Citrix Always On Tracing

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Introduction to Always On Tracing

August 18, 2026

What is AOT?

Always On Tracing (AOT) is a diagnostic framework built into Citrix Virtual Apps and Desktops. It continuously captures log data from infrastructure components —VDA, DDC, StoreFront™, NetScaler®, and others —and sends it to a centralized Log Server for indexed storage.

AOT is a curated subset of Citrix Diagnostic Facility (CDF) traces, extended with structured log data from other components. The key difference: it runs in the background automatically without requiring you to start a trace or reproduce the problem.

The Problem AOT Solves

Traditional Citrix troubleshooting requires:

1. **Reproduce the issue** —which may be intermittent or already resolved
2. **Start CDF tracing manually** —requires admin access and coordination
3. **Collect logs** —engineering-level tooling required to parse output
4. **Escalate to Citrix Support** —with incomplete or missing data

AOT eliminates every step in that chain. Logs are already captured. They're already stored. They're already searchable.

What AOT Gives You

- **Faster MTTR** —logs are available the moment an issue is reported, not after reproduction
- **No manual intervention** —tracing starts automatically when components are configured
- **Self-service troubleshooting** —IT admins can diagnose common issues without Citrix Support
- **Readable logs** —structured fields and keyword search, no parsing tools required
- **Full context for escalations** —when you do engage Support, you have everything

AOT vs. Traditional CDF Tracing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aspect	AOT	Traditional CDF Tracing
Activation	Automatic, continuous	Manual —must be started before the issue occurs
Issue reproduction	Not required	Required
Log readability	Structured, searchable fields	Raw ETW format, requires parsing tools
Diagnostic speed	Logs available immediately	Delayed by reproduction effort
Resource usage	Low overhead, optimized buffers	Moderate to high if misconfigured
Admin expertise needed	IT administrator	Engineering-level

What AOT Captures

AOT collects logs from the following Citrix components:

- Delivery Controller (DDC)
- Virtual Delivery Agent (VDA) —Windows, Linux, Mac
- StoreFront
- Citrix Director / Monitor
- Federated Authentication Service (FAS)
- Provisioning Services (PVS)
- Session Recording
- Workspace Environment Management™ (WEM)
- User Profile Management (UPM)
- NetScaler Gateway
- License Server
- Cloud Connector
- Citrix Workspace App (CWA) —Windows, Mac, HTML5, ChromeOS, Android, iOS

Each log entry is tagged with structured fields: `MachineName`, `MachineIP`, `Role`, `TimeStamp`, `Message`, `Level`, `Module`, `ProcessName`, `ProcessId`, `Thread`, `Cpu`, `SessionId`, `Class`.

Who This Is For

- **IT administrators** managing Citrix environments who need to diagnose session failures, VDA registration errors, and infrastructure issues
- **Citrix Support engineers** who need full context from customer environments to resolve escalations quickly

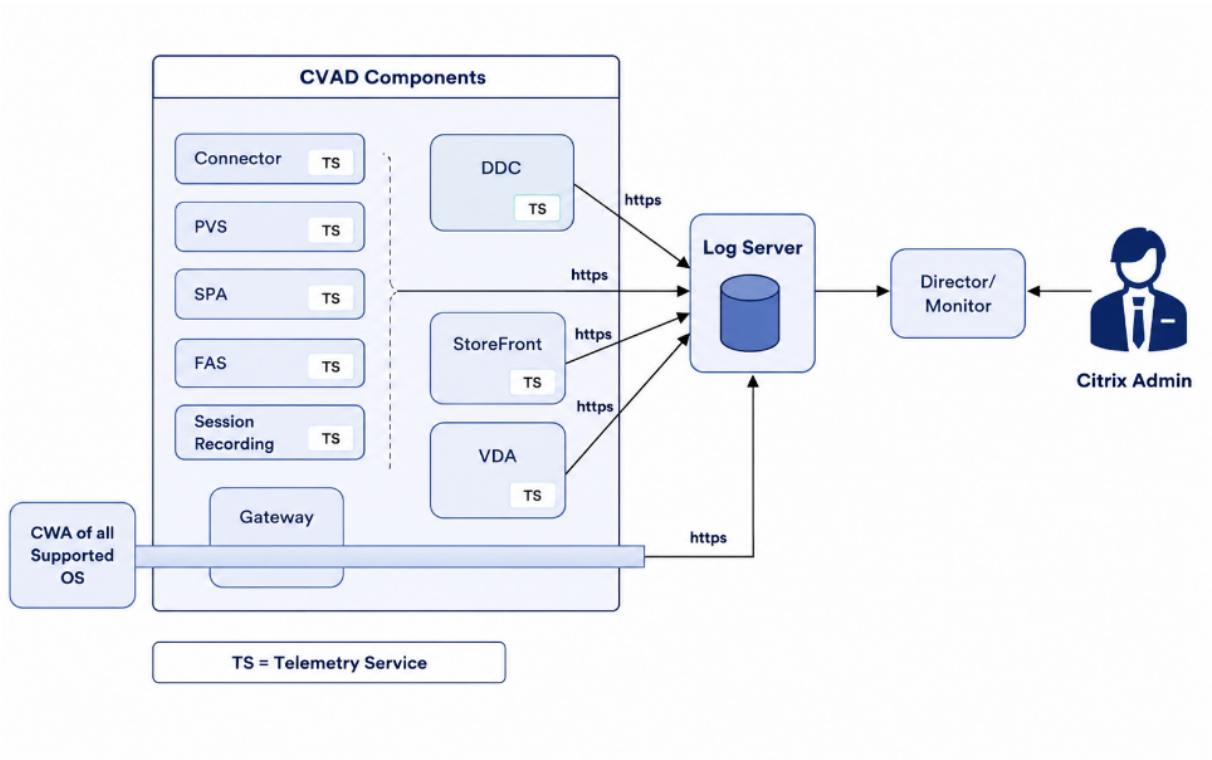
© 1997–2026 Citrix Systems, Inc. All rights reserved.

How AOT Works

August 18, 2026

The Big Picture

Always On Tracing is supported across both Citrix Virtual Apps and Desktops™ (CVAD) on-premises deployments and Citrix DaaS™ cloud-hosted deployments, providing consistent diagnostic capabilities regardless of where your infrastructure runs.



Every Citrix component equipped with the **Telemetry Service** becomes an AOT log collector. Once you configure the Log Server address in Web Studio (or DaaS Settings), the Telemetry Service on each component activates, begins collecting logs, and forwards them to the Log Server automatically.

Step-by-Step Data Flow

1. Administrator Configures AOT

The administrator enters the Log Server address, port, and authentication key in **Citrix Web Studio** (on-prem) or **DaaS Settings** (cloud).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The configuration is written to the Site database.
- Delivery Controllers read the updated settings and distribute them to VDAs in the selected delivery groups.
- StoreFront™, Director, and other supported components receive the same settings via the same mechanism.

2. Telemetry Service Activates

Once each component receives the Log Server configuration, its local **Telemetry Service** activates the real-time AOT listener. This listener tracks predefined events, step traces, and error conditions — capturing log data as events occur with no trigger required.

3. Logs Transfer to Log Server

The Telemetry Service transfers logs directly to the Log Server over HTTPS. In environments where clients connect through **Citrix Gateway**, log transfer occurs over a **SOCKS tunnel**.

4. Log Server Stores and Indexes

The Log Server receives each log entry, parses it, and indexes it into **OpenSearch**. Logs are compressed using **LZ4** (~2:1 ratio), retained for the configured period (default: 7 days), and automatically purged when disk usage exceeds 85%.

Key Components

AOT Log Generators

Supported generators: DDC, VDA (Windows/Linux/Mac), StoreFront, Director, FAS, PVS, Session Recording, WEM, UPM, NetScaler®, License Server, Cloud Connector, Citrix Workspace App. The Telemetry Service ships with all supported CVAD components running on Windows OS, and an independent service (where Telemetry Service isn't supported) to forward the logs to Log Server — no additional installation is needed.

Centralized Log Server

The Log Server is a Docker-containerized service that includes an ingestion endpoint, an OpenSearch backend, CLI scripts for log download, and a REST API for Director/Monitor queries. It runs on Linux VM, Windows VM, or Citrix Connector Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Retention and Purge

Setting	Default	Range
`MAX_RESERVE_DAYS`	7 days	1–30 days
`MAX_DISK_USAGE_PERCENTAGE`	85%	10–90%

Log Structure

Field	Description
`MachineName`	Hostname where the log originated
`MachineIP`	IP address of the source machine
`Role`	Citrix component role (VDA, DDC, StoreFront, etc.)
`TimeStamp`	UTC timestamp of the log event
`Message`	Log content —searchable by keyword
`Level`	Severity: Info, Warning, Error
`Module`	Software module that generated the log
`ProcessName`	Process that generated the log
`ProcessId`	Process ID
`Thread`	Thread ID
`Cpu`	CPU ID at the time of the log
`SessionId`	User session ID associated with the log
`Class`	Class or component within the module

Log Server Capacity Limits

Metric	Limit
Active component connections	128,000
Log ingestion rate	10,000 events/second

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Metric	Limit
Burst tolerance	~2× normal rate without loss
Log Servers per environment	**1** (current limitation)

> **Note:**
>
> The bottleneck is log throughput (events per second), not the number of connected machines. A large environment with 100,000 machines generating modest log volume can run on a single Log Server, as long as the 10,000 EPS threshold is not exceeded during peak activity.
>
> **Warning:**
>
> Currently, only **one Log Server per environment** is supported. Support for multiple Log Servers and horizontal scaling is planned for a future release.

Plan Your Deployment

August 27, 2026

Complete this page before touching the Log Server installer. The decisions you make here —platform, sizing, storage —affect everything downstream.

Step 1 —Choose a Deployment Platform

Platform	Recommended For	Key Constraint
Citrix Connector Appliance	Most environments	Port 443 only; no Docker management needed
Linux VM	Production deployments	Best reliability; runs without user session
Windows VM	When Linux is not available	Requires active user session; Docker Desktop license needed

> **Tip:** Use the Connector Appliance if you have one in your environment. Log Server updates are delivered automatically with Connector Appliance upgrades —no manual Docker pull required.
>
> **Tip:** If you are on-premises and do not already use a Connector Appliance, you can still deploy one solely as a dedicated Log Server —no Windows or Linux OS license required. The Connector

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Appliance can run alongside your existing Cloud Connector and serve the AOT Log Server function for your on-premises environment.
> **Warning:** Do not deploy on a Windows VM hosted on XenServer®. XenServer does not support nested virtualization, which prevents Docker from running.

Step 2 —Check Minimum Version Requirements

Citrix Workspace App

Platform	Minimum Version (Direct Access)	Minimum Version (via Gateway)
Windows	2511.10 and 2507 CU1 or later	2603 and 2507 CU2 or later
Mac	2603 or later	2603 or later
Linux	Coming soon	Coming soon
HTML5	2511 or later	2603 or later
ChromeOS	2511 or later	2603 or later
Android	2603 or later	2603 or later
iOS	2603 or later	2603 or later

Direct Access: The Citrix Workspace App connects directly to StoreFront™ without traversing a Citrix Gateway. This is typically used within a corporate network where the Citrix environment is reachable without a VPN or proxy.

Via Gateway: The Citrix Workspace App connects through a Citrix Gateway (NetScaler®). Typically used for external or remote access where traffic is routed through a secure gateway before reaching the Citrix environment.

Platform and Infrastructure Components

Component	Minimum Version
CVAD (VDA, DDC, PVS, FAS, Session Recording, StoreFront, WEM, UPM)	2402 CU4, 2507 CU1, 2511 or later
Citrix DaaS™	Post February 2026
Citrix NetScaler	14.1.60.57

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Component	Minimum Version
Citrix License Server	540000 or later
Citrix Connector Appliance	11.4.1.444 or later
Cloud Connector (for Monitor log retrieval)	6.141.0.13739 or later
Cloud Connector (for log forwarding)	6.169.0.22492 or later

Step 3 —Size Your Log Server

Hardware Requirements

Resource	Linux VM	Windows VM	Connector Appliance
CPU	4 cores min	8 cores min	4 vCPUs (increase from default 2)
RAM	16 GB	24 GB	16 GB (increase from default 4 GB)
Disk	500 GB SSD*	500 GB SSD*	Attach a separate virtual disk*
Docker	Docker Engine (free)	Docker Desktop (subscription may apply)	Built-in —no Docker management

* See Step 4 —Storage Calculator for the accurate storage required for your setup.

OpenSearch Memory Scaling

Connected Machines	Recommended Heap
0–999	2 GB (`-Xms2G -Xmx2G`)
1,000–1,999	4 GB (`-Xms4G -Xmx4G`)
2,000–9,999	6 GB (`-Xms6G -Xmx6G`)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 4 —Calculate Storage

Formula

```
Total Storage (GB) = Daily Log Volume (GB) × Retention Days
```

Daily Log Volume by Component Type

The table below shows a reference breakdown for a medium deployment of approximately 10,000 managed components. Use these per-component figures to estimate daily log volume for your environment.

Component	Count	Sessions / Day / Machine	Avg Log Size / Session	Total Logs / Day
Persistent VDAs	1,000	2	2 MB	4,000 MB (~4 GB)
Pooled VDAs	1,000	50	2 MB	100,000 MB (~100 GB)
CWA Endpoints	8,000	4	1–1.5 MB	48,000 MB (~48 GB)
Delivery Controllers	4	—	300 MB / DDC / day	1,200 MB (~1.2 GB)
StoreFront Servers	4	—	300 MB / server / day	1,200 MB (~1.2 GB)
NetScaler / PVS / Session Recording / FAS / Other	4	—	300 MB / server / day	1,200 MB (~1.2 GB)
Daily Total				**~156 GB/day pre-compression / ~80–125 GB/day post-compression**

> **Note**
>
> - These values are approximate and can differ widely between deployments depending on architecture, user activity, enabled components, and session patterns.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - Infrastructure components (DDC, StoreFront, Gateway, PVS, FAS, Session Recording) are estimated at 300 MB per server per day. This is a conservative planning figure.
> - The Log Server uses the LZ4 compression algorithm by default. The compression reduction is typically between 20% and 50%.
> - Deploy the AOT Log Server on SSD-backed storage for best performance.

Daily Log Volume by Deployment Size

Deployment Size	Before Compression	After LZ4 Compression
5,000 machines	~78 GB/day	~40–63 GB/day
10,000 machines	~156 GB/day	~80–125 GB/day
50,000 machines	~780 GB/day	~400–625 GB/day
100,000 machines	~1.56 TB/day	~800 GB–1.25 TB/day

Retention-Based Storage Estimate

Deployment Size	7-Day Retention	10-Day Retention
5,000 machines	~300–450 GB	~400–630 GB
10,000 machines	~600 GB–1 TB	~800 GB–1.25 TB
50,000 machines	~3–5 TB	~4–6.3 TB
100,000 machines	~6–10 TB	~8–12.5 TB

Step 5 —Plan Your Network

- The Log Server must be **reachable from all components** that will forward logs.
- Deploy the Log Server **in the same network segment as your VDAs** to minimize latency.
- Choose a port that is not in use, not in the privileged range (0–1023), and allowed through your firewall.
- **HTTPS is strongly recommended.** Example ports: 8443 (HTTPS), 8080 (HTTP).
- If using the **Connector Appliance**, configure **port 443 only**.

Checklist Before You Proceed

- Platform selected (Connector Appliance / Linux / Windows)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Hardware provisioned (CPU, RAM, SSD disk)
- CVAD component versions verified
- Daily log volume estimated
- Retention period decided
- Total storage allocated
- Port selected and firewall rules updated
- Certificate ready (for HTTPS mode)
- OpenSearch heap memory planned

Deployment Scenarios

August 13, 2026

AOT support varies by deployment model. Use this matrix to determine which components forward logs in your environment.

Component Support Matrix

#	Deployment Scenario	CWA	StoreFront	Citrix Workspace™	Gateway On-Prem	CGS	DDC On-Prem	Cloud DDC	Cloud Connector	VDA	FAS	PVS	Other
1	**On-Prem Direct** (StoreFront + on-prem DDC)	Yes	Yes	N/A	N/A	N/A	Yes	N/A	N/A	Yes	Yes	Yes	Yes
2	**On-Prem via Gateway**	Yes	Yes	N/A	Yes	N/A	Yes	N/A	N/A	Yes	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#	Deployment Scenario	CWA	StoreFront	Citrix Workspace™	Gateway On-Prem	CGS	DDC On-Prem	Cloud DDC	Cloud Connector	VDA	FAS	PVS	Other
3	**Fully Cloud** (Workspace + Cloud DDC + CGS)	Coming Soon	N/A	Yes*	N/A	Yes*	N/A	Yes*	Yes	Yes	Yes	Yes	Yes
4	**Hybrid Cloud** (Workspace + Cloud DDC + Gateway)	Coming Soon	N/A	Yes*	Yes	N/A	N/A	Yes*	Yes	Yes	Yes	Yes	Yes
5	**Hybrid Cloud** (StoreFront + Cloud DDC + Gateway)	Coming Soon	Yes (Manual)	N/A	Yes	N/A	N/A	Yes*	Yes	Yes	Yes	Yes	Yes

> **Note:**
>
> - **Yes** = uploads logs to customer-managed AOT Log Server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - **Yes*** = logs handled via Citrix-managed service, not customer-managed Log Server
> - **Manual** = requires manual configuration
>
> **Coming Soon** = not yet available **N/A** = not applicable
>
> -

Install the Log Server

August 12, 2026

The Log Server installer and setup steps differ by platform. Select the platform that matches your environment.

Platform	Guide	Best For
Citrix Connector Appliance	Install on Connector Appliance	Most environments — automatic updates, no Docker management
Linux VM	Install on Linux	Production —most reliable, no user session dependency
Windows VM	Install on Windows	When Linux is unavailable

Port and Certificate Guidelines

- Use **HTTPS** for enhanced security. HTTP is supported but not recommended in production.
- The Connector Appliance supports **port 443 only**.
- For Linux and Windows, choose any port outside the privileged range (0–1023).
- Reference ports: **8443** (HTTPS), **8080** (HTTP).
- Ensure your TLS certificate file is in `.pfx` format and trusted by all components uploading logs.

