Addons and Tools

Contents

uberAgent® Config & Support Tool

April 22, 2026

The uberAgent Config & Support Tool helps with setting up uberAgent for a proof of concept installation and creating uberAgent support bundles.

Features

- Quick and easy configuration of a uberAgent installation
- Creation of central config file management archive files
- One-click creation of uberAgent support bundles

Quick Links

- Changelog and Release Notes
- Quickstart Guide

Getting Started

To get started with the uberAgent Config & Support Tool, follow the steps outlined in the Quickstart Guide .

Related Tools

- uberAgent Event Generator for Splunk
- uberAgent Helpdesk Splunk App
- uberAgent Log Collector Splunk App

For a complete list of uberAgent addons and tools, visit our Addons and Tools page.

Changelog and Release Notes

April 22, 2026

Windows

Version 1.1.1

- Added capability to handle Citrix LAS tokens
- Enhanced support bundle to include service configuration and state diagnostics
- Decoupled bundle generation from agent installation status.

Version 1.1.0

- Added Advanced Configuration Workflow

Version 1.0.1

- Resolved an issue causing a crash during startup on Windows 10 version 1607 and Windows Server 2016.

Version 1.0.0

- Initial Release

macOS

Version 1.1.1

- Added Advanced Configuration Workflow
- Fixed race condition rendering user controls invisible

Version 1.0.3

- Added capability to handle Citrix LAS tokens

Version 1.0.1

- Initial Release

uberAgent® Config & Support Tool - 1.0.x

April 22, 2026

The **uberAgent Config & Support Tool** simplifies the configuration process for **uberAgent**, allowing you to set up a proof-of-concept installation with minimal effort.

> **Note**
>
> For Windows there is a new version 1.1.x available. You can find the documentation for that version at Quickstart 1.1.x.

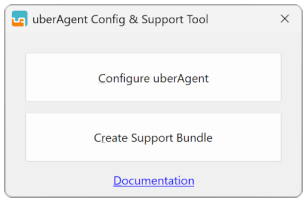
System Requirements

- Windows 10 version 1607 or later
- Windows Server 2016 or later
- macOS Ventura or newer

Download and Installation

1. Install uberAgent before proceeding.
2. Download the *uberAgent Config & Support Tool* from the Citrix Observability website.
3. Once the download has finished, launch the tool.

Creating a Support Bundle

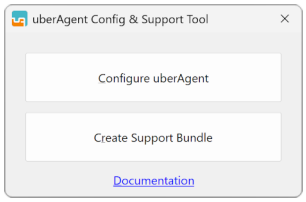


To generate an **uberAgent support bundle**, select the **"Create Support Bundle"** button. Upon completion, you'll receive a notification, and the bundle will be saved to your desktop.

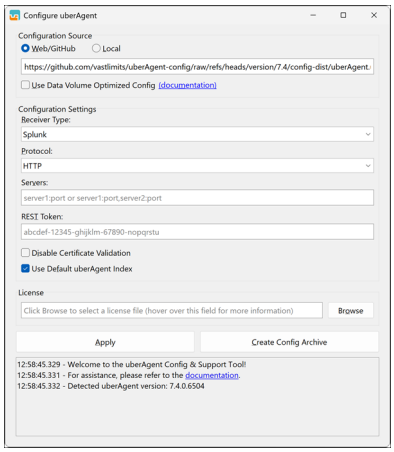
Configuring uberAgent

The **Configuration Dialog** can be used to configure a local uberAgent installation or to create configuration archives that can be used for Central Config File Management (CCFM).

1. Open the Configuration Dialog



Click on the **"Configure uberAgent"** button in the main window to open the configuration dialog.



2. Select the Configuration Source

- **Web/GitHub**: the tool downloads the configuration templates from the specified URL.
  - By default, it downloads the corresponding version from the uberAgent config GitHub repository.
- **Local**: Uses a template archive from the local disk.
  - When using **Local**, click **Browse** to locate and select a configuration archive.

3. (Optional) Enable Data Volume Optimization

The **"Use Data Volume Optimized Config"** option activates an optimized configuration designed to minimize data transmission volume. This is especially beneficial when reducing costs is a priority.

However, this optimization comes with a trade-off: instead of sending data for all processes, only the top five processes per category are transmitted. Additionally, data collection intervals are extended, leading to greater smoothing of peaks, making them less visible.

