White Paper

Citrix Cloud Services Data Protection Overview

November 2022

Contents

Introduction

Citrix understands that data protection is one of the top priorities for our customers when selecting a cloud service. Data protection is also a rapidly-evolving domain and requires enterprises to assess more information over time about the data handling practices of their vendors.

Citrix has created this document to help provide our customers an overview of Citrix Cloud Services data protection practices. It is organized around the following topics:

- Categories of data processed by the Cloud services
- Purposes of processing
- Access controls
- Data center locations
- Cross-border data transfer mechanisms
- Information security
- Information security incident management
- Sub-processors
- Compliance with privacy requirements
- Exercising Data Subject Rights
- Data deletion and retention
- Certifications

Our goal is to provide you the information you need to gain a better understanding of the controls we have implemented in Citrix Cloud Services and an access point for more detailed Citrix Cloud Service documentation.

Citrix Cloud Services Covered

The Citrix Cloud Services Data Protection Overview covers the data protection practices for the following Cloud Services. For a more detailed description of the Cloud Services and the related legal terms and conditions, customers should refer to the applicable online service descriptions and/or product documentation.

Citrix Cloud Platform

Citrix Cloud Services integrate with the Citrix Cloud Platform to provide a unified experience, including optional services for identity and access management with the Citrix Identity Platform. For more information regarding the collection of Customer Content and Logs by Citrix Cloud Platform, please see Appendix A: Citrix Cloud Platform Data Collection.

Citrix DaaS (formerly Virtual Apps and Desktops Service)

Citrix DaaS provides virtualization services designed to give the customer's IT organization control of its virtual machines, applications, and security while providing end-users remote access for any device managed within the environment. For more information regarding the collection of customer content and logs by the Citrix DaaS Cloud Service, please see Appendix B: Citrix DaaS Data Collection.

Citrix Endpoint Management

Citrix Endpoint Management (CEM) is a solution for managing endpoints and offering mobile device management (MDM) and mobile application management (MAM) capabilities. For more information regarding the collection of Customer Content and Logs by Citrix Endpoint Management, please see Appendix C: Citrix Endpoint Management (CEM) Data Collection.

Citrix ShareFile

Citrix ShareFile Cloud Service (formerly ShareFile) is designed to enable the customer to easily and securely exchange documents, send large documents by secure email, and securely handle document transfers to third parties. Learn more information about Citrix ShareFile by visiting Citrix Content Product Documentation. For more information regarding the collection, storage, and retention of Customer Content and Logs by Citrix ShareFile, please see the ShareFile Security White Paper.

Citrix Analytics Service

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

Citrix Intelligent Traffic Management

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

Citrix App Delivery and Security Service

Citrix App Delivery and Security (CADS) service is a part of Citrix Cloud services, and it uses Citrix Cloud as the platform for signup, onboarding, authentication, administration, and licensing. Citrix collects and stores data in Citrix Cloud as part of the CADS service. For more information about what data is collected and methods of data collection, storage, and transmission, please see Citrix App Delivery and Security service Data Governance.

Citrix Secure Private Access

Citrix Secure Private Access is a cloud delivered Zero Trust Network Access (ZTNA) solution that delivers adaptive access to IT sanctioned applications whether they are deployed on-prem, or in the cloud. Citrix Secure Private Access provides access to applications at the application layer and provides customer admins with a set of security controls enabling their users to access IT sanctioned applications on any

device, whether managed or BYO. For more information regarding the collection of customer content and logs by Citrix Secure Private Access service, please see Citrix Secure Private Access Data Governance.

Categories of Data Processed

When performing DaaS services, Citrix processes two types of information:

- **Customer Content**, which means any data that we access or receive or that customers send or upload for storage or processing in order for Citrix to perform services. It also includes proprietary technical information associated with a customer's environment, such as a customer's system or network configurations and the controls a customer selects.
- **Logs**, which means information related to performance, stability, usage, security, support, hardware, software, services or peripherals associated with use of Citrix products or services.

For service-specific information about categories of data processed by the service, please refer to the attached appendices and/or the applicable documentation available on http://www.docs.citrix.com/.