Scripts Created After Installation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Script (Linux .sh / Windows .bat)	Purpose
`StartLogServer`	Start the Log Server container
`GetAuthKey`	Generate an authentication key
`ListMachines`	List machines that have sent logs
`DownloadLogsByTime`	Download logs by time range
`DownloadLogsByWords`	Download logs by keyword search

Verify the Installation

After installing and starting the Log Server, call the ping endpoint from a browser or curl:

```
https://YourLogServerFQDN:8443/Ping
```

Expected response:

```
Pong UTC:08/19/2025 01:03:29 Version: 2511.1.6
```

If the ping fails, check `configpath/weblogs.txt` and review the Troubleshooting section.

Install on Citrix Connector Appliance

August 27, 2026

- **No Docker management** —the Log Server container is built into the appliance
- **Automatic updates** —Log Server version tracks Connector Appliance upgrades
- **Recommended for most environments**

> **Warning:**
>
> Mutual TLS (mTLS) is not supported on the Connector Appliance. If your security requirements mandate mTLS, use the Linux or Windows installation instead.
>
> **Note:**
>
> Cloud Monitor retrieves AOT logs through the Monitor Connector service on a supported Windows Cloud Connector in the same Resource Location. A Windows Cloud Connector running version **6.141.0.13739** or later must also be present.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

- Connector Appliance version **11.4.1.444** or later
- Appliance registered with Citrix Cloud™
- At least **4 vCPUs** and **16 GB RAM** (default is 2 vCPUs / 4 GB —you must increase this)
- A valid TLS certificate signed by your organization (the appliance self-signed cert must be replaced). Certificate and private key should be in .PEM format.
- An additional virtual disk sized for your log storage needs
- A DNS A record pointing the Connector Appliance's FQDN to its IP address
- Joining the Connector Appliance to the domain is not mandatory —it can operate without domain membership
- Cloud Monitor retrieves AOT logs through the Monitor Connector service running on a supported Windows Cloud Connector in the Resource Location
- If the Log Server is deployed on the Citrix Connector Appliance, a supported Windows Cloud Connector must also be present in the same Resource Location —the Connector Appliance alone is not sufficient for Cloud Monitor to retrieve AOT traces
- The Cloud Connector must be running version **6.141.0.13739** (or **4.420.0.13739**) or later — earlier versions will cause the GetAotTraces API call to fail, resulting in an HTTP 500 error in Monitor
- The Connector Appliance provides a self-signed certificate to browsers connecting to its administration page —to connect to the Log Server via HTTPS, you must replace this with a certificate signed by your organization or generated by using your organization's chain of trust. For more details refer to Replace Server Certificate

Step 1 —Deploy or Upgrade the Connector Appliance

If you do not have a Connector Appliance, download the appliance image from Citrix Cloud, import it into your hypervisor, and register it with Citrix Cloud. If you already have one, upgrade it to version **11.4.1.444** or later. The Log Server is onboarded automatically during the upgrade.

Step 2 —Increase Appliance Resources

1. Shut down the appliance VM.
2. In your hypervisor/hyperscaler, increase resources to at least **4 vCPUs** and **16 GB RAM**.
3. Power the appliance back on.
4. Install all pending updates before proceeding to the next section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3 —Replace the TLS Certificate

The Connector Appliance ships with a self-signed certificate. Replace it with a certificate signed by your organization's CA using the Citrix documentation for Replace Server Certificate on the Connector Appliance.

Step 4 —Access the Log Server UI

1. Open a browser and navigate to:

```
https://<connector-appliance-FQDN>/?enable=logserver
```

The `?enable=logserver` query parameter is required to show the Log Server tab.

1. Sign in to the Connector Appliance admin UI.
2. Select the **Log Server** tab. You will see two sections: **Log server** and **Authentication keys**.

Step 5 —Add Storage

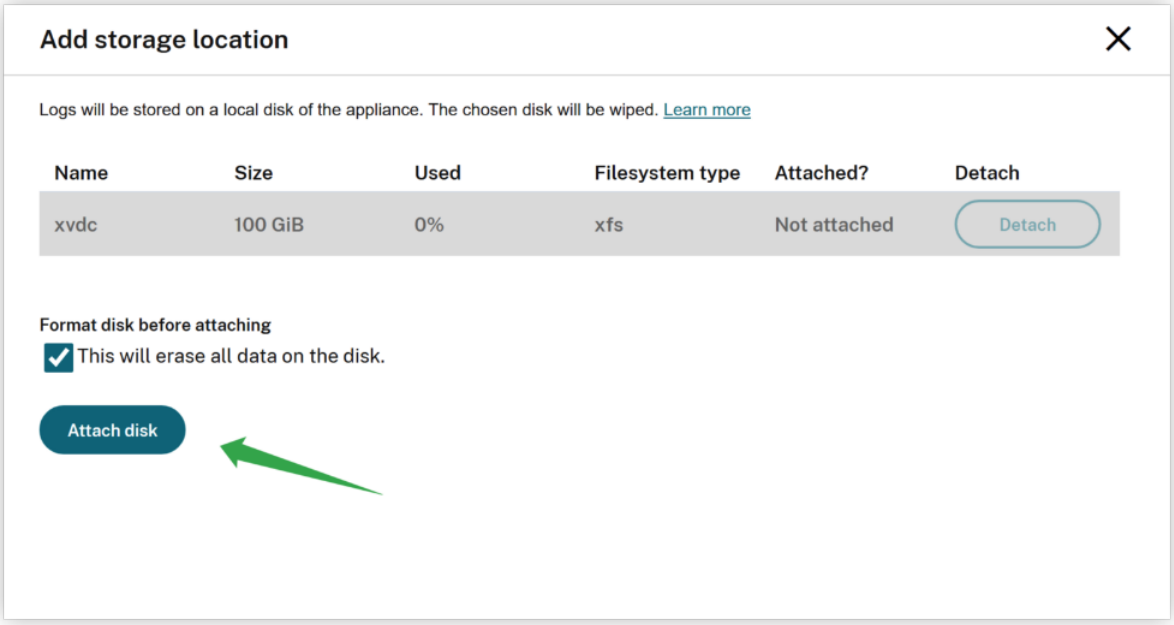
The appliance boot disk is only 20 GB —not sufficient for log storage. You must attach an additional virtual disk dedicated for log storage.

1. In your hypervisor/hyperscaler, add a new virtual disk to the Connector Appliance VM.

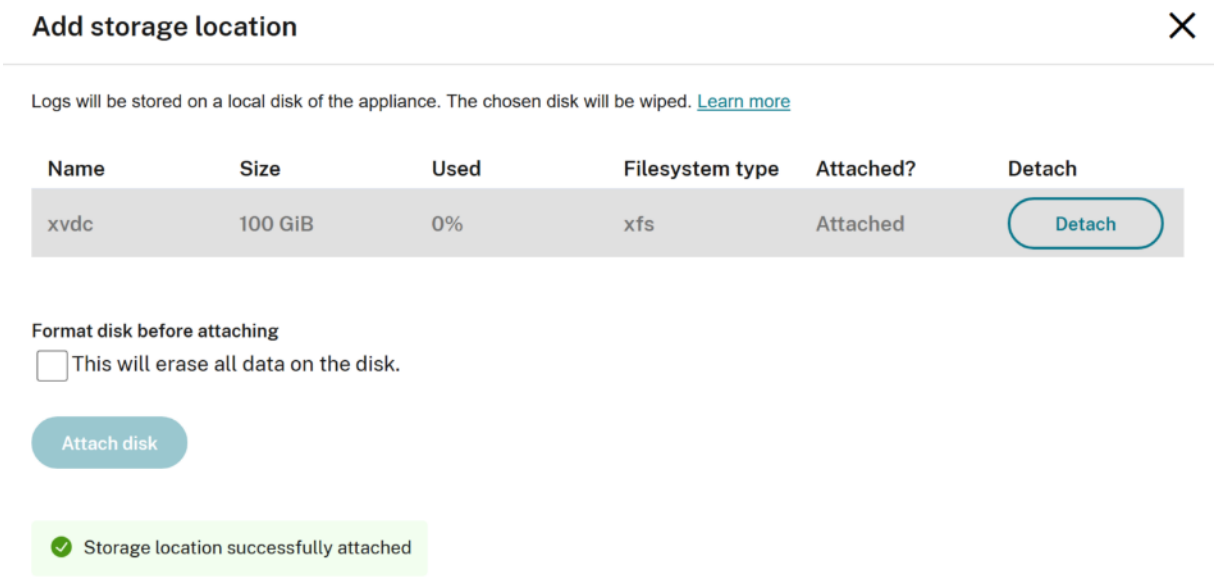
> **Warning:**
>
> VMware ESXi requirement: Attach the additional data disk to a **different SCSI controller** than the one used by the root disk.

1. Return to the Log Server tab in the Connector Appliance UI.
2. Click **+ Add storage location**. The new disk appears in the list.

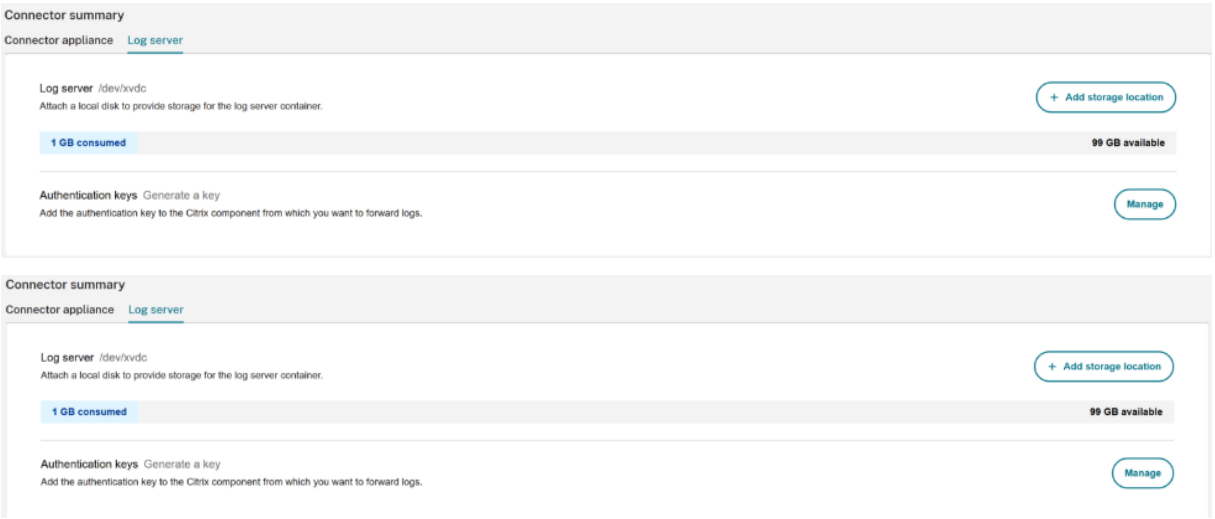
© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Check **Format disk before attaching** (ensures it is a new, empty disk).
2. Click **Attach disk**.
3. Wait for the confirmation: **Storage location successfully attached**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



The Log Server main page displays disk size, space used, and space remaining after storage is attached.

Step 6 —Verify the Log Server is Running

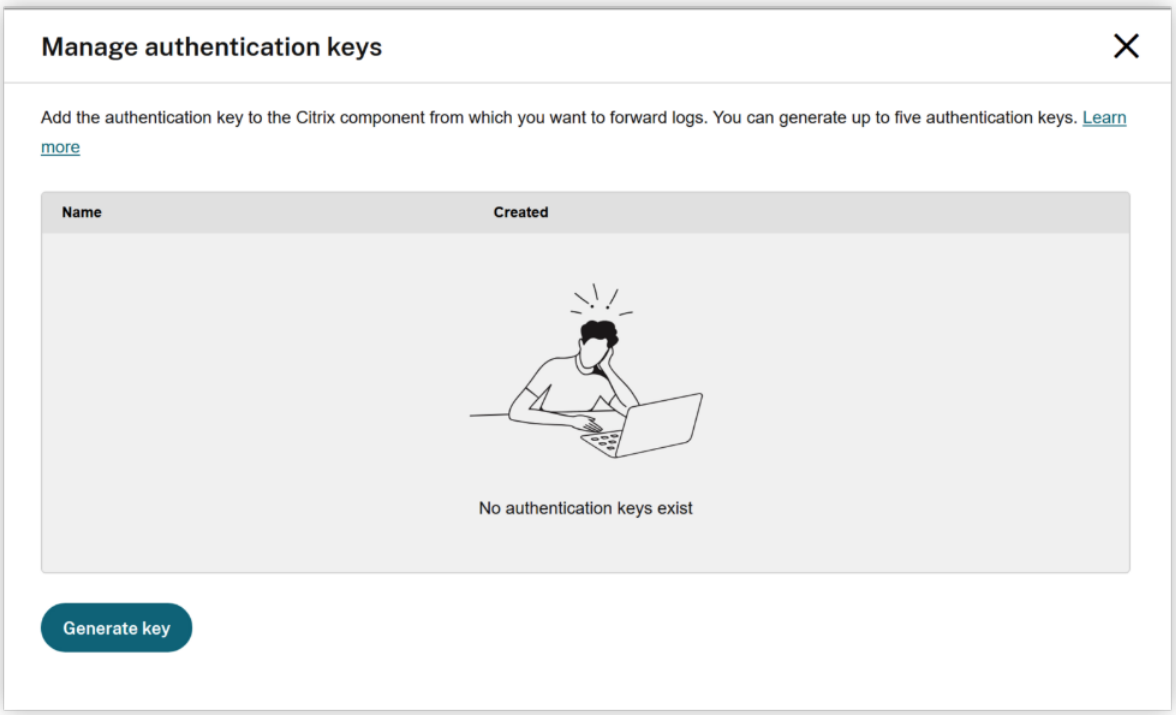
```
https://<connector-appliance-FQDN>/ctxlogserver/Ping
```

A **Pong** response confirms the Log Server started successfully.

Step 7 —Generate an Authentication Key

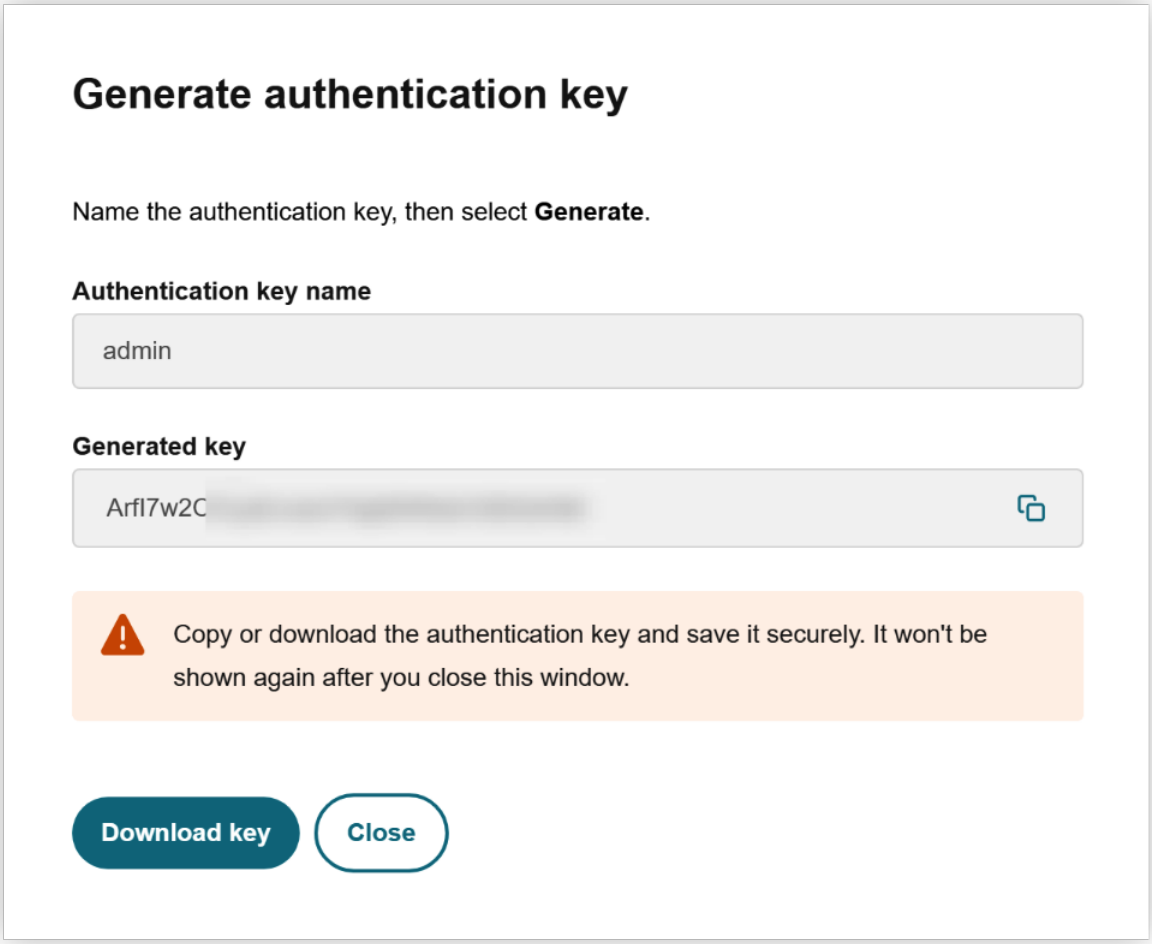
1. On the Log Server tab, click **Manage** in the Authentication keys section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Click **Generate key**.
2. Enter a name for the key (for example: `admin`).
3. Copy or download the generated key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Warning:**
>
> The key is shown **only once**. Copy or download it before closing the window. If you lose it, you must generate a new one.

Store the key securely —you will need it when configuring Web Studio in Configure Components.

Managing Advanced Settings via API

The Connector Appliance does not expose Log Server advanced settings through the UI. Use the local API instead. Settings can be configured via Postman, Curl, or PowerShell.