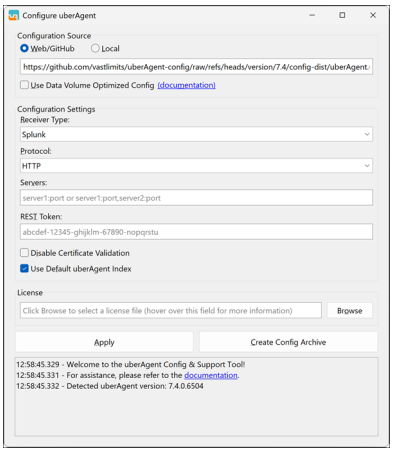
For more information, see Reducing the Data Volume.

4. Select a Receiver Type

The **Receiver Type** specifies the backend to which uberAgent sends the collected data. The available options are:

- **Splunk**
- **Elasticsearch**
- **OMS Log Analytics**
- **Kafka**
- **Azure Event Hubs**

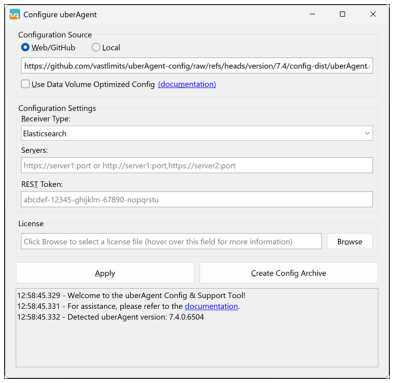
Configuration for each Receiver Type



Splunk

- **Protocol**: Choose either HTTP or TCP.
- **Servers**: Specify the Splunk server address (e.g., `https://server1:port` for HTTP, or `server1:port` for TCP).
- **REST Token**: Enter the Splunk HTTP Event Collector (HEC) token (required for HTTP).
- **Disable Certificate Validation**: Enable this option if you are using a Splunk Cloud trial instance, as the HEC certificate will likely not be trusted on your machines (**not recommended for production use**).
- **Use Default uberAgent Index**: If you want to use a different Splunk index than the default, uncheck this option.

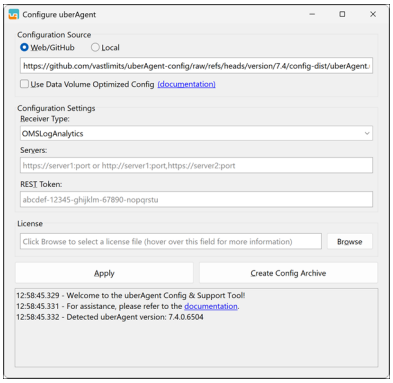
For more details, see Configuring Splunk's HTTP Event Collector.



Elasticsearch

- **Servers**: Enter the Elasticsearch endpoint (e.g., `https://server1:port`).
- **REST Token**: Provide the authentication token in the format `username:password`.

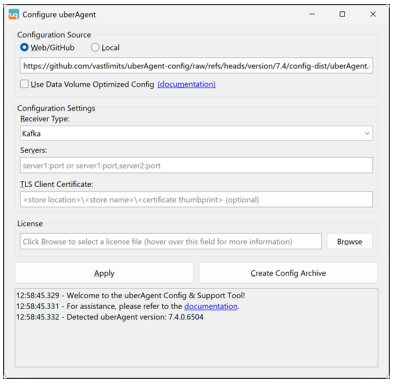
For more details, see Installing and Configuring Elasticsearch & Kibana.



Azure Monitor (OMS Log Analytics)

- **Servers**: Enter the Log Analytics workspace endpoint.
- **REST Token**: Provide the workspace key for authentication.

For more details, see Configuring Microsoft Azure Monitor.

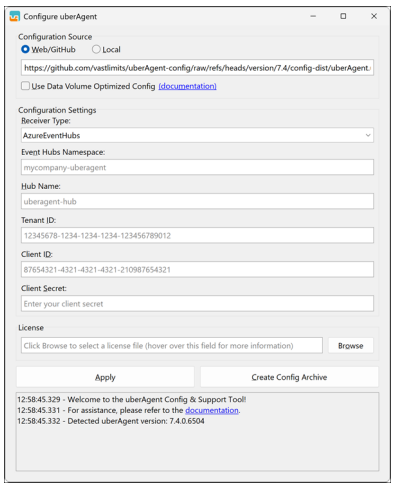


Kafka

- **Servers**: Enter the Kafka broker addresses (e.g., `https://server1:port`).

