is subject to change at Citrix's discretion.

The following terms are used in this article:

- **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 the Services.
- **Log** means records of Services, including, but not limited to, data and information on performance, stability, usage, security, support, and technical information about devices, systems, related software, services or peripherals associated with Customer's use of Services.
- **In-flight** means the time when Customer Content or Log data is actively moving from one location to another within the Services environment(s). Some In-flight data may be stored as described in the sections below.
- **Stored** means data at rest, or inactive Customer Content or Log data within the Cloud Services environment(s).
- **Personal Data** means any information that can identify a unique individual, directly or indirectly, in particular by reference to an identifier such as a name, an identification. Number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of individuals (also known as Personal Information).

This information is provided "AS-IS" without warranties of any kind (express or implied) and is subject to change at Citrix's discretion.

Citrix Cloud Services Overview

Customers determine the Customer Content that they choose to upload to a Citrix Cloud Service, and Citrix processes that data as a data processor for its Customers. Citrix does not access Customer Content (for example, Microsoft Office files, databases, and so on) except as requested for support or troubleshooting, and as further described in service-specific sections in this article, in other service specific documentation which can be found on the Citrix Trust Center or in the contract for Cloud Services.

Security

The Citrix Services Security Exhibit describes the security controls applied to Citrix Cloud Services and other services, including access and authentication, security program management, business continuity, and incident management. The Citrix Services Security Exhibit is available here.

Geographic location

Citrix Cloud Services are available across multiple regions. However, a customer's Cloud Services environment may be located only in one region. When a customer is onboarded to Citrix Cloud, it is asked to choose one of the following regions:

- United States
- European Union
- Asia Pacific South

Once the customer chooses a region, the environment storing its Customer Content may not be moved during the term of the Cloud Services.

Citrix stores certain Customer Content and other information related to the customer's use of the Cloud Services in the customer's chosen region, which includes:

- Citrix Cloud Services administrator and end-user details, including the name, username, and password.
    - Passwords are hashed and salted when stored, and sent over SSL/TLS
- Data resulting from traffic directed through your region by any connectors you install, such as authentication data using your domain controllers (whether managed on your premises or through your subscription with a public cloud vendor).
- Information used to map users to library offerings. For example, if you add Microsoft Office to your library as an offering for your users, and then add five users to that offering as subscribers, the data linking each user to that offering (such as user name and domain name) is stored in your region.
- Data about users for any Cloud Services available in your region, such as data used for Citrix Endpoint Management in your region (e.g., name, address, and telephone number).

Logs and Customer Content may be replicated and accessed globally as necessary to support the Cloud Services, including support or troubleshooting, monitoring performance, security, auditing, and to allow for cross-region authentication (for example, when an EU-based support engineer needs to access a US-based environment).

See Geographical Considerations for more details.

Customer Content Collected in Specific Citrix Cloud Services

Citrix Workspace intelligent features

Citrix Workspace intelligent features, such as Data Integration Provider, Credential Wallet, and Intelligent Microapps, collect Customer Content and Logs that may be in-flight, stored or both. For more information about these features, please see the Microapps Technical Security Overview and the Citrix Microapps Service Tech Brief. See below for information about what Customer Content and Logs are stored and in-flight.

Stored data

In addition to information detailed in the Logs collected across the Cloud Services section above, Citrix Workspace intelligence features also collect and store the following additional data:

- User notification scoring data
- Notification card data
- Data cache from enabled microapp system of record integrations as configured by the customer
- Encrypted system account credentials and OAuth 2.0 tokens. This is **not** stored or logged in plaintext.

In-flight data

In addition to the stored elements described above, Citrix Workspace intelligent features takes action on certain in-flight data as follows:

- The Data Integration Provider (DIP) retrieves data from the system of record, and streams it to the microapp service.
- The microapp service sends raw events to Citrix Analytics
- The microapp service retrieves data from the data cache
- Notifications are sent to endpoints

Citrix Virtual Apps and Desktops

Citrix Virtual Apps and Desktops provides virtualization services designed to give IT control of virtual machines, applications, and security while providing anywhere access for any device. For more information about the service, please see the Citrix Virtual Apps and Desktops service product documentation. The Citrix Virtual Apps and Desktops service does 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 the customer's control.

Stored data

No Customer Content or Log data is stored in addition to the data listed above in the Logs collected across the Cloud Services section.

In-flight data

In addition to the elements described above, the Citrix Virtual Apps and Desktops Cloud Service collects:

- Name of client device

Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops)

Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops) delivers Windows apps and desktops from Microsoft Azure. Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops) offers cloud-based management, provisioning, and managed capacity for delivering virtual apps and desktops to any device. Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops) service does not collect, inspect or transfer Customer Content files (for example Microsoft Word and Excel files) from the virtual machines that end-users' access.