1. Authentication: Generating a JWT

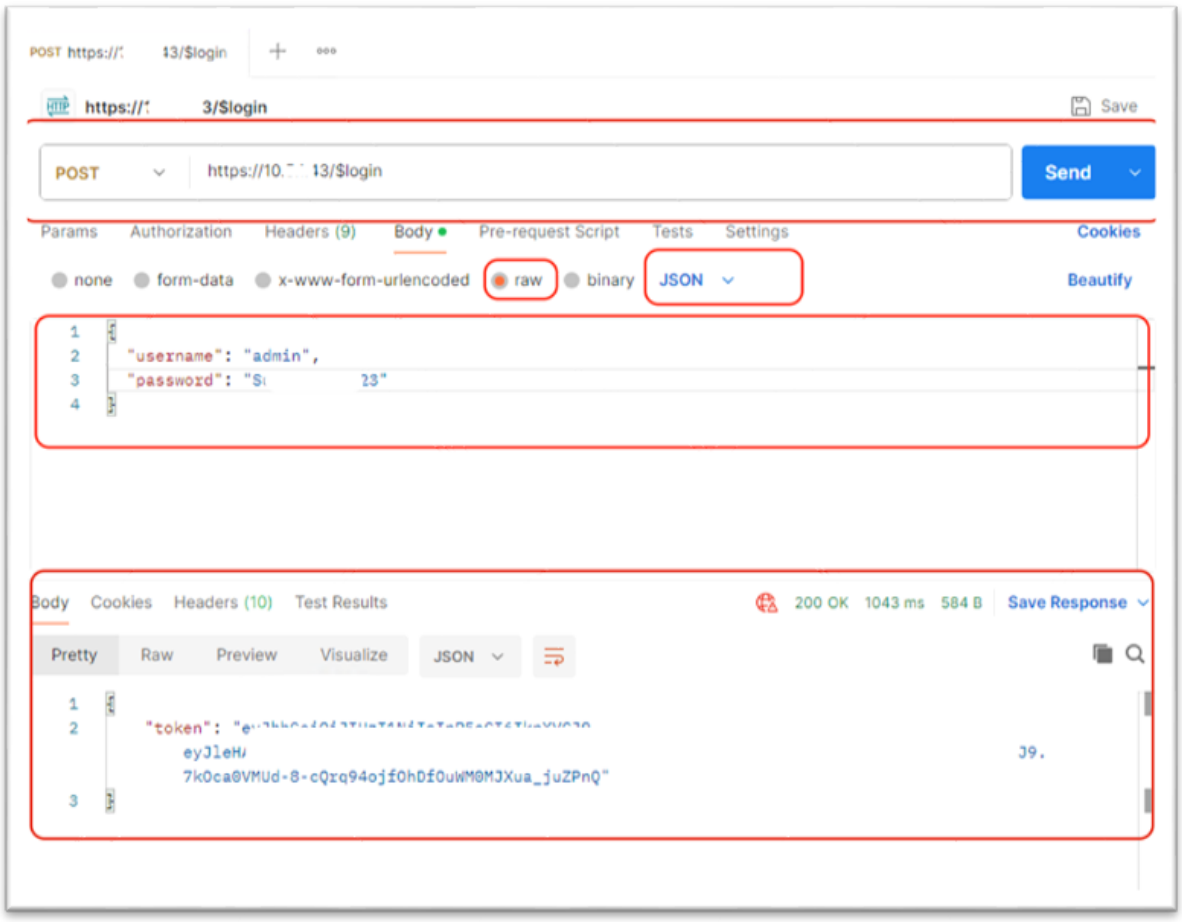
All API calls must be authenticated using a JSON Web Token (JWT). You must first generate a token which is then included in the header of subsequent requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

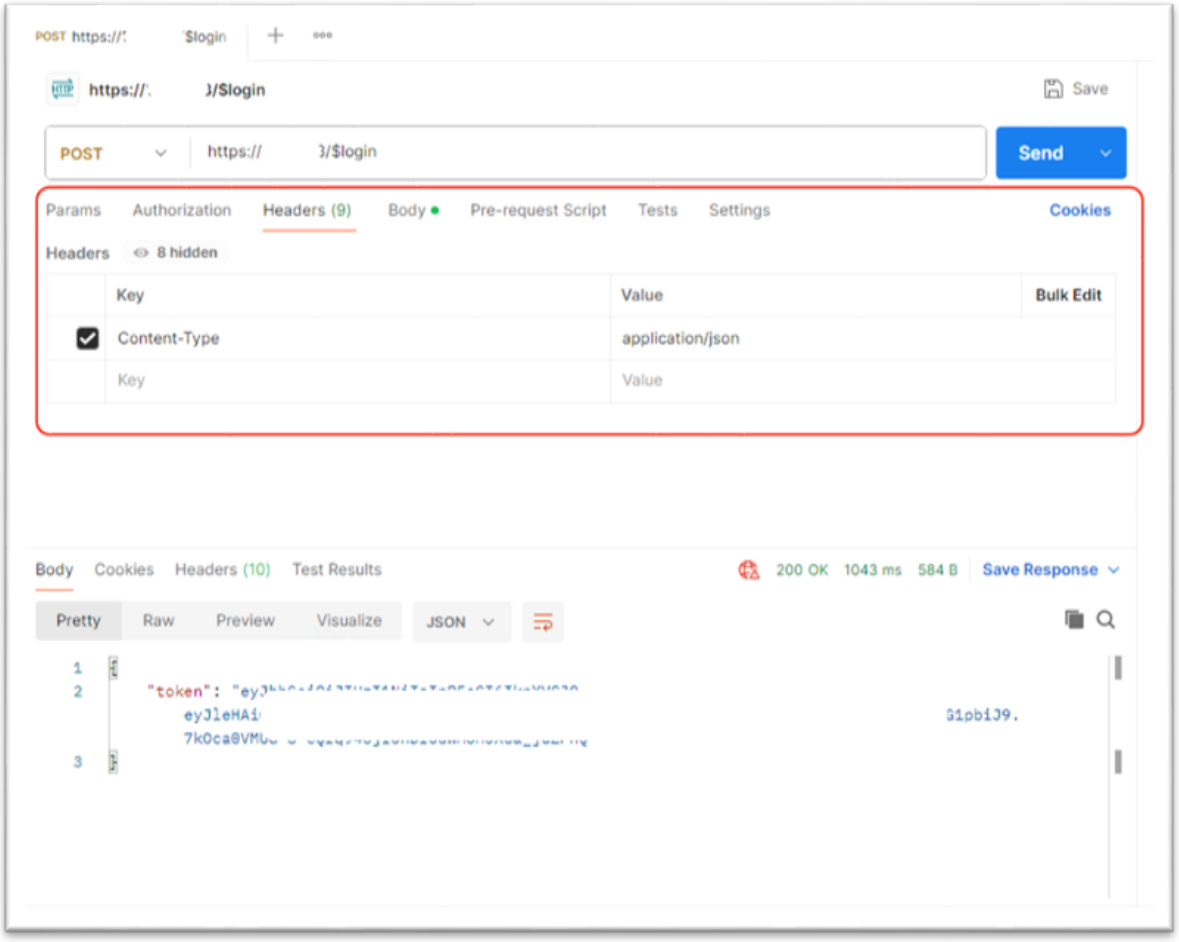
Step 1.1 —Generate a Token

To generate a token, submit a POST request to the login endpoint:

- Endpoint: `POST https://<appliance-IP>/$login`
- Body: You'll need to include the necessary JSON payload for authentication (e.g., username and password).
- On success, the API returns a token value



© 1997–2026 Citrix Systems, Inc. All rights reserved.



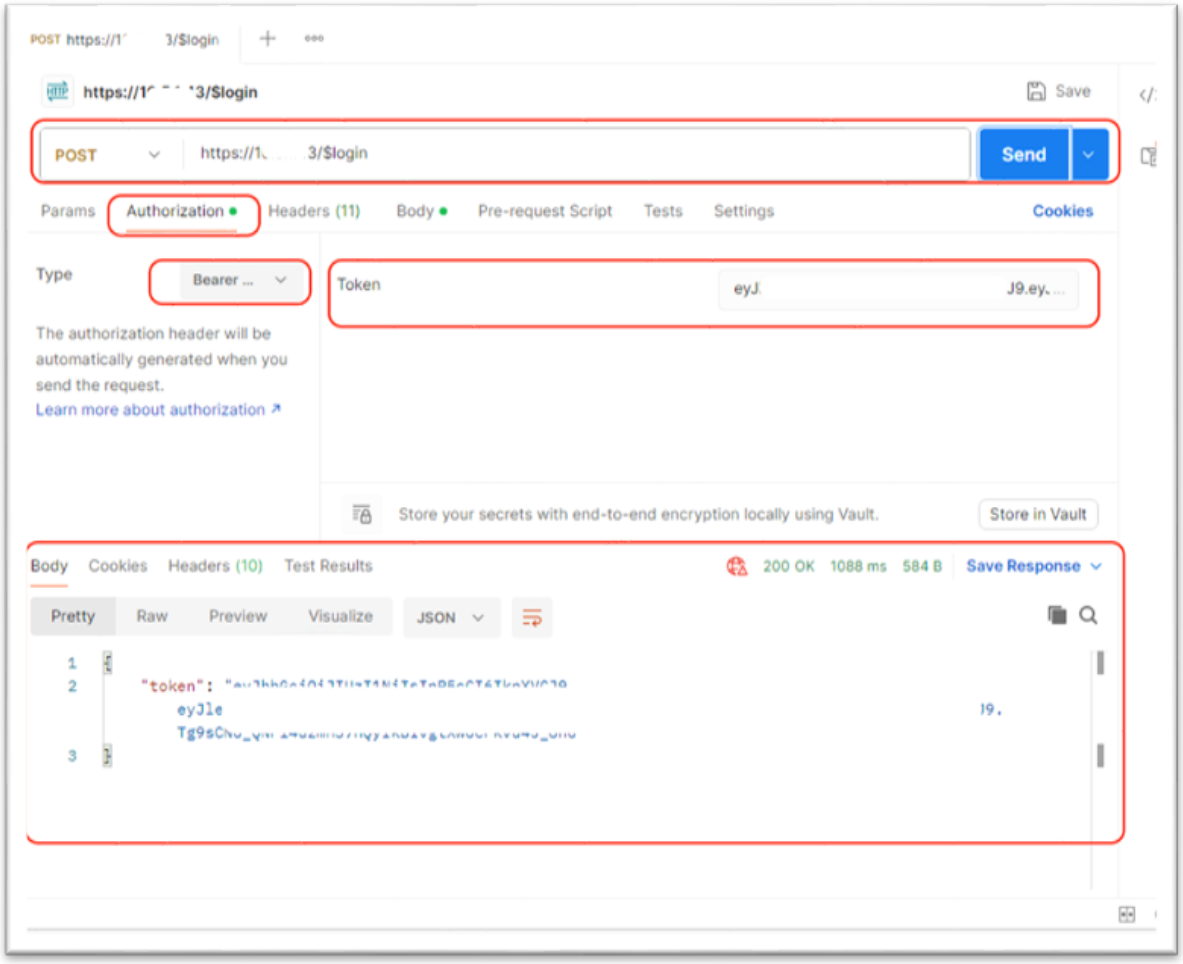
Step 1.2 —Authorize API Calls

The token must be included in the Authorization header, prefixed with "Bearer":

```
Authorization: Bearer abCD.efGH.ijKL
```

A valid token will allow the API call to proceed. An invalid or expired token will be rejected with an error message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Set Maximum Retention Days

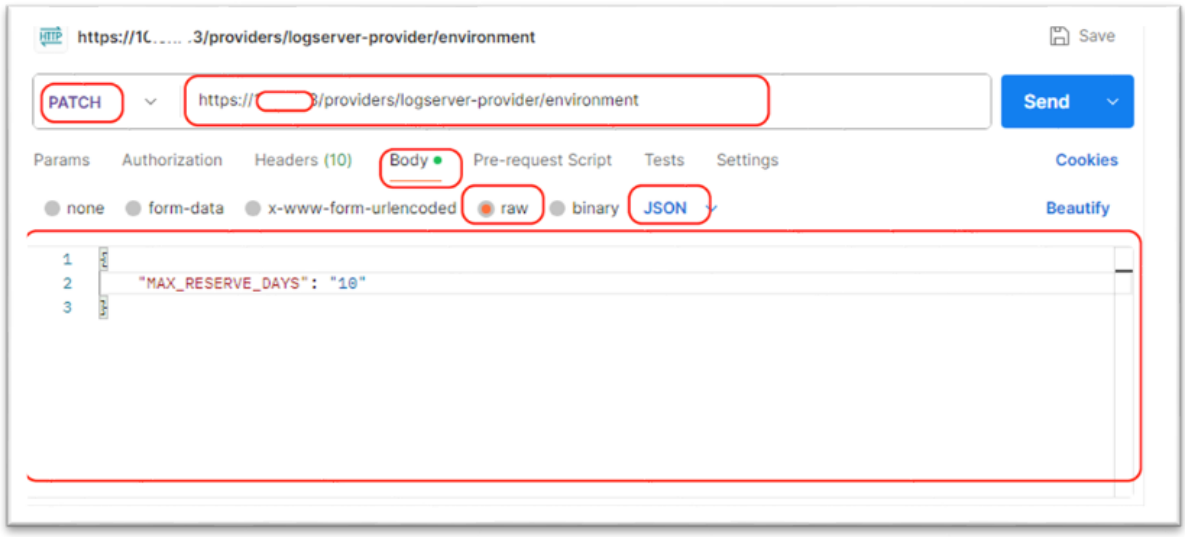
This action configures the MAX_RESERVE_DAYS for the logserver.

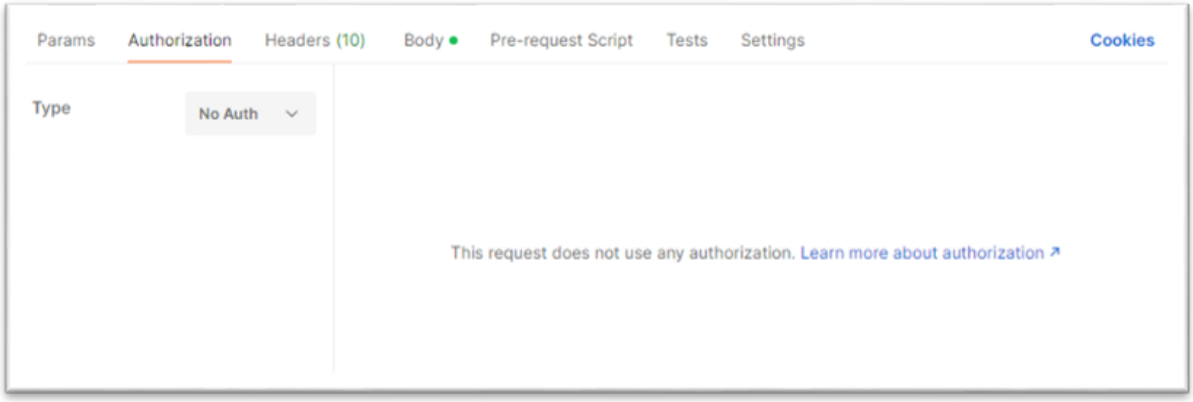
- Endpoint: `https://<appliance-IP>/providers/logserver-provider/environment`
- Method: `PATCH`
- Request Body: `{ "MAX_RESERVE_DAYS": "7"}`

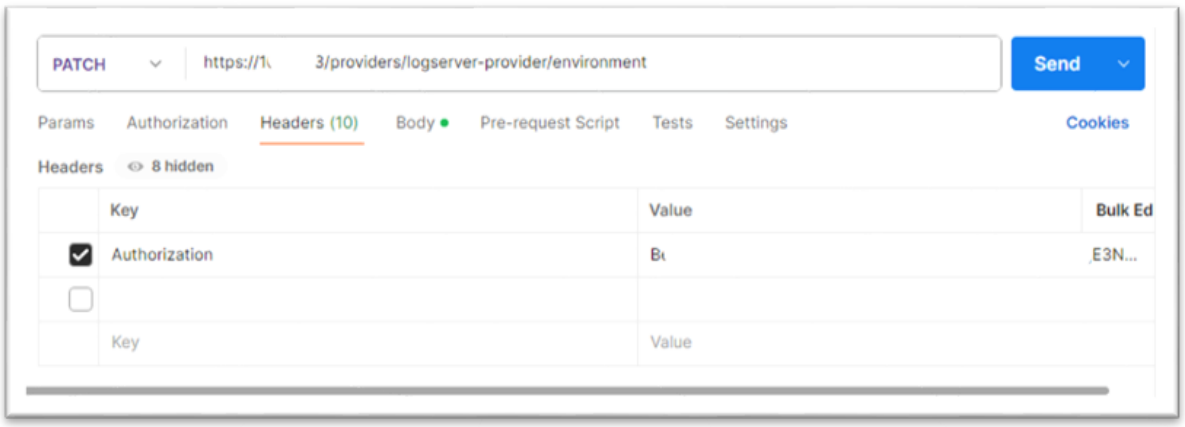
Fields

- `MAX_RESERVE_DAYS` (string, required): Default value is 7 days. Log Server stores log entries max days based on the TimeStamp field. Logs that were inserted 7 days ago will be deleted. Check every 10 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

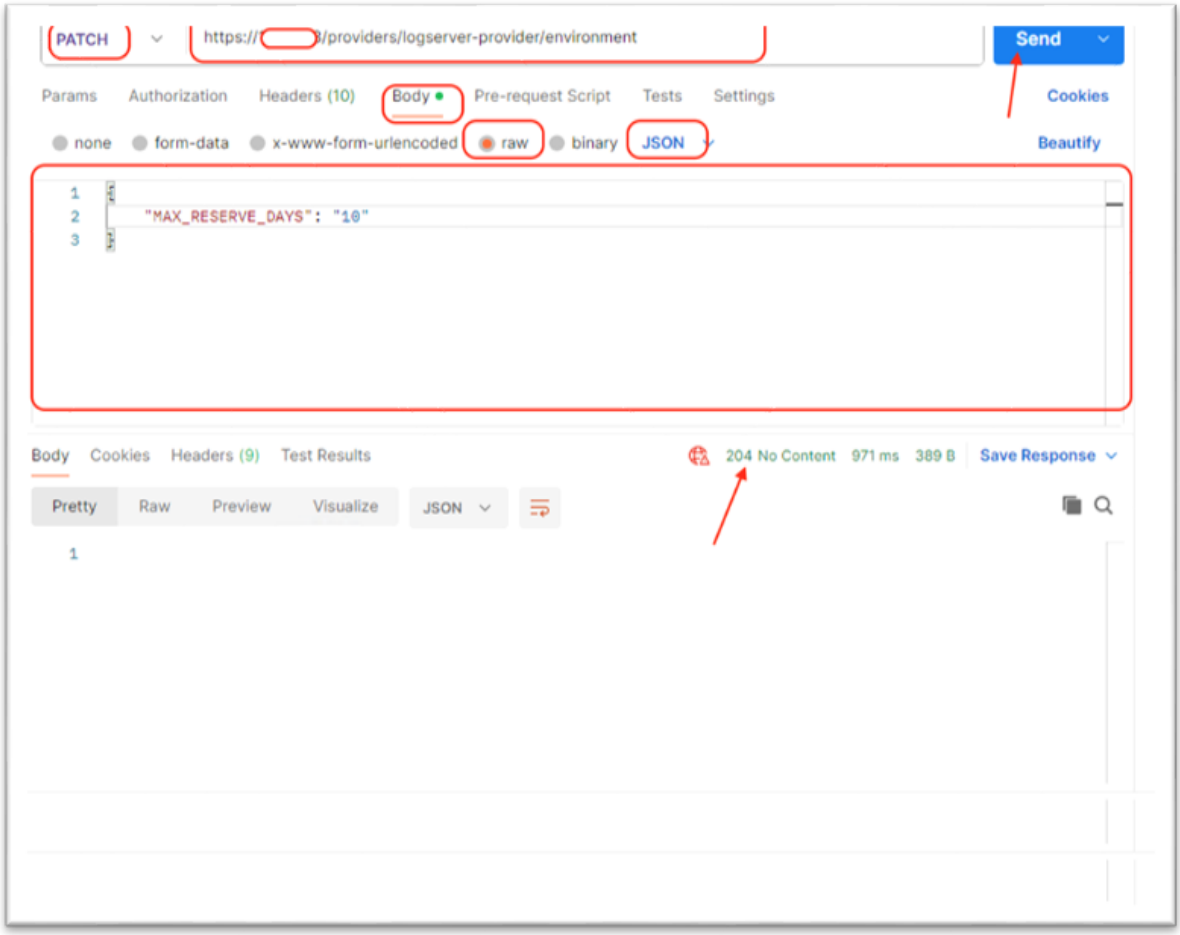






Response A `204 No Content` response confirms the setting was applied.