Purpose of Processing

Citrix processes Customer Content only for the purposes of performing the Services in accordance with a customer's written instructions as specified in the contract for services, the Citrix Data Processing Addendum, and in accordance with applicable data Protection Laws.

Citrix does not use a customer's Customer Content to:

- Sell your Customer Content (including any personal data)
- Monitor or track user geolocation
- Produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means

Citrix collects and uses Logs (i) for providing, securing, managing, measuring and improving the Services, (ii) as requested by Customer or its end-users, (iii) for billing, account management, internal reporting, and product strategy, and/or (iv) for compliance with Citrix agreements, policies, applicable law, regulation or government request. This may include monitoring the performance, stability, usage and security of the Services and related components. Logs may include access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant information and activity.

Additional detail can be found in Sections 3 and 4 of the Citrix Data Processing Addendum (DPA).

Access Controls

Citrix Access

Citrix requires the use of access control measures designed to ensure appropriate privileges are assigned and maintained for access to company systems, assets, data and facilities in order to protect against potential damage, compromise, or loss. Citrix follows the Least Privilege Principle, or role-based security, limiting user's access to only what is necessary to perform job functions or roles.

Data Type	Who has access at Citrix	Purpose of access
Customer Content	• Citrix Engineering • Citrix Support	• Performing the Services as specified in the contract for services, the Citrix Data Processing Addendum, and in accordance with applicable data Protection Laws
Logs	• Citrix Engineering • Citrix Product Development • Citrix Support • Citrix Security	• providing, securing, managing, measuring and improving the Services • as requested by Customer or its end-users • billing, account management, internal reporting, and product strategy, and/or • compliance with Citrix agreements, policies, applicable law, regulation or government request

Customer Access

The customer determines the Customer Content that they upload to a Citrix Cloud Service, and is solely responsible for managing access by their users. Citrix enables customers to access and export their Customer Content throughout the duration of their agreement.

Data Center Locations

When a customer is onboarded to a Citrix Cloud Service, they are asked to choose one of the following regions for the location of the data center that will host their Cloud Services environment:

- United States
- European Union
- Asia Pacific South

Citrix Cloud Services use the customer's designated region to store Customer Content and Logs, except with select Logs collected by Citrix sub-processors or for which non-regional storage is necessary for performance of the service, including for support or troubleshooting, monitoring performance, security, auditing, and to allow for cross-region authentication (such as when an EU-based support engineer needs to access a US-based environment). Customer Content and Logs may be accessed on a global basis as necessary to perform the services.

Table 1: Regional Options for Citrix Cloud Services

Service	Data Type	US	EU	APS
Citrix Cloud Platform	Customer Content	Non-regional		
	Logs	Non-regional		
Citrix Identity Platform	Customer Content	Non-regional		
	Logs	Non-regional		
Citrix Endpoint Management[1]	Customer Content	Regional with choice	Regional with choice	Regional with choice
	Logs	Regional with choice	Regional with choice	Regional with choice

Citrix DaaS[2,3]	Customer Content	Regional	Regional	Regional
	Logs	Regional	Regional	Regional
Citrix Application Delivery Management	Customer Content	Regional	Regional	Regional
	Logs	Regional	Regional	Regional
Citrix ShareFile[1,4]	Customer Content	Regional	Regional	US or EU Region
	Logs	Regional	Regional	US or EU Region
Citrix Analytics	Customer Content	Regional	Regional	Regional
	Logs	Regional	Regional	Regional
Citrix App Delivery and Security Service	Customer Content	Regional	Regional	Regional
	Logs	Regional	Regional	Regional
Citrix Secure Private Access[3]	Customer Content	Non-regional		
	Logs	Non-regional		
Citrix Intelligent Traffic Management	Customer Content	Non-regional		
	Logs	Non-regional		

1. Services with more options for service location within regions
2. Citrix DaaS for Google Cloud Platform uses US or EU Region
3. Data used for optional Adaptive Authentication service may be non-regional
4. ShareFile provides additional options for Storage Zones within each region

See Geographical Considerations for more details.

For all Cloud Services, Logs and Customer Content may be backed up to a disaster recovery datacenter and mirrored in real time to a secondary server location to ensure service can be quickly resumed in case of a disruption at the primary location. Backups may be stored in different data centers for redundancy, but are located in the same region as the production environment. Please see the Citrix Cloud Business Continuity Overview for more information.