- **TLS Client Certificate**: Specify the certificate path in the format `<store location>\<store name>\<thumbprint>`.

For more details, see Configuring Apache Kafka & Confluent REST Proxy.



Azure Event Hubs

- **Event Hubs Namespace**: Enter the namespace.
- **Hub Name**: Specify the hub name.
- **Tenant ID**: Enter the Azure **Tenant ID**.
- **Client ID**: Provide the **Client ID** for authentication.
- **Client Secret**: Enter the authentication secret.

For more details, see Configuring Microsoft Azure Data Explorer (ADX) & Azure Event Hubs.

5. (Optional) Select License File

When a license file is selected, the tool automatically copies it to the uberAgent installation directory. This ensures that the service can start immediately after applying the configuration.

If you only plan to create a configuration archive for Central Config File Management (CCFM), it is not necessary to specify a license file. The generated archive does not include a license. The target machines must have a valid license file in their uberAgent installation directory for the service to work.

6. Apply and Save the Configuration

Once the configuration has been defined, you have two options for applying or saving it:

Apply the Configuration Selecting **Apply** immediately applies the configuration to the locally installed uberAgent installation.

- If a valid license file is already present in the installation directory or has been specified within the tool's UI, the tool will also automatically start the uberAgent service.
- If no valid license file is found or specified, the service will not start. In this case, you must manually copy a valid license file to the uberAgent installation directory before the service can be started.

Create Config Archive Selecting **Create Config Archive** generates a configuration archive without applying it to the local system. This is especially useful for Central Config File Management (CCFM) deployments, where configurations are distributed to multiple machines.

No license file is required when creating the archive. However, for uberAgent to function on the target machines, a valid license file must be present in the installation directory of each system where it is deployed.

For more details, see Central Config File Management (CCFM).

uberAgent® Config & Support Tool - 1.1.x

April 22, 2026

The **uberAgent Config & Support Tool** simplifies the configuration process for **uberAgent**, allowing you to set up a proof-of-concept installation with minimal effort.

System Requirements

- Windows 10 version 1607 or later
- Windows Server 2016 or later
- macOS 14.0 (Sonoma) or later

Download and Installation

Starting with uberAgent 7.5, the **uberAgent Config & Support Tool** is included as part of the uberAgent installer and is installed into the uberAgent installation directory.

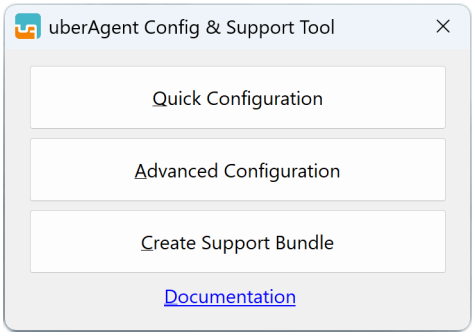
1. Install uberAgent 7.5 or later.
2. During the visual setup process, you can launch the Config & Support Tool directly from the final step of the installer.
3. Alternatively, you can launch the tool manually from the uberAgent installation directory after installation is complete.

Standalone Version

Alternatively, you can use the standalone version:

1. Download the *uberAgent Config & Support Tool* from the Citrix Observability website.
2. Once the download has finished, launch the tool.

Main Dialog Options



The tool provides three options:

- **Quick Configuration**: Streamlined configuration process for basic uberAgent setup - perfect for proof-of-concept installations.
- **Advanced Configuration**: Extended configuration options with maximum flexibility.
- **Create Support Bundle**: Collects log files and settings for troubleshooting.

Quick Configuration

The Quick Configuration option provides a streamlined approach to configuring uberAgent with pre-defined templates and simplified settings. This option maintains the same functionality as described in the Quickstart 1.0.x documentation, including:

- Configuration source selection (Web/GitHub or Local)
- Data volume optimization options
- Receiver type configuration (Splunk, Elasticsearch, OMS Log Analytics, Kafka, Azure Event Hubs)
- License file selection
- Apply configuration or create config archive options

For detailed instructions on using Quick Configuration, refer to the Quickstart 1.0.x documentation.