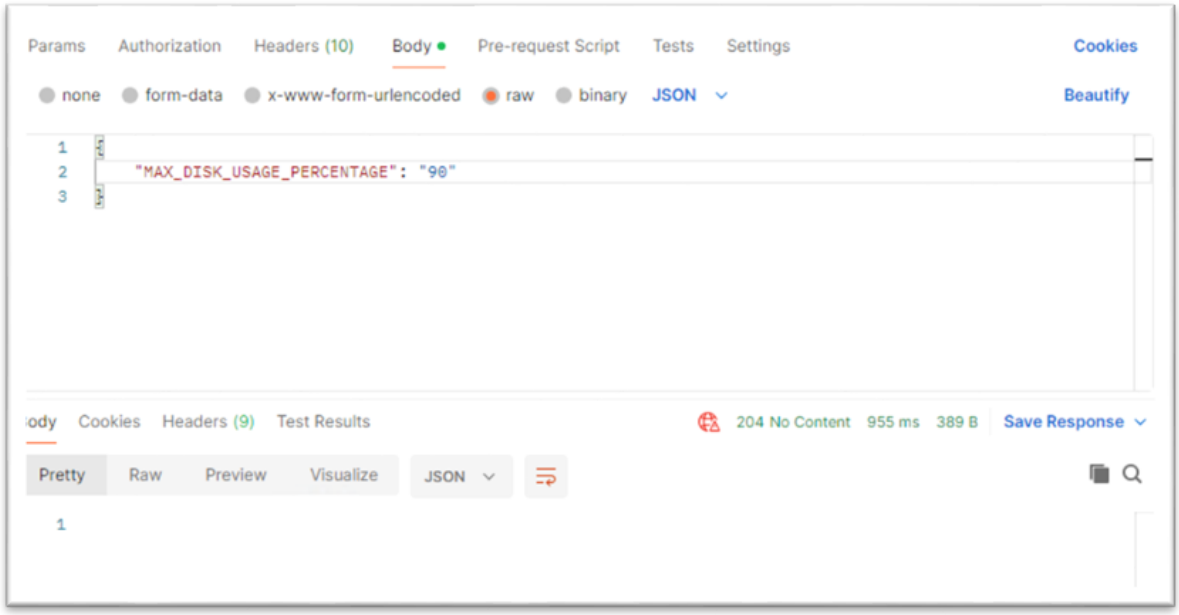
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Set Maximum Disk Usage Percentage

Using the same endpoint and method, adjust `MAX_DISK_USAGE_PERCENTAGE` from its default of 85. When disk usage hits the threshold, older logs are purged to make room for new ones.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A `204 No Content` response confirms the setting was applied.

Upgrade and Maintenance

Log Server updates on the Connector Appliance are **fully automatic** —delivered as part of Connector Appliance upgrades. No manual steps are required.

Install the Log Server on Linux

August 18, 2026

Prerequisites

- Supported OS: Ubuntu 24.04 or RHEL 8.10 / 9.4
- CPU: 4 cores minimum
- RAM: 16 GB minimum
- SSD-backed storage strongly recommended
- Docker Engine for Linux installed
- User can run Docker commands **without sudo**
- Chosen port is open in firewall rules and not in use
- TLS certificate in `.pfx` format (for HTTPS mode)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1 —Download the Installer

Download the Log Server Docker container image and installer from Citrix Downloads. Place all downloaded files in the **same directory**.

Step 2 —Make the Installer Executable

```
chmod +x ./InstallLogServer
```

Step 3 —Run the Installer

HTTPS mode (recommended)

```
./InstallLogServer --https --cert </path/to/your_cert.pfx> --port 8443
```

HTTP mode

```
./InstallLogServer --port 8080
```

HTTP with custom config and data paths

```
./InstallLogServer --port 8080 --config /Path/LogServer/Config --
   database /Path/LogServer/Data
```

HTTPS with custom config and data paths

```
./InstallLogServer --https --cert </path/to/your_cert.pfx> --port 8443
   --config /path/to/LogServer/Config --database /path/to/LogServer/
   Data
```

Supporting CWA Client Log Uploads (optional)

```
#To support CWA client uploading AOT logs, some additional parameters
   need to be added after the install log server command.
--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:
   PORT
```

Where,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter	Description
`--sta-server`	`STA_SERVER_FQDN` is the hostname or IP address of the STA server. In an on-premises insta
`--log-server`	`LOG_SERVER_FQDN` and `PORT` are the hostname of the Log Server itself and the port specif

> **Note:**
>
> These parameters are optional if CWA clients do not need reconnection STA tickets or connect to the Log Server directly without a gateway.

Generated Script Files

After installation, the following scripts are created in the same directory:

- `StartLogServer.sh` —starts the Log Server container
- `GetAuthKey.sh` —generates an authentication key
- `DownloadLogsByTime.sh` —downloads logs by time range
- `DownloadLogsByWords.sh` —downloads logs by keyword
- `ListMachines.sh` —lists machines sending logs

Step 4 —Start the Log Server

```
./StartLogServer.sh
```

> **Note:**
>
> Linux startup typically takes 30–60 seconds.

Step 5 —Confirm the Log Server Started

```
cat $HOME/LogServer/Config/weblogs.txt
```

Look for:

```
Now listening on https://[::]:5000   # HTTPS mode
Now listening on http://[::]:5000    # HTTP mode
```

> **Warning:**
>
> If the Log Server runs in HTTPS mode, its certificate must be **trusted on all machines upload-**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **ing AOT logs**. Install the certificate on each component's Trusted Root Certification Authorities store.

Step 6 —Verify with Ping

```
https://YourLogServerFQDN:8443/Ping   # HTTPS mode
http://YourLogServerFQDN:8080/Ping    # HTTP mode
```

Expected: `Pong UTC:08/19/2025 01:03:29 Version: 2511.1.6`

> **Note:**
>
> - If verification fails, run `docker logs logserver` or check `$HOME/LogServer/Config/weblogs.txt` for errors.
> - Port 8443 and port 8080 are just for reference. Change port to your configured port if not using the default one.

Step 7 —Generate an Authentication Key

Run the generated script to create an authentication key:

```
./GetAuthKey.sh
```

Store the key securely —you will need it when configuring Web Studio or DaaS in the Configure Components step.

Mutual TLS (Optional —Advanced Security)

mTLS adds certificate-based mutual authentication between the Log Server and each client. Enable it only if your environment requires it.

Mutual TLS (mTLS) provides an additional layer of security between the Log Server and clients (VDA, DDC, StoreFront, CWA). When mTLS is enabled, both the client and the server authenticate each other using certificates issued by your enterprise PKI.

mTLS is useful in environments where:

- Network segments are untrusted or shared
- There is a requirement to authenticate not only the Log Server but also each AOT log client
- Customers want to prevent unauthorized systems from sending log data
- Regulatory or compliance policies require certificate-based authentication

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Although mTLS is optional, it enhances security by ensuring that only trusted Citrix components can communicate with the Log Server, and that the Log Server can verify every incoming connection before accepting telemetry data.

Certificate Requirements

File	Used By
`aotclient.pfx`	AOT log clients (VDA, DDC, StoreFront, CWA)
`logserver.pfx`	The Log Server
`enterprise-ca.cer`	Root/intermediate CA that signed both .pfx files

> **Note:**
>
> - Skip this Mutual TLS section if you use Citrix Connector Appliance, as it isn't supported.
> - The `enterprise-ca.cer` file must be imported into the Trusted Root Certification Authorities store on both the Log Server and telemetry clients.
> - The `aotclient.pfx` and `logserver.pfx` certificates should not be protected by password.
> - The subject of `aotclient.pfx` must be **CitrixAOTClient**, allowing the telemetry client to automatically locate the certificate during runtime.

Install with mTLS Enabled

```
./InstallLogServer --https --cert logserver.pfx --ca enterprise-ca.cer
   --port 8443

# with customized path
./InstallLogServer --config /YourPath/LogServer/Config --database /
   YourPath/LogServer/Data --cert /YourPath/logserver.pfx --ca /
   YourPath/enterprise-ca.cer --port 8443
```

Secure the Certificate Files

```
# delete temp certificate logserver.pfx in current install directory
sudo rm -rf /YourPath/logserver.pfx

# keep logserver.pfx accessed only by the container process user '
   ubuntu'.
sudo chmod 400 LogServer/Config/logserver.pfx
sudo chown ubuntu:ubuntu LogServer/Config/logserver.pfx
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure mTLS on Each Client (DDC, StoreFront, VDA)

If mutual TLS authentication is required, run the following PowerShell command in DDC, Storefront, VDA and other CVAD components with administrator privileges.

```
# import client cert at the machine aot client
Import-PfxCertificate -CertStoreLocation Cert:\LocalMachine\My\ -
    FilePath c:\aotclient.pfx

# Verify successful import
Get-ChildItem Cert:\LocalMachine\My | Where-Object {
  $_.Subject -like "*AOTclient*"  }


# delete temp certificate aotclient.pfx
Remove-Item -Path "C:\aotclient.pfx" -Force
# Ensure LogServer's certificate is trusted on all machines uploading
    AOT logs.
```

Grant NETWORK SERVICE Access to the Client Certificate

The telemetry service is running in “network service”account, so it is required to manually grant NETWORK SERVICE full control over the private key of the CitrixAOTClient certificate, using the certlm.msc graphical interface.

1. Press **Win + R**, type `certlm.msc`, press Enter.
2. Expand **Certificates (Local Computer)** → **Personal** → **Certificates**.
3. In the right pane, locate the certificate issued to **CitrixAOTClient**.
4. Right-click → **All Tasks** → **Manage Private Keys**.
5. Click **Add**, type `NETWORK SERVICE`, click **Check Names**.
6. Click **OK** to apply.

If customer supplies self-signed certificates, do as follows:

- On the logserver side, `logserver.pfx` and `aotclient.cer` are installed as previously described. The `aotclient.cer` serves the role of `enterprise-ca.cer`.
- On the client side, `aotclient.pfx` and `logserver.cer` are imported as previously described. The `logserver.cer` serves the role of `enterprise-ca.cer`.
- For more information, see Create a new certificate.

Upgrade

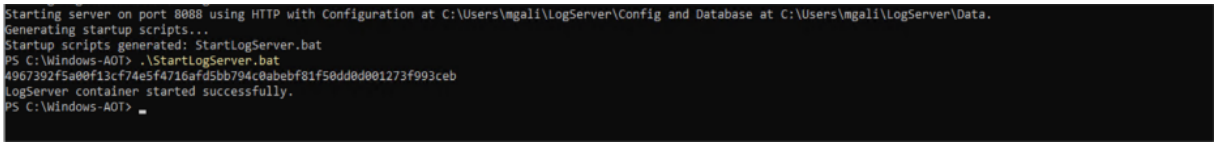
Before upgrading, remove the existing container by running:

```
docker rm -f logserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Download the new installation images and updated executable log server file.
2. Run `InstallLogServer` with the same arguments as the original installation.
3. When prompted, you may safely delete the current container and images —log data and configurations are saved separately.

> **Warning:**
>
> - To keep the old container, rename and stop it (`docker stop logserver`) before upgrading.
> - Never run both old and new containers simultaneously with the same `--data` path —doing so will corrupt log data.
> - After upgrading, use the newly generated scripts to start the Log Server.



> **Note:**
>
> This step is not required for Connector Appliance, as updates are managed automatically by Citrix.

Uninstall

```
docker rm -f logserver
docker rmi logserver

# List containers and images to make sure

docker ps -a
docker images

# Delete Log Server config and data files if not needed any more,
    change $HOME/LogServer to real installed path if not installed with
    the default one

rm -r $HOME/LogServer
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install the Log Server on Windows

August 18, 2026

> **Warning:**
>
> Docker Desktop on Windows is a user-session-based application. If the user who started Docker Desktop logs out, Docker Desktop stops —and the AOT Log Server container stops with it. **For production deployments, use Linux or the Connector Appliance instead.** If you must use Windows: keep the session active or in a **disconnected** state —do not fully log off.
> **Warning:**
>
> Running the Log Server on a Windows VM hosted on XenServer® is not supported. XenServer does not support nested virtualization, which prevents Docker from running inside the guest VM.

Prerequisites

- Supported OS: Windows 10, Windows 11, Windows Server 2022, or Windows Server 2025
- CPU: 8 cores minimum
- RAM: 24 GB minimum
- SSD-backed storage strongly recommended
- Docker Desktop installed (Docker Desktop subscription may be required)
- WSL version 2.1.5 or later
- Windows features enabled: Hyper-V, Virtual Machine Platform, Windows Subsystem for Linux
- Docker Desktop memory limit set to ≥ 12 GB
- Chosen port open in firewall rules and not in use
- TLS certificate in `.pfx` format (for HTTPS mode)

Step 1 —Install and Configure Docker Desktop

On a Windows machine, complete the following prerequisites.

1.1 —Enable Required Windows Features

Open **Windows Features** (search "Turn Windows features on or off") and enable: **Hyper-V**, **Virtual Machine Platform**, **Windows Subsystem for Linux (WSL)**. Restart if needed.

1.2 —Install Docker Desktop

Download and install Docker Desktop for Windows from Docker's website.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1.3 —Update WSL and Set Default Version

```
wsl --update
wsl --set-default-version 2
```

1.4 —Configure Docker Desktop Memory Limit

Open Docker Desktop → **Settings** → **Resources** → set **Memory** to at least **12 GB** → click **Apply & Restart**.

Step 2 —Download the Installer

Download the Log Server Docker container image and installer (`InstallLogServer.exe`) from Citrix Downloads. Place all downloaded files in the **same directory**.

Step 3 —Run the Installer

HTTP mode

```
InstallLogServer.exe --port 8080
```

HTTP with custom config and data paths

```
InstallLogServer.exe --port 8080 --config C:\LogServer\Config --
    database C:\LogServer\Data
```

HTTPS mode (recommended)

```
InstallLogServer.exe --https --cert c:\path\cert.pfx --port 8443
```

HTTPS with custom config and data paths

```
InstallLogServer.exe --https --cert c:\path\cert.pfx --port 8443 --
    config C:\LogServer\Config --database C:\LogServer\Data
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supporting CWA Client Log Uploads (optional)

```
#To support CWA client uploading AOT logs, some additional parameters need to be added after the install log server command.
--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:PORT
```

Where,

Parameter	Description
`--sta-server`	`STA_SERVER_FQDN` is the hostname or IP address of the STA server (In on-prem installation
`--log-server`	`LOG_SERVER_FQDN` and `PORT` are the hostname of the Log Server itself, and the port specif

> **Note:**
>
> These parameters are optional if CWA clients do not need reconnection STA tickets or connect to the Log Server directly without a gateway.

Generated Script Files

After installation, the following scripts are created in the same directory:

- `StartLogServer.bat` —starts the Log Server container
- `GetAuthKey.bat` —generates an authentication key
- `DownloadLogsByTime.bat` —downloads logs by time range
- `DownloadLogsByWords.bat` —downloads logs by keyword
- `ListMachines.bat` —lists machines sending logs

> **Note:**
>
> These files can be moved after installation —remember the new location for future configuration use.

Step 4 —Start the Log Server

```
StartLogServer.bat
```

> **Note:**
>
> Windows startup can take 1–10 minutes depending on hardware.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 5 —Confirm the Log Server Started

Check the web log file at `C:\Users\<username>\LogServer\Config\weblogs.txt`. Look for:

```
Now listening on: https://[::]:5000   # HTTPS mode
Now listening on: http://[::]:5000    # HTTP mode
```

Step 6 —Verify with Ping

```
https://YourLogServerFQDN:8443/Ping   # HTTPS mode
http://YourLogServerFQDN:8080/Ping    # HTTP mode
```

Expected: `Pong UTC:08/19/2025 01:03:29 Version: 2511.1.6`

> **Note:**
>
> - If verification fails, run `docker logs logserver` or check `C:\Users\<username>\LogServer\Config\weblogs.txt` for errors.
> - Port 8443 and port 8080 are just for reference. Change port to your configured port if not using the default one.

Step 7 —Generate an Authentication Key

Run the generated script to create an authentication key:

```
GetAuthKey.bat
```

Store the key securely —you will need it when configuring Web Studio or DaaS in the Configure Components step.

Mutual TLS (Optional —Advanced Security)

mTLS adds certificate-based mutual authentication between the Log Server and each client. Enable it only if your environment requires it.

Mutual TLS (mTLS) provides an additional layer of security between the Log Server and clients (VDA, DDC, StoreFront, CWA). When mTLS is enabled, both the client and the server authenticate each other using certificates issued by your enterprise PKI.

mTLS is useful in environments where:

- Network segments are untrusted or shared
- There is a requirement to authenticate not only the Log Server but also each AOT log client

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Customers want to prevent unauthorized systems from sending log data
- Regulatory or compliance policies require certificate-based authentication

Although mTLS is optional, it enhances security by ensuring that only trusted Citrix components can communicate with the Log Server, and that the Log Server can verify every incoming connection before accepting telemetry data.