Information Security

The Citrix Services Security Exhibit describes in-depth the security controls applied to Citrix Cloud Services, including access and authentication, system development and maintenance, security program management, asset management, encryption, operations management, HR security, physical security, business continuity, and incident management.

The security of Citrix Cloud products is controlled by encryption and key management policies. Refer to the Security Development Processes whitepaper for more details on how Citrix employs security throughout its product development lifecycle.

Encryption

Citrix maintains a Certificate, Credential, and Secret Management policy which covers authentication and credential lifecycles, including the requirements for encryption key management.

In transit

All data in transit is encrypted using TLS 1.2 or higher. Citrix Cloud authenticates administrators and stores user tokens as needed (by prompting the administrator explicitly) on encrypted storage.

At rest

Citrix Cloud storage is encrypted during the provisioning process (e.g., Storage Accounts, Microsoft Azure SQL databases, etc.). Encryption keys are AES-256 bit or higher.

Hypervisor passwords have a second level of encryption with keys managed by Citrix.

Key management

Citrix has key management policies in place to ensure the protection of all customer data, and Citrix does not bind keys to identifiable owners.

Citrix manages the unique encryption of customer data in the Citrix Cloud Platform by leveraging cloud native key management.

Depending on the customer's choice of control plane, Azure Key Vault or Google Cloud Platform Secret Manager is used for key management in Citrix Cloud in accordance with Citrix's Global Security Assurance policies and standards. The customer can manage encryption of the data in the resource domain that they control. For DevOps engineers that administer the services, the keys that have access to the services are rotated at a regular frequency. Per Citrix's Security Encryption Standards, database administrators do not have access to keys stored in databases.

Information Security Incident Management

Citrix maintains a comprehensive Cyber Security Incident Response Plan (IRP) that details the processes and procedures Citrix follows to respond, contain and resolve a potential or actual security incident involving (i) Citrix managed networks and/or systems or (ii) any Customer Content, meaning data uploaded to Customer's account for storage or data in Customer's computing environment to which Citrix may be provided access to in order to perform Services. If Citrix determines that Customer Content within its control has been subject to unauthorized access resulting in the loss of confidentiality, integrity or availability, Citrix will notify the impacted customer(s) without undue delay and as required by applicable law.

Additional detail can be found in Section 10 of the Citrix DPA.

Sub-processors

Citrix may engage third-party service providers (also known as sub-processors) to perform specific, limited functions involved in Citrix's delivery of Cloud Services. These sub-processors are obligated to meet Citrix information security standards outlined in the Citrix Supplier Security Standards when accessing, processing, or storing Customer Content or Logs.

These third-party service providers are subject to change, and not all third-party service providers are utilized by all Citrix Cloud Services. For a current list of Citrix Cloud Services sub-processors, the functions they perform and additional information, please refer to the Citrix Sub-processor list.

Additional detail can be found in Section 6 of the Citrix DPA.

Compliance with Privacy Requirements

Citrix describes its Cloud Services privacy practices in the Citrix Data Processing Addendum (DPA), which is posted to the Citrix Trust Center and incorporated into the Citrix Services Agreement used to acquire the Services. Built around the core GDPR data processor requirements but designed to cover all applicable global data protection laws, the DPA specifies, among other things, our limitations on use, controls on third-party providers, legal terms around international transfer of data, incident reporting, procedures for audit and assistance, and data deletion practices.

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. In addition, the international data transfer section of the DPA has recently been updated to incorporate the new EU Standard Contractual Clauses (2021/914/EU).

Citrix will not disclose Customer Content in response to a subpoena, judicial or administrative order, or other binding instrument (a demand) unless required by law. Citrix will promptly notify customers of any demand unless prohibited by law and provide reasonable assistance to facilitate a timely response to the demand.

Additional detail can be found in the Citrix DPA.