Responsibility for end-users′ virtual machines in Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops) service is shared between the customer and Citrix. For more information, see the Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops) Technical security overview.

Stored data

No Customer Content or Log data is stored in addition to the data listed above in the Logs collected across the Cloud Services section.

In-flight data

In addition to the stored elements described above, the Citrix Virtual Apps and Desktops for Azure (formerly Managed Desktops) Cloud Service collects:

- Name of client device

Citrix Endpoint Management

Citrix Endpoint Management is a solution for managing endpoints, offering mobile device management (MDM) and mobile application management (MAM) capabilities. This applies to the control plane, which is where the Citrix Endpoint Management database is located. It is also the central location for all enrolled device traffic, such as enrollments, device check-in, and app store traffic. Data traffic, such as VPN and mail, does not transverse the control plane.

Stored data

In addition to the stored elements described above, the Citrix Endpoint Management collects:

User data:

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

Device data:

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

In-flight data

Citrix Endpoint Management Cloud Services also collects in-flight the user data described above in the "Stored Data" section.

Citrix Content Collaboration

The Citrix Content Collaboration Cloud Service (formerly ShareFile) is designed to enable the customer to easily and securely exchange documents, send large documents by email, and securely handle document transfers to third parties. Learn more information about Citrix Content Collaboration by visiting Citrix Content Product Documentation.

Stored data

In addition to the stored elements described above, the Citrix Content Collaboration collects:

- User data:
  - Admin Security Question in its databases
  - File and folder metadata (such as name, size, and type)
  - Uploaded Customer Content in Citrix Managed Storage Zones

In-Flight data

In addition to the in-flight elements described above, the Citrix Content Collaboration collects:

- File and folder metadata (such as name, size, and type)

Geographic location

Citrix provides separate US and EU instances of the Citrix Content Collaboration control plane, which performs functions such as user authentication, access control, reporting, and brokering. This data is stored in the Customer's US or EU instance, as applicable. See Content Collaboration locations and Storage Zones on the Geographical Considerations page for more details.

Citrix Analytics Service

Citrix Analytics is designed to provide customers with insight into activities in their Citrix computing environment. For more information regarding the collection, storage, and retention of logs by Citrix Analytics Service, please see Citrix Analytics Data Governance.

Citrix Intelligent Traffic Management

Citrix Intelligent Traffic Management is designed to provide customers unmatched visibility into the network experience of shared cloud services and private infrastructures as measured by a world-wide community of website and application users. For more information regarding the collection, storage, and retention of logs by Citrix Intelligent Traffic Management, please see Citrix Intelligent Traffic Management Customer Content and Logs.

Citrix Application Delivery Management

Citrix Application Delivery Management (ADM) Service provides centralized network management, analytics, and automation as a service from the cloud to support virtualized or containerized applications deployed across public clouds and on-premises datacenters. For more information regarding the collection, storage, and retention of logs by Citrix Application Delivery Management, please see the Citrix Application Delivery Management Data Governance Document.

Logs collected across the Cloud Services

Citrix collects the following Log data for the Cloud Services.

In-flight and stored data

- Administrator and end-user user name
- Administrator and end-user first and last name
- Administrator and end-user email address
- Administrator and end-user password
    - Passwords are hashed and salted when stored, and sent over SSL/TLS
- Administrator phone number
- Administrator address
- Administrator country
- End-User principal used to log on by end-users (example: domain\username)
- Internet facing device IP address used by the administrator to access the Cloud Services

Cloud Services Backups

For all Cloud Services, Logs and Customer Content may be included in backups. Online backups may be made to Microsoft Azure and Amazon AWS.

Offline backups are not made for any Cloud Service. Backups may be stored in different regions for redundancy. Please see the Citrix Cloud Business Continuity Overview for more information.

Third-party services that may store or process Logs and Customer Content on behalf of Citrix

Citrix may use third-party service providers to store or process Logs and Customer Content. These third- party service providers are subject to change, and not all third- party service providers are utilized by all Citrix Cloud Services. More details are available in the Subprocessor list for Citrix products.

Frequently asked questions

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

No, it is not possible to opt out of logging or storage of Logs. These are required to ensure that Citrix Cloud Services function properly.

Are the products detailed in this document compliant with GDPR?

Citrix products and services are designed to facilitate customer's 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 at https://www.citrix.com/buy/licensing/citrix-data-processing-agreement.html.

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

Additional services in Citrix Cloud are planned to be included in future versions of this article.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States