Certificate Requirements

File	Used By
`aotclient.pfx`	AOT log clients (VDA, DDC, StoreFront, CWA)
`logserver.pfx`	The Log Server
`enterprise-ca.cer`	Root/intermediate CA that signed both .pfx files

> **Note:**
>
> - Skip this Mutual TLS section if you use Citrix Connector Appliance, as it isn't supported.
> - The `enterprise-ca.cer` file must be imported into the Trusted Root Certification Authorities store on both the Log Server and telemetry clients.
> - The `aotclient.pfx` and `logserver.pfx` certificates should not be protected by password.
> - The subject of `aotclient.pfx` must be **CitrixAOTClient**, allowing the telemetry client to automatically locate the certificate during runtime.

Install with mTLS Enabled

```
InstallLogServer.exe --https --cert logserver.pfx --ca enterprise-ca.
    cer --port 8443
```

Configure mTLS on Each Client (DDC, StoreFront, VDA)

If mutual TLS authentication is required, run the following PowerShell command in DDC, Storefront, VDA and other CVAD components with administrator privileges.

```
# import client cert at the machine aot client
Import-PfxCertificate -CertStoreLocation Cert:\LocalMachine\My\ -
    FilePath c:\aotclient.pfx

# Verify successful import
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ChildItem Cert:\LocalMachine\My | Where-Object {
  $_.Subject -like "*AOTclient*"  }


# delete temp certificate aotclient.pfx
Remove-Item -Path "C:\aotclient.pfx" -Force
# Ensure LogServer's certificate is trusted on all machines uploading
    AOT logs.
```

Grant NETWORK SERVICE Access to the Client Certificate

The telemetry service is running in "network service"account, so it is required to manually grant NETWORK SERVICE full control over the private key of the CitrixAOTClient certificate, using the certlm.msc graphical interface.

1. Press **Win + R**, type `certlm.msc`, press Enter.
2. Expand **Certificates (Local Computer)** → **Personal** → **Certificates**.
3. In the right pane, locate the certificate issued to **CitrixAOTClient**.
4. Right-click → **All Tasks** → **Manage Private Keys**.
5. Click **Add**, type `NETWORK SERVICE`, click **Check Names**.
6. Click **OK** to apply.

If customer supplies self-signed certificates, do as follows:

- On the logserver side, `logserver.pfx` and `aotclient.cer` are installed as previously described. The `aotclient.cer` serves the role of `enterprise-ca.cer`.
- On the client side, `aotclient.pfx` and `logserver.cer` are imported as previously described. The `logserver.cer` serves the role of `enterprise-ca.cer`.
- For more information, see Create a new certificate.

Upgrade

Before upgrading, remove the existing container by running:

```
docker rm -f logserver
```

1. Download the new installation images and updated executable log server file.
2. Run `InstallLogServer.exe` with the same arguments as the original installation.
3. When prompted, you may safely delete the current container and images —log data and configurations are saved separately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Warning:**
>
> - To keep the old container, rename and stop it (`docker stop logserver`) before upgrading.
> - Never run both old and new containers simultaneously with the same `--data` path —doing so will corrupt log data.
> - After upgrading, use the newly generated scripts to start the Log Server.

> **Note:**
>
> This step is not required for Connector Appliance, as updates are managed automatically by Citrix.

Uninstall

```
docker rm -f logserver
docker rmi logserver

# List containers and images to make sure

docker ps -a
docker images

# Delete Log Server config and data files if not needed any more,
    change ~/LogServer to real installed path if not installed with the
    default one

Remove-Item -Recurse -Force ~/LogServer
```

Configure the Log Server

August 18, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the Log Server is running, you may need to adjust retention, enable remote access for Director/-Monitor, verify health, or scale OpenSearch memory. Advanced settings are stored in the start script —changing them requires stopping the container, editing the script, and restarting.

Configuration Reference

Variable	Default	Range	Description
`MAX_RESERVE_DAYS`	7	1–30	Log retention in days. Logs older than this value are deleted. Checked every 10 minutes.
`MAX_DISK_USAGE_PERCENTAGE`	85	10–90	Disk usage threshold. When exceeded, old logs are deleted day by day until usage falls below this value.
`LOCAL_DOWN_ONLY`	true	true/false	When **`true`**, only the Log Server machine can call the `/Download/` APIs. Set to **`false`** to allow Director/Monitor and remote CLI access.
`OPENSEARCH_JAVA_OPTS`	`"-Xms2G -Xmx2G"`	2G → MaxMem/2	OpenSearch heap memory. Increase for larger environments.
`LOG_LEVEL`	2	0–4	Log verbosity. 0=Trace, 1=Debug, 2=Info, 3=Warning, 4=Error.
`CORS_ORIGINS`	(unset)	URL or `url1;url2`	Required for CWA HTML5/Chrome clients. Enter the allowed origin URLs separated by `;`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Editing Configuration on Linux or Windows

Step 1 —Stop the Container

```
docker stop logserver
```

Step 2 —Edit the Start Script

Open `StartLogServer.sh` (Linux) or `StartLogServer.bat` (Windows) in a text editor. Find the environment variable block and edit the values:

```
-e MAX_RESERVE_DAYS=14
-e MAX_DISK_USAGE_PERCENTAGE=85
-e LOCAL_DOWN_ONLY=false
-e OPENSEARCH_JAVA_OPTS="-Xms4G -Xmx4G"
```

Step 3 —Restart the Log Server

```
# Linux
./StartLogServer.sh

# Windows
StartLogServer.bat
```

Enabling Director/Monitor Access

By default, `LOCAL_DOWN_ONLY=true` restricts log downloads to the Log Server machine. To allow Citrix Director or Monitor to retrieve logs remotely:

1. Stop the container.
2. Set `LOCAL_DOWN_ONLY=false` in the start script.
3. Restart the Log Server.

> **Note:**
>
> When installed in HTTPS mode (version 2603 and later), `LOCAL_DOWN_ONLY` is automatically set to `false`. When installed in HTTP mode, it defaults to `true` and must be manually changed.

OpenSearch Memory Scaling

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connected Machines	Recommended Setting
0–999	`-Xms2G -Xmx2G`
1,000–1,999	`-Xms4G -Xmx4G`
2,000–9,999	`-Xms6G -Xmx6G`

Verifying Health

Ping Endpoint

```
https://YourLogServerFQDN:8443/Ping
```

Expected: `Pong UTC:<timestamp> Version: <version>`

Docker Logs

```
docker logs logserver
```

Container Health

```
docker exec -it logserver bash
curl http://localhost:5000/Ping
curl http://localhost:9200/_cluster/health?pretty
tail Config/applogs.txt
tail Config/weblogs.txt
exit
```

Check Current Configuration Values

```
docker exec -it logserver env | grep MAX_RESERVE_DAYS
```

Startup Log Location

Platform	Default Path
Linux	`$HOME/LogServer/Config/weblogs.txt`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Platform	Default Path
Windows	`C:\Users\<username>\LogServer\Config\weblogs.txt`
Custom install	`<your-config-path>\weblogs.txt`

> **Note:**
>
> Configuration on Citrix Connector Appliance is managed via the REST API. See the API section in Install on Connector Appliance.

Configure Components to Forward Logs

August 18, 2026

AOT Configuration Methods

Beginning with CVAD 2507 CU1 and CVAD 2511, AOT is configured using one of three methods depending on the component. CWA is a special hybrid case —it requires Web Studio to set the log server address (propagated via StoreFront™) and a native registry key to enable the collection switch.

Configuration Method	Target Component Type	Upload Path	Applicable Components
Web Studio (Centralized)	CVAD Core Components	Web Studio → Component → Telemetry Service → Log Server	DDC, StoreFront, VDA, Director
Telemetry PowerShell Cmdlets (Local)	Standalone CVAD Components That Rely on Telemetry Service	Component → Telemetry Service → Log Server	PVS, Session Recording Server, FAS, WEM
Component Native (Direct Upload)	Other Components That Do Not Rely on Telemetry Service	Component → Log Server (direct)	License Server, NetScaler® / Citrix Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Method	Target Component Type	Upload Path	Applicable Components
Web Studio + Component Native (Hybrid)	Citrix Workspace App (Special Case)	Web Studio → StoreFront → CWA → Log Server (direct)	CWA for Windows / HTML5 / Chrome OS

Citrix Web Studio for on-premises and Citrix DaaS™ Settings for cloud provide a centralized location for configuring, centralizing, and forwarding Always On Tracing (AOT) logs across the site or sites. This setting defines where AOT logs are sent and automatically propagates the configuration to relevant components in the environment.

When you configure the log server in Web Studio:

- The configuration is written in the Site database.
- Delivery Controllers retrieve the updated settings and distribute them to the VDAs in the selected delivery groups.
- VDAs use the received configuration to forward their AOT logs to the specified log server.
- StoreFront that participates in AOT logging receives the necessary details through the same centralized mechanism.
- Director uses the provided AuthKey and log server details to query and display AOT logs for monitoring and troubleshooting.

This centralized approach removes the need to configure each component individually. You set up the log server details once in Web Studio, and Citrix automatically propagates the configuration across the site.

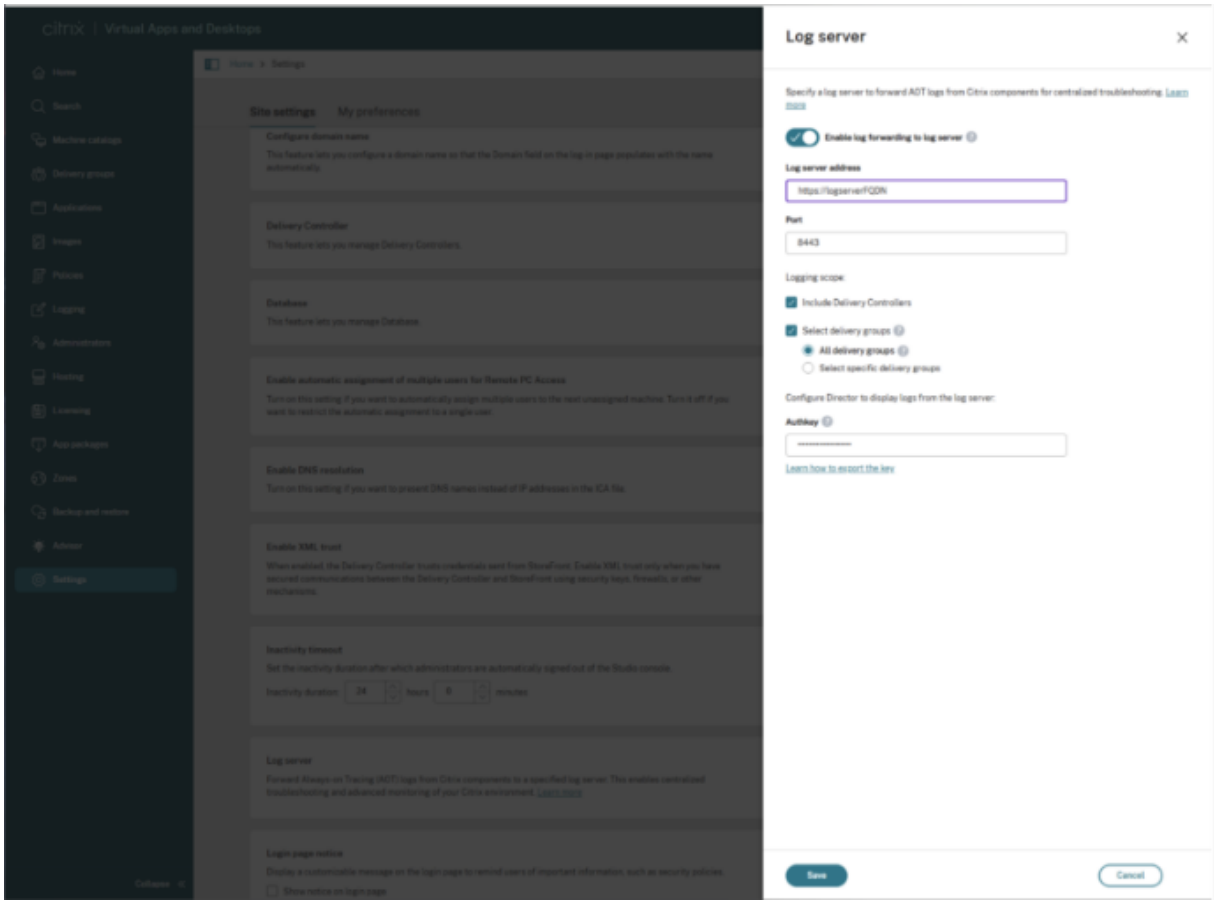
Configuring Web Studio propagates Log Server details automatically to DDC, VDA, StoreFront, Director, and CWA. **You set this once. Citrix distributes it automatically.**

On-Premises CVAD —Citrix Web Studio

1. Sign in to **Citrix Web Studio**.
2. Select **Settings** in the left pane.
3. In the **Log server** tile, click **Add** (or **Edit** if already configured).
4. Turn on **Enable log forwarding to log server**.
5. Enter the **Log server address** (FQDN) and **Port**.
   If using the Connector Appliance, enter port 443 only.
6. Under **Logging scope**, choose which components forward logs.
7. Enter the **AuthKey** generated from the Log Server (see Step 7 for Connector Appliance, Linux, or Windows).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Click **Save**.



> **Warning:**
>
> **Known Issue (fixed in 2603 / Web Studio 73):** If you modify the Log Server address or port without re-entering the AuthKey, the key placeholder is cleared after saving —even though the save appears successful. This causes Director/Monitor to fail silently. Always re-enter and validate the AuthKey whenever editing Log Server settings.

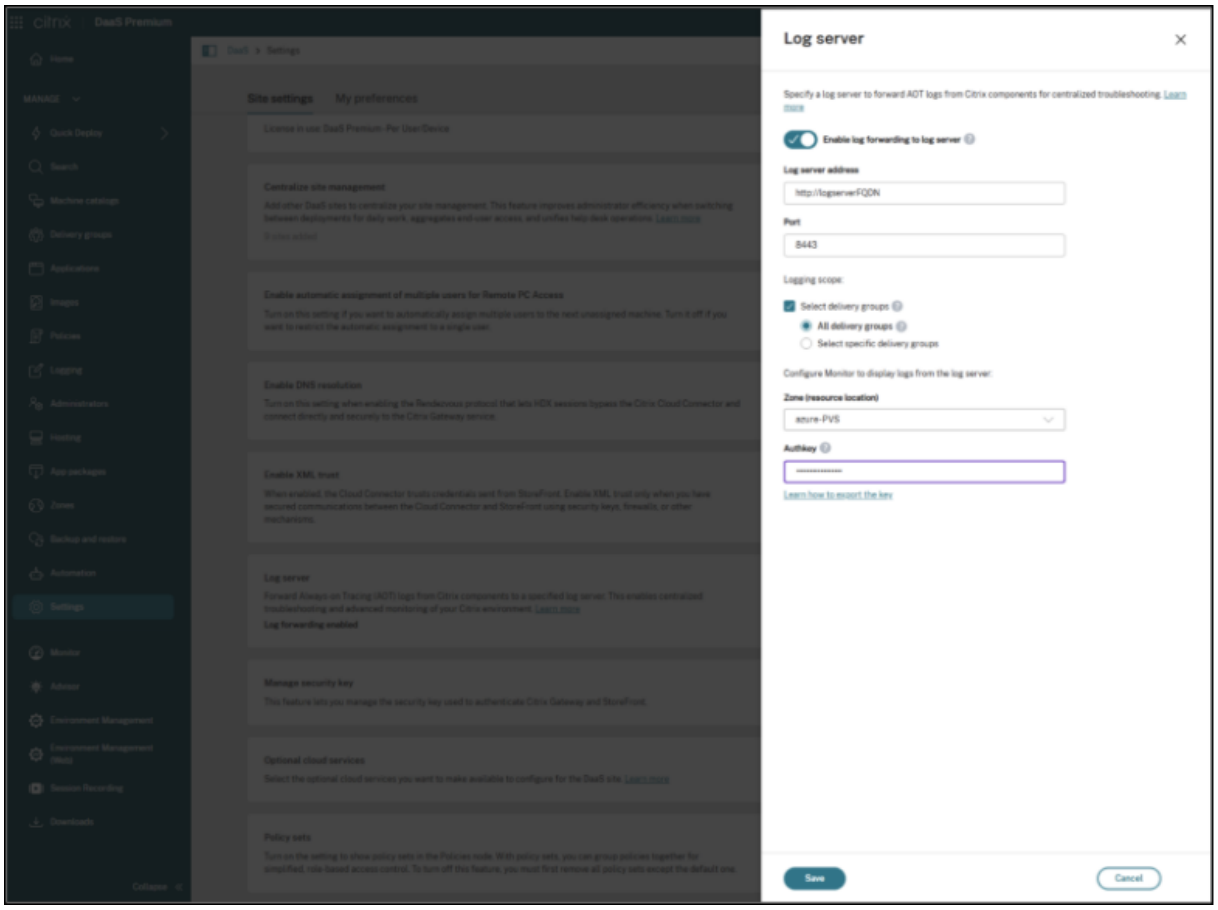
Citrix DaaS —Cloud Environment

> **Note:**
>
> Citrix DaaS control plane components (Cloud DDC) do not forward logs to your customer-managed Log Server. Only components in your resource location (VDAs, StoreFront, Gateway) forward logs to your Log Server.

1. Sign in to **Citrix Web Studio for DaaS**.
2. Select **Settings** → **Log server** tile → click **Add**.
3. Enter the **Log server address** and **Port**.
4. Under **Logging scope**, select delivery groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select the **Zone (resource location)** where the Log Server is deployed.
6. Enter the **AuthKey** generated from the Log Server (see Step 7 for Connector Appliance, Linux, or Windows).
7. Click **Save**.



Log Forwarding Configuration for Other Components

Not all Citrix components receive Log Server configuration automatically through Web Studio or the Site database. Components such as Session Recording Server, FAS, PVS, License Server, NetScaler, and Cloud Connector (with on-prem DDC) operate independently and must be configured separately on each server. The steps below cover how to enable AOT log forwarding for each of these components.

Configure AOT Log Upload for StoreFront in Citrix Cloud Deployments

For Citrix Cloud (hybrid) deployments, when on-prem StoreFront is used (instead of Citrix Workspace) with Cloud DDC, StoreFront does not automatically receive the AOT Log Server configuration from

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the Cloud Connector. Run the following PowerShell command on the StoreFront server to manually configure the AOT Log Server endpoint.