Cross-Border Data Transfer Mechanisms

Customers may select specific regions for the location of the data center that will host their DaaS cloud services environment. Citrix may transfer personal data to the United States and/or to other third countries as necessary to perform the services. If this transfer involves personal data subject to applicable data protection laws in the European Economic Area, Switzerland and the United Kingdom to a jurisdiction that has not been deemed to provide an adequate level of data protection under applicable data protection laws and there is not another legitimate basis for the international transfer, then the transfer is subject to either the EU Standard Contractual Clauses and/or the UK SCC Addendum (as applicable) or other valid transfers mechanism available under applicable data protection laws. All other transfers are subject to the data protection terms specified in the Citrix DPA and applicable data protection laws.

Additional detail can be found in Section 7 of the Citrix DPA.

Exercising Data Subject Rights

Citrix will make available to customers the personal data of their data subjects and the ability to fulfill requests by data subjects to exercise one or more of their rights in a manner consistent with Citrix's role as a data processor. Citrix provides reasonable assistance to assist customers with their responses. If Citrix receives a request directly from a customer's data subject to exercise one or more of their rights, Citrix will direct the data subject to the customer unless prohibited by law.

Additional detail can be found in Section 8 of the Citrix DPA.

Data Retention and Deletion

Active accounts

Customer Content, files and golden images (required for provisioning), stay under customer control and protection. The customer is responsible for managing encryption, backup, and recovery related to customer's user data and environment.

Citrix has documented retention policies that permit the retention of logs for as long as the data is necessary to provide the services and as required by law. Deleted data is maintained within an active account for a period of time. After the time period has expired, files go into a deletion queue. Data is deleted and the encryption key is destroyed.

Service termination

Customers have 30 days to download their Customer Content after the service is terminated. Customers must contact Citrix technical support for download access and instructions. Citrix will promptly delete the data following that period, except for back-ups that are deleted in the ordinary course, or as required by applicable law. During such time, Citrix will continue to apply the controls specified in the Citrix Services Security Exhibit and the DPA to protect this information.

Certifications

Citrix has products certified by industry-accepted security standards that can provide customers assurance concerning Citrix Cloud Services. For details about the services assessed, please see the Citrix Trust Center.

System and Organization Controls (SOC) 2 reports

Many Citrix services undergo regular SOC 2 assessments by a licensed CPA firm that issues a resulting SOC 2 report. The SOC 2 report is used to verify the design and operating effectiveness of the Citrix system of internal controls. The report provides detailed information and assurance about the protections at Citrix relevant to the security, availability, and confidentiality of customer data.

ISO/IEC 27001

Citrix has services certified with the internationally recognized ISO/IEC 27001 standard. This is part of the ISO 27000 series of standards that focuses on information security, risk management, and privacy management which, when combined, creates a globally recognized framework applicable to organizations of all sizes and sectors.

HIPAA

Citrix offers HIPAA-compliant configurations for certain products and services and Business Associate Agreements for those customers who need to store or process covered health information in the cloud. Citrix undergoes an annual independent assessment evaluating our services and controls under the HIPAA Security, Privacy, and Breach Notification rules

FIPS 140-2

Citrix has services certified with the United States Federal Information Processing Standard (FIPS) 140-2. This standard provides a benchmark for implementing cryptographic software.

IRAP

Citrix has services accredited at the “Protected” level with the Australian Information Security Registered Assessors Program (IRAP) standard.

Common Criteria

Citrix is committed to providing secure software to our customers, as evidenced by our progress in attaining the Common Criteria Certification, an ISO standard for software security function. Our defined Security Target, Configuration Guide and Certification Report are available for download on the Common Criteria page on the Citrix Trust Center.

Appendix A: Citrix Cloud Platform Data Collection

All services integrate with the Citrix Cloud Platform to provide a unified experience across Citrix Cloud. Citrix Cloud implements services that are common across all services, including optional service with the Citrix Identity Platform.

The table, Citrix Cloud Platform Data Collection, lists the Customer Content and Logs that are used to run the services.

Citrix Cloud Platform Data Collection

Platform	Customer Content	Logs
Citrix Cloud Platform	Administrator email, First Name, Last Name End User email, First Name, Last Name Company Name & Address	Citrix Gateway URL Resource Location Name AD Domains OrgId CC Customer Id CC Connector reference UserID Azure AD tenantID Per-customer encryption key Resource Location ID Notification Information SIEM data
Citrix Identity Platform	Administrator Login email, First Name, Last Name, address Password Partner Name	Sub (subscription) OrgId CC CustomerId Aad tenantID Athena CustomerId Clientids Device IDs Backup Codes FeatureIDs SIEM data

Appendix B: Citrix DaaS Data Collection

DaaS provides virtualization services designed to give the customer's IT organization control of its virtual machines, applications, and security while providing remote access for any device.