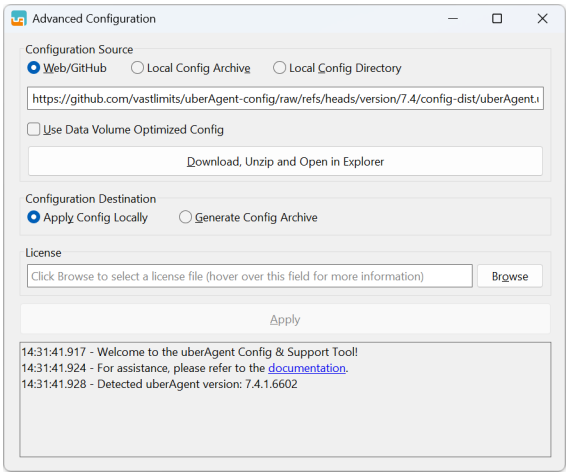
Advanced Configuration

The Advanced Configuration option provides enhanced flexibility for managing uberAgent configurations with extended configuration source options.

> **Note**
>
> If uberAgent is not installed, the configuration cannot be applied locally.

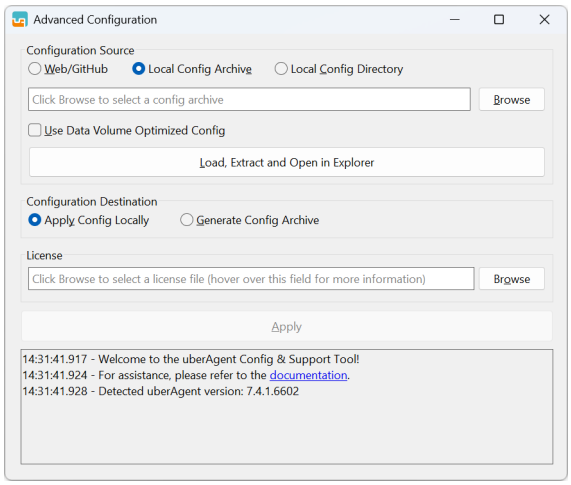
Supported Configuration Sources

The Advanced Configuration supports three configuration sources:



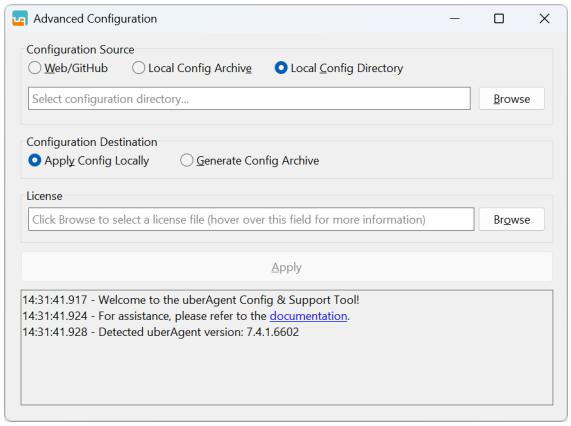
Web/GitHub

Downloads configuration templates from specified URLs, typically from the uberAgent config GitHub repository.



Local Config Archive

Uses a configuration archive from the local disk. This is particularly helpful for configuring machines without internet access or for editing existing configuration archives and repackaging them.



Local Config Directory

Works with a local configuration directory structure. This is particularly helpful for creating configuration archives for Central Config File Management.

> **Note**
>
> When using the uberAgent configuration directory (`C:\ProgramData\vast limits\uberAgent\Configuration`) as source, only creating a config archive is available.

Advanced Configuration Workflow

The workflow is identical for all Advanced Configuration options:

1. **Select Source**: Choose your configuration source (Web/GitHub, Local Config Archive, or Local Config Directory)
2. **Load Configuration**: If available, click the **Load** button to load the configuration files
3. **Edit Configuration**: The working directory with config files automatically opens in File Explorer. Make your changes using any text editor of your choice (e.g., Notepad, Notepad++, VSCode)
4. **Select Destination**: Choose whether to apply the configuration locally or create a config archive
5. **Apply Changes**: Click the **Apply** button to execute the selected process

Creating a Support Bundle

To generate an **uberAgent support bundle**, select the **"Create Support Bundle"** button from the main dialog. Upon completion, you'll receive a notification, and the bundle will be saved to your desktop.

uberAgent® Event Generator for Splunk

April 22, 2026

The uberAgent Event Generator is a powerful tool designed for product demonstrations of uberAgent. It simulates a large number of endpoints and generates data for all dashboards, allowing you to showcase the full capabilities of uberAgent without the need for a complex setup.