Run the following command in StoreFront PowerShell:

```
# Enable
Enable-CitrixAOTUpload -AoTDataStoreEndpoint https://FQDNofLogServer
    :8443 -Role StoreFront

# Disable
Disable-CitrixAOTUpload
```

> **Note:**
>
> Execute this command only for Citrix Cloud (hybrid) deployments that use Cloud DDCs. Do not run this command for on-premises CVAD deployments where StoreFront is paired with on-premises Delivery Controllers, as the Log Server configuration is automatically synchronized and no manual configuration is required.

Session Recording Server

```
Enable-CitrixAOTUpload -AotDataStoreEndpoint https://YourLogServerFQDN
    :8443 -Role SessionRecording
Disable-CitrixAOTUpload
```

Federated Authentication Service (FAS)

```
Enable-CitrixAOTUpload -AotDataStoreEndpoint https://YourLogServerFQDN
    :8443 -Role FAS
Disable-CitrixAOTUpload
```

Provisioning Services (PVS)

```
Enable-CitrixAOTUpload -AotDataStoreEndpoint https://YourLogServerFQDN
    :8443 -Role PVS
Disable-CitrixAOTUpload
```

> **Note:**
>
> - If you have multiple servers, run this command on each one individually.
> - Replace your Log Server FQDN with the actual FQDN of your Log Server, and port number 8443 with the actual port number that you have selected. This is just for example purposes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workspace Environment Management (WEM)

```
Enable-CitrixAOTUpload -AotDataStoreEndpoint https://YourLogServerFQDN
    :8443 -Role WEM
Disable-CitrixAOTUpload
```

License Server

Uploading AOT Logs for License Server

The Log Server URL needs to be updated inside the SLS config file, which can be found at the location `C:\Program Files (x86)\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml` with XML tag `AotServerURL`.

Example:

```
<AotServerURL>https://FQDNofLogServer:443/ctxlogserver/
    UploadCitrixLogStream</AotServerURL>
```

> **Note:**
>
> - **When are logs generated in License Server?** License Server AOT logs are generated only during specific events such as: License Server installation or upgrade, WSL (Citrix Web Services for Licensing) service restart, license activation failure, dark site activation failures, and clock-related licensing issues.
> - If none of these events occurred recently, the absence of logs does not necessarily indicate a problem.

Quick Checks

- Confirm whether a qualifying event (restart, upgrade, activation issue, etc.) occurred recently.
- Restart the Citrix Web Services for Licensing service and allow up to one hour for upload processing.
- Verify the AOT Log Server URL is configured correctly.
- Confirm the Citrix Web Services for Licensing service is running.
- Check: `C:\Program Files (x86)\Citrix\Licensing\LS\resource\aot` —if the file contains data, logs may be waiting for upload.

> **Note:**
>
> - License Server AOT logging is event-driven, not continuous. It is normal to see no logs when no qualifying events have occurred.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - The License Server periodically uploads the logs to the AOT Log Server automatically.

Cloud Connector

Configure AOT Logs Upload for Citrix Connector

To collect Cloud Connector logs in the AOT Log Server, the following requirements apply:

- Cloud Connector must be on version **6.169.0.22492** or later.
- In Cloud DDC deployments, Log Server configuration details are automatically synchronized to the registry with the May release, and no manual configuration is required.
- In hybrid deployments (on-prem DDC), manual registry configuration is required to enable log collection. Create the following registry entries on the Cloud Connector machine:
  - Path: `HKLM\Software\Citrix\ConfigSyncService`
  - Entries:
    - `LogServerEnabled` (`REG_DWORD`) = 1
    - `LogServerEndpoint` (`REG_SZ`) = `https://<logserver-fqdn>:<port>`

NetScaler Gateway

Step 1 —SSH into NetScaler and Enter Shell

```
shell
```

Step 2 —Navigate to the Analytics Config Directory

```
cd /var/analytics_conf
```

Step 3 —Generate the Schema File

Run the interactive Python script to define HTTP headers and payload attributes:

```
python auditlog_schema_generator_for_hec_export.py
```

The script prompts for fields like `Auth-Token`, `Content-type`, `User-agent`, `Role`, `HostName`, and `MachineIP`. Each can be included or excluded and given aliases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Snippet of the output generated by this script

```
root@Raju-adc2# python auditlog_schema_generator_for_hec_export.py
Schema Builder: Follow the prompts to define your schema.
Include 'Auth-Token'? (Y/n):
Enter the display name (alias) for 'Auth-Token' (press Enter to keep as
    is): Authkey
'Auth-Token' can only go in 'header'. Automatically selected.
Include 'HostName'? (Y/n): n
Include 'Content-type'? (Y/n): y
Enter the display name (alias) for 'Content-type' (press Enter to keep
   as is):
'Content-type' can only go in 'header'. Automatically selected.
Default value for 'Content-type' is 'application/json'.
Do you want to change it? (y/N):
Include 'User-agent'? (Y/n):
Enter the display name (alias) for 'User-agent' (press Enter to keep as
    is):
'User-agent' can only go in 'header'. Automatically selected.
Default value for 'User-agent' is 'AUDITLOGS/1.0'.
Do you want to change it? (y/N):
Include 'Role'? (Y/n): y
Enter the display name (alias) for 'Role' (press Enter to keep as is):
Where should 'Role' be included? (HEADER/payload): HEADER
Default value for 'Role' is 'GW'.
Do you want to change it? (y/N): y
Enter new default value for 'Role': Gateway
```

Sample schema file generated:

```
{

    "Header": {

        "Auth-Token": {

            "name": "AuthKey"
         }
 ,
        "Content-type": {

            "name": "Content-type",
            "value": "application/json"
         }
 ,
        "User-agent": {

            "name": "User-agent",
            "value": "AUDITLOGS/1.0"
         }
 ,
        "Role": {

            "name": "Role",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "value": "Gateway"
            }
    ,
           "MachineIP": {

                "name": "MachineIP"
            }
    ,
           "MachineName": {

                "name": "MachineName"
            }

        }
    ,
       "Payload": {

           "LogLevel": "Level",
           "MessageContent": "Message",
           "ModuleName": "Module",
           "Time": "TimeStamp"
        }
    ,
       "Format": {

           "delimiter": ""
        }

    }
```

Step 4 —Exit Shell and Return to NetScaler CLI

```
exit
```

Step 5 —Create a Syslog Action which defines the Syslog Server, Ports and the schema file (created in the previous step) etc

```
add audit syslogAction {
 Action Name }
  {
 AOT Server IP/FQDN }
  -serverPort {
 Destination Port }
  -logLevel {
 Log Level }
  -transport HTTP -httpAuthToken {
 Auth Token }
  -httpEndpointUrl {
 AOT Server URL }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -httpSchemaFile {
Schema File }
```

Example:

```
add audit syslogAction act1 10.102.154.196 -serverPort 8088 -logLevel
    ALL -transport HTTP -httpAuthToken fbb94d5b234d86a6cb155e3f808dd33c
    -httpEndpointUrl "/services/collector/event" -httpSchemaFile sample.
    json
```

Step 6 —Bind the syslogAction to the Audit Syslog Policy

```
add audit syslogPolicy {
 PolicyName }
  True {
 SyslogActionName }
```

Example:

```
add audit syslogPolicy pol1 true act1
```

Citrix Workspace App (CWA)

System Requirements

Ensure the required version of the selected Citrix Workspace App (CWA) is installed. For more information, see Supported versions.

CWA log upload is **automatic** in the on-prem setup with Direct access to StoreFront, and via Citrix Gateway —no manual configuration is required on individual clients. When AOT is enabled via Web Studio or DaaS Settings, CWA automatically uploads client-side AOT logs when a user launches a resource.

CWA logs upload in fully cloud and hybrid cloud scenarios will be supported in future releases.

> **Note:**
>
> CWA HTML5 and ChromeOS clients require the `CORS_ORIGINS` setting to be configured on the Log Server. Add the allowed origin URLs to the `CORS_ORIGINS` variable in the start script.

Citrix Workspace App Web Launches

For Citrix Workspace App web launches (including WebHelper, direct ICA file download, and web browser extension launch methods), StoreFront must be configured to use the modern User Interface

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(UI Experience). For instructions on enabling the modern UI experience, see the StoreFront documentation.

Configuration Best Practices

> **Warning:**
>
> **Do Not Mix Configuration Methods on the Same Machine**
>
> - Never run Telemetry PowerShell Cmdlets on machines that host CVAD Core Components (DDC, Director, StoreFront, or VDA). Doing so can cause incorrect or overwritten `Role` registry values, configuration drift between components, and broken synchronization paths between DDC and StoreFront.
> - Always use Web Studio as the single source of truth for AOT configuration on any machine hosting a CVAD Core Component.
>
> **Warning:**
>
> **Always Re-Enter AuthKey When Modifying Log Server Settings**
>
> - Whenever the log server address or port is changed in Web Studio, the AuthKey must be re-entered. If saved without re-entering, the value becomes empty —causing Director and Monitor to lose the ability to authenticate against the log server.
>
> **Warning:**
>
> **PVS Multi-Node Environments Require Per-Machine Configuration**
>
> - PVS does not support centralized propagation. `Enable-CitrixAOTUpload` must be run individually on every PVS server in the environment.
>
> **Note:**
>
> **CWA AOT Upload Requires Both Web Studio and Registry Key Configuration**
>
> - CWA AOT log upload depends on two independent conditions both being satisfied: Web Studio is configured with a valid log server address and the address is propagated to StoreFront, and the `AotLogCollectionEnabled` registry key is set to `True` on the CWA client machine.
> - A user must also actively launch a resource to trigger the upload.
> - Always complete the Web Studio and StoreFront configuration before enabling the CWA registry key.
>
> **Note:**
>
> **Verify Minimum Version Requirements Before Deployment**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> - Full cross-component AOT log collection requires CVAD 2511 or CVAD 2507 CU1 or later.
> - The License Server-specific AOT upload issue was resolved in version 2603. Ensure your License Server is updated accordingly.

Verify Component Configuration

August 12, 2026

Telemetry-Based Components

For all components that use the Telemetry Service (DDC, StoreFront™, VDA, PVS, FAS, Session Recording, WEM), the configuration is written to the same registry location and can be verified using the following methods.

Registry Path

All Telemetry-based components share this registry path, managed exclusively by the Telemetry Service:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry\AOT
```

Registry Query Commands

Windows-based components (DDC, StoreFront, Windows VDA, PVS, FAS, Session Recording, WEM):

```
Get-ItemProperty -Path "HKLM:\SOFTWARE\Citrix\Telemetry\AOT"
```

Linux VDA and Mac VDA:

```
/opt/Citrix/VDA/bin/ctxreg dump | grep -i AOT
```

Expected Registry Values

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registry Value	Type	Expected Value	Description
`EnableAotDataCollection`	DWORD	1	AOT is enabled. 0 means AOT is disabled.
`AotDataStoreEndpoint`	REG_SZ	:	The log server endpoint. Must not be empty.
`Role`	REG_SZ	See table below	Identifies which Citrix component role(s) are active on this machine.

Expected Role Values by Component

Machine Type	Expected Role Value
Delivery Controller only	`DDC`
StoreFront only	`StoreFront`
DDC + StoreFront on the same machine	`DDC,StoreFront`
Windows VDA	`WVDA`
Linux VDA	`LVDA`
Mac VDA	`MVDA`
PVS Server	`PVS`
FAS Server	`FAS`
Session Recording Server	`SessionRecording`
WEM Server	`WEM`

Verify via Telemetry Service Log

In addition to registry checks, confirm that the Telemetry Service has successfully initialized AOT log collection by inspecting the AOT Listener log file.

Log File Location:

```
C:\ProgramData\Citrix\TelemetryService\AotListener.log
```

Verification Command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Select-String -Path "C:\ProgramData\Citrix\TelemetryService\AotListener
    .log" `
     -Pattern "Adding provider|Start RealTimeAOTTraceSession"
```

Key Log Entries to Look For:

Log Entry	Description
`Adding provider [GUID] for AOT Uploading`	A specific component provider has been successfully registered for AOT log collection.
`Start RealTimeAOTTraceSession for [Role]`	The real-time AOT trace session has been started for the specified component role (e.g., DDC, StoreFront, VDA).

Direct-Upload Components

The following components bypass the Telemetry Service and upload AOT logs directly to the log server. Verification must be performed using component-specific methods.

License Server

Run the following command to confirm the `AotServerURL` value is populated in the License Server config file:

```
Select-String -Path "C:\Program Files (x86)\Citrix\Licensing\
    WebServicesForLicensing\SimpleLicenseServiceConfig.xml" `
     -Pattern "AotServerURL"
```

Expected Output:

```
<AotServerURL>https://<log-server-ip>:<port>/ctxlogserver/
    UploadCitrixLogStream</AotServerURL>
```

Citrix Workspace App (CWA) for Windows

CWA uses a native registry key to control the AOT collection switch. Verify it is set correctly on the client machine:

Registry Path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle
```

Verification Command:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-ItemPropertyValue -Path "HKLM:\SOFTWARE\WOW6432Node\Citrix\Dazzle"
    `
    -Name "AotLogCollectionEnabled"
```

Expected Output: `True`

> **Note:**
>
> Even when this registry key is correctly set, CWA AOT logs are only uploaded when a user actively launches a resource. If no uploads are observed, confirm that AOT is enabled on the Delivery Controller side first, and verify that StoreFront has a valid log server address synchronized from Web Studio.

NetScaler® / Citrix Gateway

Verification is performed through the NetScaler CLI.

Step 1 —Verify the Syslog Action exists and is correctly configured:

```
show audit syslogAction <ActionName>
```

Field	Expected Value
`Server`	IP or FQDN of the AOT log server
`serverPort`	Configured log server port
`Transport`	HTTP
`httpEndpointUrl`	AOT log server URL
`httpAuthToken`	AuthKey value (non-empty)
`httpSchemaFile`	Path to the generated schema file

Step 2 —Verify the Syslog Policy is bound:

```
show audit syslogPolicy <PolicyName>
```

Expected Output:

```
Name: <PolicyName>    Rule: TRUE    Action: <ActionName>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Server API Response Codes

August 12, 2026

The following table documents all HTTP response codes used by the Citrix Log Server API. These codes help clients determine request success, diagnose issues, and debug API calls when integrating with the Log Server.

Code	Status	Description
200	OK	Request succeeded.
400	Bad Request	Server couldn't process the request due to missing parameters, malformed syntax, or absent required HTTP headers (e.g., missing MachineName or Role fields).
401	Not Authorized	Client not permitted to access the Log Server —triggered when the IP address or AuthKey is not allowed.
404	Not Found	The API path requested does not exist —returned when the endpoint is invalid or mistyped.
500	Internal Error	Unexpected server-side condition preventing fulfillment; commonly caused by resource exhaustion such as memory or disk space issues.

View and Use Logs

August 18, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Method	Best For
Citrix Director UI	Day-to-day monitoring, searching by user/machine/event
CLI scripts (Log Server)	Bulk downloads, automated workflows, support escalations

Configure the LOCAL_DOWN_ONLY Setting

The `LOCAL_DOWN_ONLY` setting controls whether Citrix Director/Monitor can retrieve AOT logs remotely from the Log Server. The way this setting is configured depends on your deployment type.

- **Windows** —Edit the `StartLogServer.bat` file. This file contains all configuration parameters used to start the AOT Log Server container, including `LOCAL_DOWN_ONLY`.
- **Linux** —Edit the `StartLogServer.sh` file. The same `LOCAL_DOWN_ONLY` variable applies with identical behavior.
- **Connector Appliance** —The Connector Appliance does not use a start script. `LOCAL_DOWN_ONLY` defaults to **`false`**, enabling Citrix Director and Monitor to retrieve logs remotely without additional configuration.

Regardless of deployment type, the behavior of this setting is the same:

- When `LOCAL_DOWN_ONLY=`**`false`**, the Log Server accepts remote log-viewing requests. This allows Citrix Director/Monitor to connect to the Log Server and display AOT logs directly in the Monitor UI.
- When `LOCAL_DOWN_ONLY=`**`true`**, the Log Server restricts log access to local-only connections. In this mode, you must connect directly to the Log Server machine to view logs, and Citrix Director/Monitor will not be able to retrieve or display logs.

Method 1 —Citrix Director

Prerequisites

1. `LOCAL_DOWN_ONLY=`**`false`** must be set in the Log Server start script.
2. Web Studio must be configured with the Log Server address, port, and AuthKey.
3. Once Web Studio is saved, Director automatically receives the Log Server connection details.

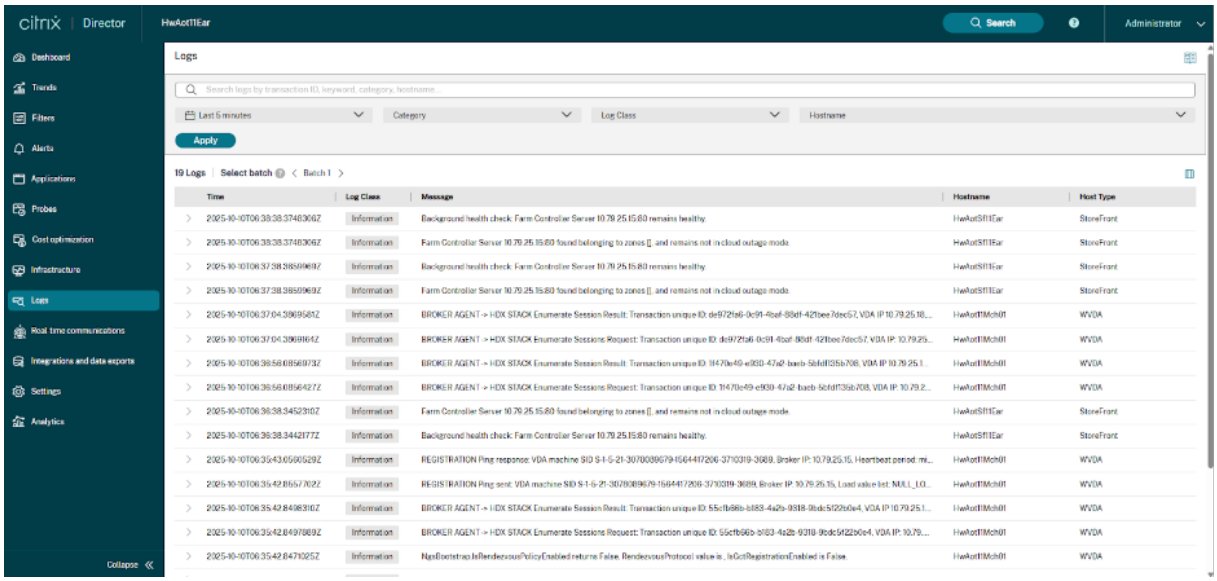
Accessing the Logs Page

1. Open **Citrix Director**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. A new **Logs** item appears in the left navigation panel.
3. Click **Logs**. If a Get Started screen appears, click **Close**.

Searching and Filtering



Free-text search —type any keyword: username, machine name (`VDAWIN01`), event keyword (`registration`, `authentication`), transaction IDs, or error message strings.

Time filter —narrow results to Last 5 minutes, Last 1 hour, Last 24 hours, or a custom range.

Category filter —filter by subsystem: Application launch, Registration, VDA configuration, Graphics, HDX™ Direct, ICA connection.

Log Class filter —filter by severity: Information, Warning, Error, Failure.

Hostname filter —drill into logs for a single specific machine.

Method 2 —CLI Scripts

Step 1 —Generate an AuthKey