With the Citrix DaaS Cloud Service, application servers remain under the customer's control, in a resource location consisting of the customer's own datacenter or a customer-provided account with a third-party cloud vendor such as Microsoft Azure, Amazon Web Service, or Google Cloud Platform. While Citrix provides management and monitoring capabilities for these servers, it does not have access to the data within the servers, including the contents of user files, applications, and disk images (unless enabled by the customer, e.g., as part of customer support). The Citrix DaaS Cloud 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.

For a list of selected categories and data elements that may be processed by the Citrix DaaS Cloud Service, see the Selected DaaS API Properties table. This list is not exhaustive, but is designed to provide customers an understanding of the types of data being processed as part of the DaaS Service. For more information about the DaaS Service, please see the Citrix DaaS product documentation.

Selected DaaS API Properties

Category	Property	Description
End Users	Id	Unique identifier for the User. (Citrix Created)
	Sid	Security Identifier for the user. (synced with customer's AD)
	Upn	User Principal Name - has two parts: the UPN prefix (the user account name) and the UPN suffix (a DNS domain name). The parts are joined together by the at sign (@) symbol to make the complete UPN. (synced with customer's AD)
	UserName	Username in the form of DOMAIN\UserName (synced with customer's AD)
	FullName	Full name of the user (usually in the form "Firstname Lastname") (synced with customer's AD)
	Domain	Domain the user is associated with (synced with customer's AD)
	ClientName	The host name of the client connected to the session
	ClientAddress	The IP address of the client connected to the session
	ClientVersion	The version of the Citrix Receiver running on the client connected to the session
	ClientPlatform	The name of client platform, as indicated by client product ID for session
	ClientProductId	The product ID of the client connected to the session.
	DeviceId	Unique identifier for the client device that has most recently been associated with the session.
	HardwareId	Unique identifier for the client hardware that has been most recently associated with the session.
VDA Usage	SessionStart	
	SessionEnd	
	IdleDuration	Period for which session has been idle, or null if it is not considered idle.

	UntrustedUserName	The name of the logged-on user reported directly from the machine (in the form DOMAIN\user). This may be useful where the user is logged in to a non-domain account, however the name cannot be verified and must therefore be considered untrusted.
	EffectiveLoadIndex	Percentage of Total load
	Cpu	Percentage of CPU load
	Memory	Percentage of Memory load
	Disk	Percentage of Disk load
	Network	Percentage of Network load
	SessionCount	Percentage of Session Count load maps to
VDA Process-Level Data	ProcessName	
	AverageProcessorLoad	
	ProcessorLoadPeak	
	AverageMemoryUtilization	
	MemoryUtilizationPeak	
Applications	Name	Specifies the name of the application (must be unique within folder).
	CommandLineExecutable	Specifies the name of the executable file to launch. The full path need not be provided if it's already in the path. Environment variables can also be used.
	AdminFolder	The folder in which the new application should reside (if any).
	ClientFolder	Specifies the folder that the application belongs to as the user sees it. This is the application folder that is seen in the Citrix Online Plug-in, in Web Services, and also in the end-user's Start menu.
	CommandLineArguments	Specifies the command-line arguments to use when launching the executable. Environment variables can be used.