Features

- Simulates multiple endpoints
- Generates data for all uberAgent dashboards
- Perfect for product demonstrations and testing

Quick Links

- Changelog and Release Notes
- Quickstart Guide

Getting Started

To get started with the uberAgent Event Generator:

1. Download the Event Generator from the Citrix Observability website
2. Install the Event Generator on your Splunk instance
3. Access your uberAgent Splunk dashboards to see the simulated data

For more detailed instructions, please refer to our Quickstart Guide.

Related Tools

- uberAgent Config & Support Tool
- uberAgent Helpdesk Splunk App
- uberAgent Log Collector Splunk App

For a complete list of uberAgent addons and tools, visit our Addons and Tools page.

Changelog and Release Notes

April 22, 2026

Version 7.1

Release notes

- Increased .NET version to 7.
- Changed configuration file format to JSON.

Improvements

- Log messages are written to stdout and a log file located in the `%TEMP%` (Windows) or `/tmp` (Linux) directory.
- The fields `SessionFgBrowserType`, `SessionFgBrowserType` and `SessionFgBrowserActiveT` of sourcetype `uberAgent:Session:SessionDetail` are now available on macOS, too.

New Sourcetypes

- New sourcetype `uberAgentESA:System:SecurityInventory` with fields: `SecurityInventory` , `SecurityInventoryName`, `SecurityInventoryScore`, `SecurityInventoryRiskScore` , `SecurityInventoryResultData`, `SecurityInventoryErrorCode`, `SecurityInventoryEr` , `SecurityInventoryScope`, `SecurityInventoryScopeEntity`.

Updated Sourcetypes

- **Sourcetype [B287]:** `uberAgent:Process:ProcessStatistics` has new field(s): `ProcInputDelayMaxMs`, `ProcInputDelaySumMs` and `ProcInputDelayCount`.
- **Sourcetype [B287]:** `uberAgent:Session:SessionDetail` has new field(s): `SessionInputDelay` , `SessionInputDelaySumMs` and `SessionInputDelayCount`.
- **Sourcetype [B751]:** `uberAgent:OnOffTransition:BootDetail2` has new field(s): `UserLogonWaitDurationMs`.
- **Sourcetype [B766]:** `uberAgentESA:Process:DnsQuery` has new field(s): `DnsRisk52Chars` , `DnsRisk27UniqueChars`, `DnsRiskEmptyResponse`, `DnsRiskTXTRecord`, `DnsRiskHighEntropy`, `DnsResponseStatus`.

Version 7.0

Release notes

- macOS client machines are now supported.

Improvements

- Machines get their IP addresses once and they do not change.
- Machines get their disk volumes only once and they do not change during their lifetime.
- A random in-session process needs a long time to start.
- Application UI delay events can now only be generated by processes started during a session.
- WiFi data is now sent only for WiFi adapters.
- BSODs are now sent less frequently.

New Sourcetypes

- **Sourcetype:** new sourcetype `uberAgent:CitrixSession:VirtualChannelDetail` with fields: `SessionGUID`, `SessionUser`, `VirtualChannelVendorName`, `VirtualChannelData`, `VirtualChannelDataVolumeOutputMB`.
- **Sourcetype:** new sourcetype `uberAgent:CitrixSession:SessionConfig` with fields: `SessionGUID`, `SessionUser`, `AudioActualPriority`, `AudioPolicyAllowMicrophoneRedir`, `AudioPolicyAllowRedirection`, `AudioPolicyPriority`, `AudioPolicySoundQuality`, `CdmActualPriority`, `CdmVolumes`, `CdmPolicyAllowDriveRedirection`, `CdmPolicyPriority`, `CdmPolicyReadOnly`, `DisplayMode`, `ThinwireActualPriority`, `ThinwireColorDepth`, `ThinwireComponentEncoder`, `ThinwireHardwareEncodeInUse`, `ThinwireVideoCodecType`, `ThinwireColorspace`, `ThinwireVideoCodecUse`, `ThinwirePolicyFps`, `ThinwirePolicyPriority`, `ThinwirePolicyUseHardwareEncoding`, `ThinwirePolicyUseVideoCodec`, `ThinwirePolicyVisualQuality`, `FramehawkActualPri`, `FramehawkPolicyPriority`, `D3DActualPriority`, `D3DPolicyAeroRedirection`, `D3DPolicyGraphicsQuality`, `D3DPolicyPriority`, `GraphicsActualPriority`, `GraphicsPolicyDisplayDegradeNotifyUser`, `GraphicsPolicyDisplayDegradePolicy`, `GraphicsPolicyPriority`, `NetworkConnectedVia`, `NetworkEdtMtu`, `NetworkPolicyAcce`, `NetworkPolicyICAListenerPortNumber`, `NetworkPolicySessionReliabilityPort`, `NetworkPolicySessionReliabilityTimeout`, `PrinterActualPriority`, `PrinterSessionPrinter`, `PrinterPolicyAllowRedirection`, `PrinterPolicyAutoCreate`, `PrinterPolicyPriority`, `USBActualPriority`, `USBPolicyAllowPNPRedirection`, `USBPolicyAllowUSBSupport`, `USBPolicyPriority`.
- **Sourcetype:** new sourcetype `uberAgent:Process:ProcessStatistics` with fields: `ProcHandleCount`, `ProcThreadCount`, `ProcPriority`, `ProcPrivateMB`,