```
# Linux
./GetAuthKey.sh <role-name>

# Windows
GetAuthKey.bat <role-name>
```

Replace <`role-name`> with any label (e.g., `admin`, `support`). The output is a long 32-bit hex string —copy and save it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2 —List Machines That Have Sent Logs

```
# Linux
./ListMachines.sh <AuthKey>

# Windows
ListMachines.bat <AuthKey>

# Remote (PowerShell)
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/ListMachine" `
  -Headers @{
  AuthKey = "<AuthKey>"  }
```

Step 3 —Download Logs by Time Range

```
# Linux
./DownloadLogsByTime.sh <AuthKey> <MachineName> <StartTime> <EndTime> <OutputFile>

# Example
./DownloadLogsByTime.sh ebac9b77... VDAWIN01 2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv

# Windows
DownloadLogsByTime.bat <AuthKey> <MachineName> <StartTime> <EndTime> <OutputFile>
```

> **Note:**
>
> Time values must be in **UTC format:** `YYYY-mm-ddTHH:MM:SSZ`

Step 4 —Download Logs by Keyword

```
# Linux
./DownloadLogsByWords.sh <AuthKey> <StartTime> <EndTime> "session launch" logs.csv

# Windows
DownloadLogsByWords.bat <AuthKey> <StartTime> <EndTime> "failed vda" logs.csv
```

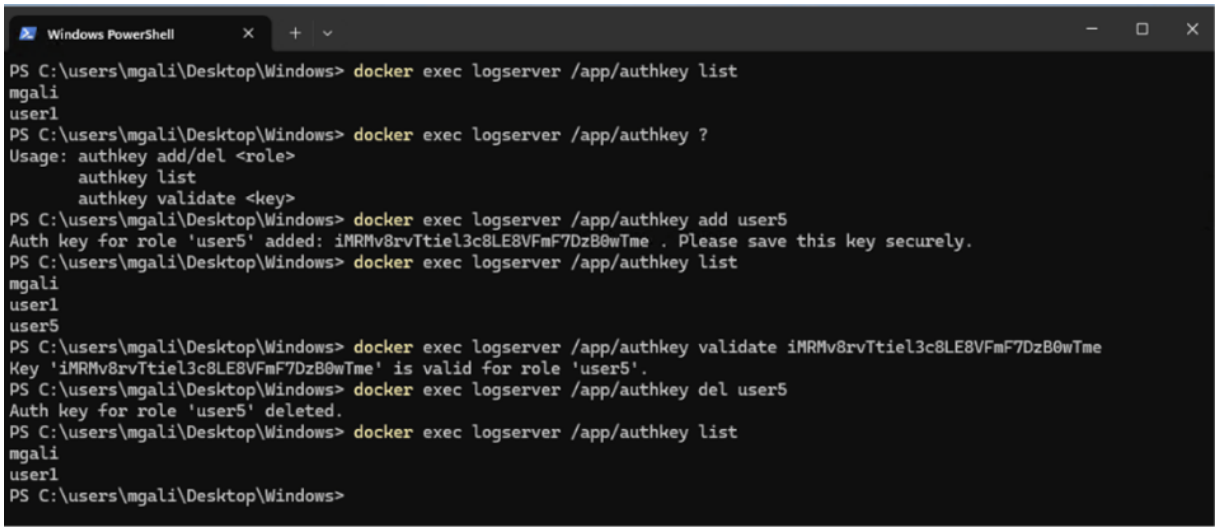
Managing Auth Keys

The AOT Log Server provides commands to manage authentication keys associated with different roles or users. These commands allow administrators to add, list, validate, and delete auth keys di-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rectly from the container. Use the available docker exec commands directly on the Log Server container.

Action	Command
Add a new key	`docker exec logserver /app/authkey add <RoleName>`
List all keys	`docker exec logserver /app/authkey list`
Validate a key	`docker exec logserver /app/authkey validate <key>`
Delete a key	`docker exec logserver /app/authkey del <RoleName>`
View help	`docker exec logserver /app/authkey ??`



Log Server API Response Codes

Code	Status	Meaning
`200`	OK	Request succeeded
`400`	Bad Request	Missing parameters, malformed headers, or missing required fields

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Code	Status	Meaning
401	Not Authorized	IP address or AuthKey is not permitted to access the Log Server
404	Not Found	API endpoint path is invalid or mistyped
500	Internal Error	Server-side issue —commonly disk space exhaustion or memory pressure

Common Issues and Fixes

August 18, 2026

Quick Diagnostics

```
# 1. Is the container running?
docker ps

# 2. Is the Log Server responding?
curl https://YourLogServerFQDN:8443/Ping

# 3. Any errors in the container?
docker logs logserver

# 4. Has any component sent logs?
./ListMachines.sh <AuthKey>

# 5. OpenSearch health (from inside container)
docker exec -it logserver curl http://localhost:9200/_cluster/health?
   pretty
```

Top Challenges

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Symptom	Most Likely Cause
Director shows no Logs menu	`LOCAL_DOWN_ONLY=true` or AuthKey not saved
ListMachines returns empty array	Components not yet sending, AuthKey mismatch, or cert not trusted
Log Server container not starting	Docker memory, port conflict, or cert issue

Troubleshooting by Issue

Director Cannot Display Logs

1. Confirm `LOCAL_DOWN_ONLY=false` is set in the Log Server start script. Stop the container, edit the script, restart.
2. Confirm Web Studio is configured with the correct Log Server address, port, and a valid AuthKey.
3. Confirm network connectivity from the Delivery Controller to the Log Server on the configured port.
4. Confirm the Log Server TLS certificate is trusted on the Director machine.

No Machines Appearing in ListMachines

1. Wait 5–10 minutes. Components begin uploading after the Telemetry Service activates.
2. Confirm the component can reach the Log Server: ping the FQDN from the VDA or DDC.
3. Confirm the TLS certificate is trusted on the component machine (HTTPS mode).
4. Confirm the AuthKey entered in Web Studio matches a key on the Log Server (`docker exec logserver /app/authkey list`).
5. Check the Telemetry Service status on a VDA or DDC: open Services (`services.msc`) and look for `CitrixTelemetryService`.

Log Server Container Not Starting

1. Check Docker logs: `docker logs logserver`
2. Check the weblogs.txt file for the startup failure reason.
3. Confirm the port is not already in use:

```
# Linux
ss -tlnp | grep 8443

# Windows
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
5    netstat -ano | findstr 8443
```

1. On Windows, confirm Docker Desktop is running and has ≥ 12 GB memory allocated.
2. Confirm the `.pfx` certificate file exists and is not password-protected.

Director/Monitor Cannot Remotely Access Logs

Check `LOCAL_DOWN_ONLY` setting first. If already **`false`**, check for a port conflict (known issue XASUP-7658). Stop the container, change the port in the start script, restart, and update the port in Web Studio.

Troubleshoot Common Issues with Always On Tracing

August 27, 2026

Applies to: Citrix Virtual Apps and Desktops™ 2402 CU4, 2507 CU1, 2511, 2603 and later, DaaS **Requires:** AOT L

Always On Tracing (AOT) captures logs continuously across all Citrix components —VDAs, Delivery Controllers, StoreFront™, License Server, and Citrix Workspace App. When a problem is reported, the data is already there. This article shows how to use the **Logs** node in Citrix Director or Monitor to identify the cause of an issue and how to export logs from Director or Monitor for submission to Citrix Technical Support.

> **Note:**
>
> **Before you start —collect this for every scenario**
>
> - **Affected user or machine** —a specific username, VDA hostname, or delivery group name
> - **Time of failure** —even an approximate window helps narrow the default time filter. Adjust the time range to cover the period before the reported failure.
> - **Scope** —one user, one machine, or environment-wide? Scope alone often points to the correct failure pattern before you open a log
> - **Recent changes** —any CVAD updates, Group Policy changes, power management changes, or network changes in the relevant window

When to Use AOT for Customer-Reported Issues

AOT is designed to help with a broad range of customer-reported issues. The following are some of the most commonly reported issue types where AOT logs can be sufficient to either isolate or find the root

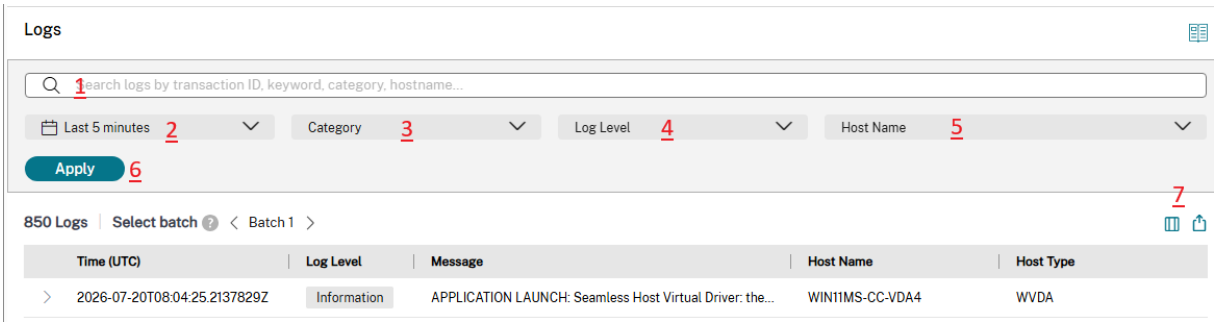
© 1997–2026 Citrix Systems, Inc. All rights reserved.

cause. This list does not cover every possible issue —there are many other issue types where AOT logs can also help. Most of these issues can definitely be isolated with AOT logs —you can identify the component at fault or sometimes find the root cause as well. You don't always need to escalate or collect additional traces for the issue types below, unless otherwise requested by a support engineer.

- StoreFront login failure
- CWA store adding failure
- Resource enumeration failure or slowness
- ICA® session launch failure
- Post-launch session slowness
- MCS provisioning failure
- Citrix policy applying failure
- User profile load/unload failure or slowness
- Power action failure or delay
- Clipboard mapping failure
- FAS authentication failure
- Citrix Director data retrieval failure
- Session not being recorded

The Logs node in Director and Monitor

The Logs node is available in both **Citrix Director** (on-premises CVAD) and **Citrix Monitor** (DaaS). To access it, select **Logs** from the left navigation panel. The interface is the same in both environments.



1. **Search bar** —keyword, transaction ID, category, or hostname
2. **Time filter** —select the window that covers the failure
3. **Category filter** —filter by event type
4. **Log Level filter** —filter by severity
5. **Host Name filter** —select one or more machines
6. **Apply button** —applies all active filter selections
7. **Export icon** —download logs to submit to Citrix Technical Support

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filter bar

The filter bar has four filters and a separate **Apply** button. Set the filters first, then click **Apply** to refresh the log view. The current log count appears below the filter bar —for example, `850 Logs | Batch 1`. Use the batch navigation arrows to page through large result sets.

Filter	What it does	Options
Time	Sets the time window for log retrieval. Set this to a window that starts before the reported failure to capture the events that led up to it.	Last 5 minutes ·Last 1 hour ·Last 24 hours ·Last 48 hours ·Last 7 days ·Custom (UTC) *(CVAD 2603 and later cloud release only)*
Category	Filters by event type. Each category corresponds to a specific part of the Citrix component lifecycle. Includes a Search Category field to quickly find a category by name.	Application Launch ·Clipboard · CWA-PostLaunch · CWA-PreLaunch ·Database · Devices ·and more
Log Level	Filters by severity. Select one or more. When a selection is active, the button label shows the number selected (e.g., *1 Log Level Selected*).	Information ·Warning ·Error · Critical
Host Name	Filters to one or more specific machines. Includes a Search Host field and a checkbox list of all machines currently sending logs to the Log Server. When active, shows *N Hostname Selected*.	All machines registered with the Log Server

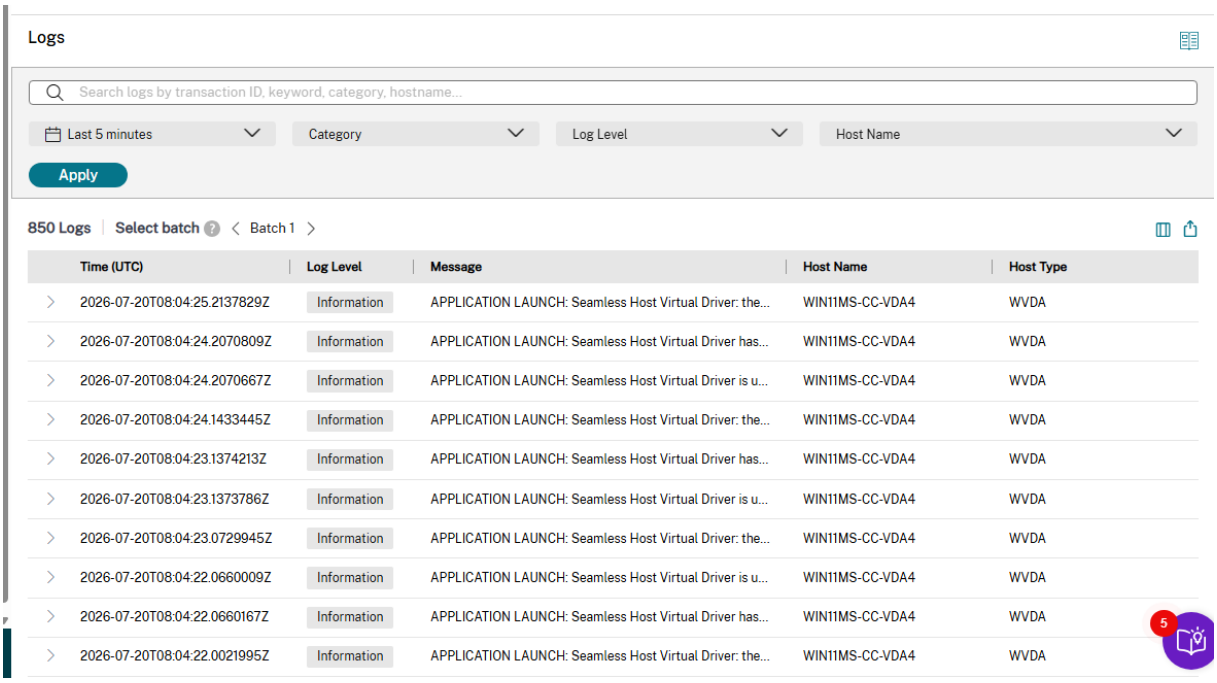
Log Level	When to use it
Information	Standard component events —session started, VDA registered, license checked out. Use to see the full lifecycle sequence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Level	When to use it
Warning	Non-critical issues that may indicate a problem —session disconnects, idle timeouts, heartbeat warnings. Start here for disconnect scenarios.
Error	Failures requiring investigation —launch errors, registration failures, license exhaustion. Start here for most scenarios.
Critical	Severe failures affecting service —typically component crashes or unrecoverable states.

Log table —columns

The log table shows five columns by default for each entry. New columns can be added by clicking the Column button. Click the **>** expand arrow on any row to see the full log message and additional fields.



Column	What it shows
Time (UTC)	Timestamp of the event in UTC, with millisecond precision. Sort ascending to read a sequence of events in the order they occurred.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Column	What it shows
Log Level	Severity badge: Information, Warning, Error, or Critical
Message	The log message from the component. Truncated in the table —click the **>** expand arrow on the row to read the full message. The full message is the primary diagnostic text.
Host Name	The machine that generated the log entry
Host Type	The component type: DDC, StoreFront, WVDA (Windows VDA), CWAWindows, and others depending on what is registered with the Log Server

Exporting logs for Citrix Technical Support

The export icon appears at the top right of the Logs section. Use it to download the current filtered log view as a file. Before exporting:

> **Note:**
>
> **Version availability:** The export icon is available on DaaS from the Cloud 129 (April–May 2026) release and later, and on Citrix Virtual Apps and Desktops from CVAD 2603 and later. The option is not available on earlier versions.
>
> **Note:**
>
> **AuthKey required:** The Logs node only shows data if the AuthKey is configured in Director or Monitor settings. The AuthKey is generated during Log Server setup. Without it, the Logs node shows no entries.

Scenario 1: Session launch failure

A user clicks a published desktop or application and gets a launch error. The session never opens. The error may appear on the Citrix Workspace App screen or the progress bar stalls and times out with no session connecting.

In the Logs node, set **Category** to **Application Launch**, **Log Level** to **Error**, and adjust **Time** to cover the failure window. Click **Apply**. Sort by **Time (UTC)** ascending and read the **Message** and **Host Type** columns together —they show which component in the launch path failed and what it reported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The log messages below are illustrative examples. Actual messages in your environment follow the same format and column structure but may differ in exact wording.

Example: No VDA available in the delivery group

The DDC received the launch request but could not assign a desktop. All VDAs in the delivery group were unregistered or at session capacity.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:14:22.1034Z	Information	APPLICATION LAUNCH: User DOMAIN\jsmith requested Desktop from delivery group 'Windows 11 VDAs'	DDC-01	DDC
2026-07-20T09:14:22.3841Z	Error	APPLICATION LAUNCH: No suitable desktop found —all VDAs in delivery group 'Windows 11 VDAs'are unregistered or at session capacity	DDC-01	DDC
2026-07-20T09:14:22.4102Z	Error	APPLICATION LAUNCH: Launch failed for user DOMAIN\jsmith —no resources available	STF-01	StoreFront

The Error from DDC tells you the broker could not find an available VDA. Check VDA registration in Web Studio → Search Machines. See Scenario 2 for VDA registration troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: VDA assigned but session initialization failed

The DDC assigned a VDA but the VDA could not start the session. Common causes: FSLogix or roaming profile container failure, Group Policy processing error, or VDA resource exhaustion.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:22:11.0234Z	Information	APPLICATION LAUNCH: VDA WIN11MS-CC-VDA4 selected for user DOMAIN\jsmith	DDC-01	DDC
2026-07-20T09:22:11.8820Z	Error	APPLICATION LAUNCH: Session initialization failed for user DOMAIN\jsmith —FSLogix profile container could not be mounted at \file-server\profiles\jsmith.vhdx	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:22:12.0011Z	Error	APPLICATION LAUNCH: Launch request failed — VDA WIN11MS-CC-VDA4 reported session preparation error for user DOMAIN\jsmith	DDC-01	DDC

The Error from Host Type WVDA identifies the VDA as the failure point and the Message shows the exact cause. Click the **>** expand arrow on that row to read the full message, which includes the full profile container path and error code.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: Virtual channel error during CWA post-launch

The session was created on the VDA side but the CWA client could not establish the ICA virtual channel connection. Filter **Host Name** to the CWA machine to see client-side errors.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:31:04.5521Z	Information	APPLICATION LAUNCH: Seamless Host Virtual Driver has been initialized successfully	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:31:05.1204Z	Error	CWA-POSTLAUNCH::VIRTUAL CHANNEL: Failed to load virtual driver —channel negotiation timeout. Check firewall rules for ports 1494 and 2598.	Win22-CC-01	CWAWindows

Host Type CWAWindows with a CWA-POSTLAUNCH error means the VDA was ready but the ICA data path between client and VDA was blocked. Verify ports 1494 and 2598 are open from the client machine to the VDA.

Scenario 2: VDA registration failure

VDAs show as **Unregistered** in Director or Web Studio → Search Machines. Users see "No desktops are available to you at this time."Published desktops appear greyed out in StoreFront or Citrix Workspace.

In the Logs node, set **Category** to **VDA registration**, **Log Level** to **Error**, and set **Host Name** to both the affected VDA and the DDC. Click **Apply**. Reading both sides of the registration handshake together —the VDA row and the DDC row at the same timestamp —shows exactly where the failure occurred.

> **Note:**
>
> The log messages below are illustrative examples. Actual messages in your environment follow

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> the same format and column structure but may differ in exact wording.

Example: VDA cannot reach the Delivery Controller

The VDA is attempting to register but the DDC never receives the request. Only VDA-side errors appear —no matching DDC rows at the same timestamps.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T08:30:11.2341Z	Error	REGISTRATION: Failed to contact Delivery Controller DDC-01.domain.com on port 443 — connection timed out	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:41.2341Z	Error	REGISTRATION: Failed to contact Delivery Controller DDC-01.domain.com on port 443 — connection timed out	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:31:11.2341Z	Error	REGISTRATION: Failed to contact Delivery Controller DDC-01.domain.com on port 443 — connection timed out	WIN11MS-CC-VDA4	WVDA

The same error repeating at a fixed interval is a retry loop —the VDA is alive but blocked. Verify ports 80 and 443 are open from the VDA to the DDC, and check the `ListOfDDCs` registry key on the VDA for stale or incorrect DDC addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: DDC rejects the registration request

The VDA reached the DDC but the DDC refused to register it. Both VDA and DDC rows appear —read the DDC Message for the rejection reason.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T08:30:11.2341Z	Information	REGISTRATION: VDA WIN11MS-CC-VDA4 attempting to register with DDC-01.domain.com	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:11.8820Z	Error	REGISTRATION: Registration rejected — machine account WIN11MS-CC-VDA4$ is disabled or not found in Active Directory	DDC-01	DDC

The Error row comes from Host Type DDC —the DDC is the failure point, not the VDA. Click the **>** expand arrow on the DDC row to read the full rejection reason. Common reasons: disabled machine account in Active Directory, VDA/DDC version mismatch, or license pool exhaustion.

Example: VDA registers then immediately deregisters

Registration succeeds but the DDC initiates deregistration within seconds. This repeats in a loop. A power management drain policy is shutting the VDA down before it can accept sessions.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:01:33.1240Z	Information	REGISTRATION: VDA WIN11MS-CC-VDA4 registered successfully with DDC-01.domain.com	WIN11MS-CC-VDA4	WVDA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Time (UTC)	Log Level	Message	Host Name	Host Type
2026-07-20T09:01:47.4421Z	Error	POWER MANAGEMENT: PowerManagementDrain initiated — machine scheduled for shutdown by delivery group power policy	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:01:47.6830Z	Error	REGISTRATION: VDA WIN11MS-CC-VDA4 deregistered — reason: power management drain	DDC-01	DDC

The 14-second gap between registration and deregistration is the tell. Check Web Studio → Delivery Group → Power Management for a drain or shutdown schedule that is applying during business hours.

> **Warning:**
>
> The scenarios in this article are examples of how to search and investigate logs in Citrix Director or Monitor. The same methodology applies to any Citrix-related issue you encounter —session failures, authentication errors, connectivity problems, VDA instability, or any other component-level issue. Set the right **Category**, **Log Level**, and **Host Name** filters, read the log sequence in **Time (UTC)** order, and expand individual rows to read the full **Message**. The component that logged the first error and what the Message says will point you to the root cause —regardless of the scenario.
>
> **Tip:**
>
> **DaaS customers with Citrix Aidrien access:** Copy the error message from the AOT log and paste it directly into Citrix Aidrien. Aidrien will explain the error and provide recommended troubleshooting steps. This may not resolve every issue on its own, but it will narrow down the root cause and in many cases guide you to a fix —before you need to contact Citrix Technical Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Escalating to Citrix Technical Support

If self-service investigation does not resolve the issue, include the following when opening a support ticket:

- **Exported log file covering the failure window** —use the export icon. You can export in two ways:
  - **Targeted export** —apply Time, Category, and Host Name filters, then export. This gives Support a focused log set scoped to the failure.
  - **Broad export** —apply only the Time filter and export without any other filters. This gives Support the full log picture for the failure window and is useful when the scope is unclear.

  When the file downloads, the filename is prefixed with **AOT**. Do not remove or rename this prefix. You can edit the portion of the filename that follows —but always retain **AOT** at the beginning.
- The failure pattern identified from the sections above
- CVAD version, component versions (VDA, DDC, StoreFront), and Log Server version
- The transaction ID or session ID of the failed event —searchable in the Logs node search bar

Because AOT captures logs continuously and every entry includes Host Name, Host Type, and timestamp, Citrix Technical Support can begin analysis immediately without asking you to reproduce the issue or collect new traces.

Frequently Asked Questions

August 27, 2026

1. How can I check the running log server configurations, like MAX_RESERVE_DAYS?

You can check the container environment values using either of the following commands:

```
docker inspect logserver |findstr MAX_RESERVE_DAYS
```

Or by checking the container environment:

```
docker exec -it logserver env |grep MAX_RESERVE_DAYS
```

If nothing is returned, it means the log server is using the default value: `MAX_RESERVE_DAYS=7`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Do I need to purchase Docker Desktop licenses when installing the log server container image on Windows?

Yes. A valid Docker Desktop license is required.

3. Should I use a new server for log server installation?

Yes. It is recommended to use a dedicated server for the log server installation to ensure performance and isolation.

4. What is the sustained ingest capacity of a single AOT Log Server? What are the maximum and safe Events-Per-Second (EPS) limits?

A single AOT Log Server supports a sustained ingest capacity of 10,000 events per second (EPS). This value represents both the maximum and the safe operating threshold for continuous ingestion.

5. How many components can a single AOT Log Server handle? Is there a maximum limit?

A single Log Server can connect up to 128,000 components, but it can only process about 10,000 logs per second. So the number of machines is rarely the issue —the real sizing factor is how many logs your users generate during peak activity.

6. What is the burst tolerance of the AOT Log Server? How much sudden log spike can it handle without loss or backlog breach?

The AOT Log Server can handle short-term bursts of up to 2× the normal event rate without losing logs. If log volume spikes beyond this (for example, 5×), the system will not be able to persist events reliably, and OpenSearch will start dropping logs because it cannot index them fast enough.

7. Can the AOT Log Server compress logs? What compression ratio should we expect?

Yes. The AOT Log Server uses the default LZ4 compression algorithm for storing logs in OpenSearch. The typical compression ratio is approximately 2:1, meaning log data is reduced to less than half its original size while maintaining fast read/write performance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. For each infrastructure type (single-site on-prem, multi-site on-prem, single-region cloud, multi-region cloud, hybrid, MSP/tenant), where should the AOT Log Server be deployed and why?

The AOT Log Server should always be deployed in the same line of sight as the VDAs. This ensures stable connectivity and helps maintain low latency between the components generating logs and the log server that ingests them. As long as every component (VDAs, DDCs, StoreFront™, Gateway, etc.) can reliably reach the log server, the environment will function correctly.

9. Do we need one log server per region, or can everything be centralized? What about latency and egress?

You can centralize the log server, but customers should evaluate the latency and egress cost implications for their environment. The latency between regions may affect log ingestion, especially during high-volume periods. If the round-trip latency is high, spikes or bursts of logs may cause delays, backlog build-up, or potential loss during peak loads. Egress charges may apply when logs cross regional or cloud boundaries.

10. Does AOT consume significant network bandwidth or system resources?

No. AOT is designed to have minimal impact on endpoint, VDA or any component, and network performance.

AOT collects logs continuously and uploads them to the AOT Log Server in near real-time over HTTPS. Individual log records are typically very small in size (often only a few kilobytes), which helps minimize network overhead during normal operation.

The overall bandwidth consumed depends on the number of active sessions, enabled components, and environment activity. In most deployments, AOT log traffic represents a very small percentage of overall network utilization.

AOT also uses compression to reduce storage requirements and optimize data transfer to the Log Server.

11. What are the minimum hardware specifications for supporting 1,000 machines with the AOT Log Server?

For environments with up to 1,000 machines, you need: 1 node (Log Server + OpenSearch combined), 4 vCPUs, 8 GB RAM, 2,000 IOPS minimum (SSD or NVMe recommended), 1 Gbps NIC. This setup is suitable for small or single-site deployments with moderate log volume.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. How can I troubleshoot if there is a problem with the Log Server?

LogServer is running as a docker container, so all docker commands could be used to find the issues:

```
docker logs logserver
docker inspect logserver
```

And also, user could attach into the running container and view logs of logserver self:

```
docker exec -it logserver bash
```

In the logserver docker container bash shell, user can verify the health of logserver and opensearch:

```
curl http://localhost:5000/Ping
curl http://localhost:9200/_cluster/health?pretty
```

And check logs inside the container:

```
tail Config/applogs.txt
tail Config/weblogs.txt
```

If need more logs, user could modify the `LOG_LEVEL=0` in `StartLogServer.sh`/`StartLogServer.bat` and restart the logserver by these script files. Then the detailed logs will include TRACE, DEBUG, INFO, WARN, ERROR all levels.

13. Recover from an improperly detached Log Server storage disk

If you remove or detach the Log Server storage disk directly from the hypervisor or cloud provider without first detaching it from the Citrix Connector Appliance administration UI, the Connector Appliance retains the storage configuration and assumes that the disk is still attached. As a result, the previously attached disk remains configured in the Connector Appliance, attaching a new disk fails, and you may see an error similar to: *A local disk is already mounted to the provider.*

Option 1 (Recommended): If the original disk is still available:

- Reattach the original disk to the Connector Appliance VM from the hypervisor or cloud provider.
- Reboot the Connector Appliance.
- After the appliance starts successfully, detach the disk using the Connector Appliance administration UI.
- You can now attach a new disk if required.

Option 2: If the original disk is no longer available, manually remove the stale storage configuration by executing the following API request. Retrieve an Authorization token and run the appropriate command:

Linux:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
curl -X POST "https://<connector-fqdn>/storage/$detach" \
-H "Content-Type: application/json" \
-H "Authorization: Bearer <token>" \
-d '{
 "targetProvider":"logserver-provider","storageType":"local" }
 '
```

Windows:

```
curl -X POST "https://<connector-fqdn>/storage/$detach" ^
-H "Content-Type: application/json" ^
-H "Authorization: Bearer <token>" ^
-d "{
 \"targetProvider\":\"logserver-provider\",\"storageType\":\"local\" }
 "
```

> **Note:**
>
> The API may return an error even though the stale storage configuration is successfully removed. Verify the storage configuration before retrying the disk attachment.

As a best practice, always detach the Log Server storage disk from the Connector Appliance administration UI before removing or detaching the disk from the hypervisor or cloud provider. This ensures that the Connector Appliance cleans up its storage configuration and prevents stale storage references.

Fixed Issues

August 12, 2026

Issue	ID	Status	Summary
OpenSearch 429 Too Many Requests under load	XASUP-8128	Fixed in 2603	Heap memory defaults were too low for large deployments.
Director/Monitor unable to access Log Server remotely	XASUP-7776	Fixed in 2603	HTTPS mode now sets `LOCAL_DOWN_ONLY=false` automatically.
Port conflict prevents Log Server from binding	XASUP-7658	Fixed in 2603	Port availability validation added to installer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Issue	ID	Status	Summary
AuthKey cleared silently when Log Server address edited	STUD-40505	Fixed in Web Studio 73 / CVAD 2603	Editing address/port without re-entering AuthKey caused silent data loss.

Known Issues and Limitations

August 18, 2026

Only One Log Server Is Supported Per Environment

The current architecture supports only a single AOT Log Server per environment, and both Web Studio and Director/Monitor are designed to work with only one Log Server configuration. All components must point to this same Log Server; configuring or distributing workloads across multiple Log Servers is not supported today. This single Log Server can handle up to 128,000 active component connections and process up to 10,000 log events per second, which is sufficient for most deployments. Since these limits are based on connection capacity and log-throughput, not on the number of components, even very large environments can operate with one Log Server as long as they remain within throughput thresholds.

However, customers with extremely high log volumes during peak activity may reach ingestion or indexing limits due to the absence of horizontal scaling. Support for multiple Log Servers and broader scaling options will be introduced in future releases as part of the evolving architecture.

Running the AOT Log Server on a Windows VM hosted on XenServer® is not supported

XenServer does not support nested virtualization, which prevents Docker from running inside the guest VM. As a result, the Log Server container cannot be deployed in this configuration.

Docker Desktop on Windows requires an active user session for AOT Log Server

When the AOT Log Server is deployed on a Windows VM using Docker Desktop, the container runs within the context of the user session that started Docker Desktop. Docker Desktop is designed as a user-session-based application and does not run as a system-level service on Windows. As a result, if

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the user logs out, Docker Desktop stops, which causes the AOT Log Server container to stop. Because of this behaviour:

- The AOT Log Server stops when the user logs out as the deployment depends on a specific user session.
- Other administrators cannot access or manage the running containers.

Workaround: Keep the user session active or in a disconnected state (do not log out) to ensure that Docker Desktop and the AOT Log Server container continue running.

Recommendation: For production deployments, use one of the following:

- Deploy the AOT Log Server on a Linux VM using Docker Engine
- Use the Citrix Connector Appliance (CCA)-based deployment where supported

These options allow the Log Server to run independently of user sessions and provide a more reliable, always-on deployment model.

> **Note:**
>
> - This approach may not be reliable in environments with session timeouts or strict security policies.
> - This behaviour is a known limitation of Docker Desktop on Windows and is not specific to the AOT Log Server.

License Server logs appear with incorrect Host Type in Director/Monitor

When viewing AOT logs from the License Server in Director, the Host Type column may incorrectly display the value as DDC instead of License Server, even though the hostname is correct.

This issue is limited to how the Host Type is represented in Director and does not impact log collection or functionality. This issue has been resolved in the latest License Server release and is fixed starting from License Server version: 55000 or later.

Citrix Cloud Connector is required to view AOT logs in Monitor

Customers using Citrix Monitor to view AOT logs must have at least one Citrix Cloud Connector deployed in their environment. This requirement applies regardless of where the AOT Log Server is hosted, including Linux VM or Windows VM or Citrix Connector Appliance.

Citrix Monitor relies on the Monitor service running on the Cloud Connector to retrieve logs from the configured Log Server and display them in the UI.

Without a Windows Cloud Connector, AOT logs cannot be fetched or displayed in Monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ADC Gateway logs display incorrectly in Citrix Director

Symptoms: When viewing Always On Tracing (AOT) logs for Citrix ADC Gateway in Citrix Director, you might observe:

- Log Level displayed as Error instead of Debug or Info.
- The Message column shows the entire raw log entry.
- The displayed timestamp differs from the original event timestamp.
- Only malformed JSON log records are affected. Valid log records display correctly.

Affected versions: Citrix ADC earlier than 14.1-73.x and Citrix ADC earlier than 15.1-8.x.

Cause: Citrix ADC Gateway uploads malformed JSON log records that cannot be parsed by the AOT Log Server. As a result, the Log Server stores the raw log entry and classifies it as an error.

Resolution: Upgrade Citrix ADC to one of the following versions or later:

- 14.1-73.x
- 15.1-8.x

Fixed in: Citrix ADC 14.1-73.x and Citrix ADC 15.1-8.x.

FIPS-compliant deployments are not supported

The AOT Log Server does not currently support FIPS-compliant deployments. Customers with mandatory FIPS requirements should defer production deployment until FIPS support becomes available.

Customers who do not require FIPS compliance may continue to deploy and evaluate the AOT Log Server in supported environments.

CWA logs not forwarded to AOT Log Server when using Citrix Gateway with StoreFront™ 2603

When Citrix Gateway is used with StoreFront 2603, Citrix Workspace app (CWA) logs are not forwarded to the AOT Log Server. As a result, CWA logs are unavailable for troubleshooting in deployments that use this configuration.

This issue affects only deployments that use Citrix Gateway with StoreFront 2603. Other AOT log sources, such as Virtual Delivery Agents (VDAs), continue to upload logs successfully.

Workaround

Use one of the following StoreFront versions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StoreFront 2507 CU1
- StoreFront 2511

These versions correctly support forwarding CWA logs to the AOT Log Server when deployed with Citrix Gateway.

> **Note:**
>
> This issue does not affect deployments where users connect directly to StoreFront without Citrix Gateway.

Third Party Notice

August 12, 2026

This release of Citrix AOT Log Server may include third-party software licensed under the terms defined in the following documents:

Citrix Centralized Log Server Third Party Notices

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.