	Description	Specifies the description of the application. This is only seen by Citrix administrators and is not visible to users.
	PublishedName	The name seen by end users who have access to this application.
	StartMenuFolder	Specifies the name of the start menu folder that holds the application shortcut (if any).
	WorkingDirectory	Specifies which working directory the executable is launched from. Environment variables can be used.
Machines (VDAs)	Description	Description of the machine.
	DNSName	The DNS host name of the machine.
	HostedMachineName	The friendly name of a hosted machine as used by its hypervisor. This is not necessarily the DNS name of the machine.
	HostingServerName	DNS name of the hypervisor that is hosting the machine if managed.
	IPAddress	The IP address of the machine.
	MachineName	DNS host name of the machine.
	OSType	A string that can be used to identify the operating system that is running on the machine.
	OSVersion	A string that can be used to identify the version of the operating system running on the machine, if known.
	SID	The SID of the machine.
	Tags	A list of tags associated with the machine.
Hypervisors	HypervisorAddress	Specifies the address to be used. The address will be validated and the hypervisor must be contactable at the address supplied. XenServer (ConnectionType = XenServer) The address being added must reference the same XenServer pool referenced by any existing addresses for the same connection.
	SnapshotName	The name of the new snapshot. This is visible in the hypervisor management console.
Other Config Data	EncodedIconData	Specifies the Base64 encoded .ICO format icon data.

	PathToUserStore	Specifies the UNC path to the configured profile store.

Appendix C: Citrix Endpoint Management (CEM) Data Collection

Citrix Endpoint Management (CEM) is a solution for managing endpoints and offering mobile device management (MDM) and mobile application management (MAM) capabilities. The Citrix Endpoint Management database is located in the control plane and is 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. Customer Content collected for the service includes the following user data: Citrix Endpoint Management cookies, Connection details, Google enterprise owner email address, and Mobile number (if applicable).

For a list of data elements that may be processed by the CEM service, see the CEM Collected Active Directory (AD) Attributes table. This list is not exhaustive but is designed to provide customers with an understanding of the types of data being processed as part of the CEM service, some which are mandatory and others which customers can control. For more information about the CEM service, please see the Citrix Endpoint Management service product documentation.

CEM Collected Active Directory (AD) Attributes

Category	Attributes	Description
Mandatory	groupScope	Defines the Scope of your Active Directory Groups search. Could be Domain local group or 0, Global group or 1, Universal group or 2
	groupCategory	Specifies the category of the group. The acceptable values for this parameter are: Distribution or 0 Security or 1
	isAccountEnabled	True/False. Tells us if the user account is enabled or disabled
	isAccountLocked	True /False. Indicates if the account is locked due to password expiry, multiple wrong password attempts, etc
	isSecurityGroup	Defines if the AD group is a security group. Examples of Built-in security groups are Domain Controllers, Administrators, etc
	daysUntilPasswordExpiry	Int. Days remaining until the current password for the user expires
	passwordNeverExpires	True/False. Based on if password expiration time is set.
	distinguishedName	Example - CN=Jay Jamieson, OU= Newport, DC=cp, DC=com.
	badPwdCount	Number of bad password attempts made by the user
	memberOf	Groups which the user is member of
	primaryGroupID	Contains the Relative IDentifier (RID) for the primary group of the user. A user's primary group must be a group that exists in the user's primary AD Domain
	userAccountControl	Used to disable an account. A value of 514 disables the account, while 512 makes the account ready for logon.
	email	Email address of the user

	accountName	Username in the form of DOMAIN\UserName
	userPrincipalName	User Principal Name - has two parts: the UPN prefix (the user account name) and the UPN suffix (a DNS domain name). The parts are joined together by the at sign (@) symbol to make the complete UPN.
Customer Controlled	commonName	The name that represents an object
	firstName	First name of the user
	lastName	This would be referred to as last name or surname.
	displayName	Name of the user used for display purposes
	streetAddress	First line of address
	city	City of the user
	state	State, Province or County
	country	Country value of the user
	workPhone	Phone numbers for the user
	homePhone	Phone numbers for the user
	mobilePhone	Phone numbers for the user
	company	Company for which the user works
	department	Work Department of the user

Customer Controlled (cont.)	description	A description for the user account
	employeeID	Employee identifier of the user
	faxNumber	facsimileTelephoneNumber
	initials	Name initials if any for the user
	ipPhone	Ip Phone number
	manager	Manager account of the user
	homePostalAddress	This attribute specifies the user's home address.
	otherMobile	Phone numbers for the user
	pager	Pager number for the user
	physicalDeliveryOfficeName	Office name
	postalCode	Zip code
	postOfficeBox	P.O. box.
	title	Job title. For example, Manager.
	organization	Organization to which the user belongs
	preferredLanguage	The preferred written or spoken language for a person. Example: en-US

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

©2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).