ProcVirtualSizeMB, ProcPageFaultsPS, ProcPageFileMB, ProcName, ProcID, ProcGUID, ProcUser and AppId.

- **Sourcetype:** new sourcetype uberAgent:System:PerformanceCounter with fields: PerformanceCounterObject, PerformanceCounterInstance, PerformanceCounterName, PerformanceCounterValue.

Updated Sourcetypes

- **Sourcetype:** uberAgent:Application:NetworkConnectFailure has new field(s): NetTargetSourcePort.
- **Sourcetype:** uberAgent:System:MachineInventory has new field(s): HwHypervisorVendor.
- **Sourcetype:** uberAgent:Session:SessionDetail has new field(s): SessionRoundTripTimeMs, SessionFps, SessionTransportProtocols.
- **Sourcetype:** uberAgent:Citrix:Applications has new field(s): CustomerId.
- **Sourcetype:** uberAgent:Citrix:Catalogs has new field(s): CustomerId.
- **Sourcetype:** uberAgent:Citrix:DesktopGroups has new field(s): CustomerId.
- **Sourcetype:** uberAgent:Citrix:Machines has new field(s): CustomerId.
- **Sourcetype:** uberAgent:Citrix:PublishedDesktops has new field(s): CustomerId.
- **Sourcetype:** replaced KV sourcetype uberAgent:PerformanceCounter:<TimerName> with CSV sourcetype uberAgent:System:PerformanceCounter.
- **Sourcetype:** uberAgent:Application:ApplicationUsage has been removed (it was marked as deprecated as of version 6.1.1).

Version 6.2.0

Updated Sourcetypes

- **Sourcetype:** uberAgent:Application:NetworkConnectFailure has new field(s): NetTargetSourcePort.
- **Sourcetype:** uberAgent:Process:NetworkTargetPerformance has new field(s): NetTargetSourcePort.

Version 6.1.1.4416

Improvements

- Improved number of sent events during session lifetime.

- Improved values in *Application Performance* dashboard.

Bugfixes

- Added chmod call to "StartEventgen.cmd".

Version 6.1.1

Improvements

- Added some more hardware models.
- Added `ModuleName` and `ExceptionCode` to the sourcetype `uberAgent:Application:Errors` (applications crashes).
- Generated outliers for Process DNS.

Updated Sourcetypes

- **Sourcetype:** `uberAgent:Process:ProcessStartup` has new field(s): `HashMD5`, `HashSHA1`, `HashSHA256`, `HashIMP`, `SignatureStatus`, `IsSignedByOSVendor`, `SignerName`.
- **Sourcetype:** `uberAgent:Process:ProcessStartup`: fields `ProcHash` and `HashType` have been removed.
- **Sourcetype:** `uberAgent:Process:ProcessStop` has new field(s): `HashMD5`, `HashSHA1`, `HashSHA256`, `HashIMP`.
- **Sourcetype:** `uberAgent:Process:ProcessStop`: fields `ProcHash` and `HashType` have been removed.
- **Sourcetype:** `uberAgent:Process:ProcessDetail` has new field(s): `SessionID`.
- **Sourcetype:** `uberAgent:CitrixADC:AppliancePerformance` has new field(s): `CpuFan0Speed`, `CpuFan1Speed`, `SystemFanSpeed`, `Cpu0Temp`, `Cpu2Temp`, `InternalTemp`, `PowerSupply1Status`, `PowerSupply2Status`, `PowerSupply3Status`, `PowerSupply4Statu`, `VoltageV33Main`, `ICAOnlySessions`, `ICAOnlyConnections`, `SmartAccessSessions`, `SmartAccessICAConnections`, `SSLSessions`.
- **Sourcetype:** `uberAgent:CitrixADC:Gateway` has new field(s): `HSTS`, `HSTSMaxAge`, `HSTSInclSubdom`, `TLS13`.
- **Sourcetype:** `uberAgent:CitrixADC:vServer` has new field(s): `HSTS`, `HSTSMaxAge`, `HSTSInclSubdom`, `TLS13`.
- **Sourcetype:** `uberAgent:System:NetworkConfigInformation` has new field(s): `NetworkConfigWiFiSignalQuality`, `NetworkConfigWiFiType`, `NetworkConfigWiFiAuthe`.

New Sourcetypes

- **Sourcetype**: new sourcetype `uberAgentESA:Process:DnsQuery` with fields: `ProcName`, `ProcGUID`, `DnsRequest`, `DnsResponse`, `DnsResponseType` and `DnsEventCount`.

Bugfixes

- SMB paths had only one backslash.

uberAgent® Helpdesk Splunk App

April 22, 2026

The uberAgent Helpdesk Splunk App is a specialized tool designed for IT professionals who support virtual or physical desktops and need to resolve issues quickly. This app provides a streamlined view of the existing uberAgent dataset, optimized for helpdesk use.

Features

- Simplified view of uberAgent data tailored for helpdesk professionals
- Quick access to key metrics and information for troubleshooting
- Intuitive interface for faster issue resolution
- Customized dashboards for common helpdesk scenarios

Quick Links

- Changelog and Release Notes
- Quickstart Guide

Getting Started

To get started with the uberAgent Helpdesk Splunk App:

1. Ensure you have uberAgent and Splunk installed and configured
2. Download the Helpdesk Splunk App from the Citrix downloads page
3. Install the app on your Splunk instance
4. Start using the specialized dashboards for efficient issue resolution

For more detailed instructions, please refer to our Quickstart Guide.

Related Tools

- uberAgent Config & Support Tool
- uberAgent Event Generator for Splunk
- uberAgent Log Collector Splunk App

For a complete list of uberAgent addons and tools, visit our Addons and Tools page.

Changelog and Release Notes

April 22, 2026

Version 1.5.0

Improvements

- **Dashboards:** session scores are now displayed after a session is selected and overall visibility is improved.

Bug fixes

- **Dashboards:** fixed wrong column name in *Machine details* panel.

Version 1.4.0

Improvements

- **Dashboards:** added user input delay metrics that were introduced in uberAgent 7.1.

Release notes

- **Dashboards:** replaced the chart *Disk latency (ms)* with *Input delay (ms)*.

Version 1.3.0

Improvements

- **Dashboards:** added Citrix metrics that were introduced in uberAgent 7.0.

- **Dashboards:** the WiFi signal quality chart is inserted into the *Network details* section dynamically. In older versions, it was always there, even for non-WiFi connections.
- **Dashboards:** all charts are now column charts for better visibility.

Bug fixes

- **Dashboards:** fixed wrong timeframe evaluation in the *Machine details* chart. It now loads much faster.

Release notes

- **Dashboards:** removed the chart *Session activity* in favor of session connection change annotations.

Version 1.2.3

Improvements

- **Splunk:** added `sc_admin` permissions to meet Splunk Cloud requirements.

Version 1.2.2

Improvements

- **Dashboards:** upgraded dashboards to version 1.1. This is a requirement for Splunk Cloud.requirements.

Version 1.2.1

Bug fixes

- **Dashboards:** rounded Wifi signal quality
- **Dashboards:** fixed timeframe issues for the machines and network details charts

Version 1.2.0

Improvements

- **Dashboards:** added WiFi metrics
- **Dashboards:** added network latency metric selector

Version 1.1

- Support for uberAgent 6.0.

Version 1.0

- Initial release

uberAgent® Helpdesk Splunk App

April 22, 2026

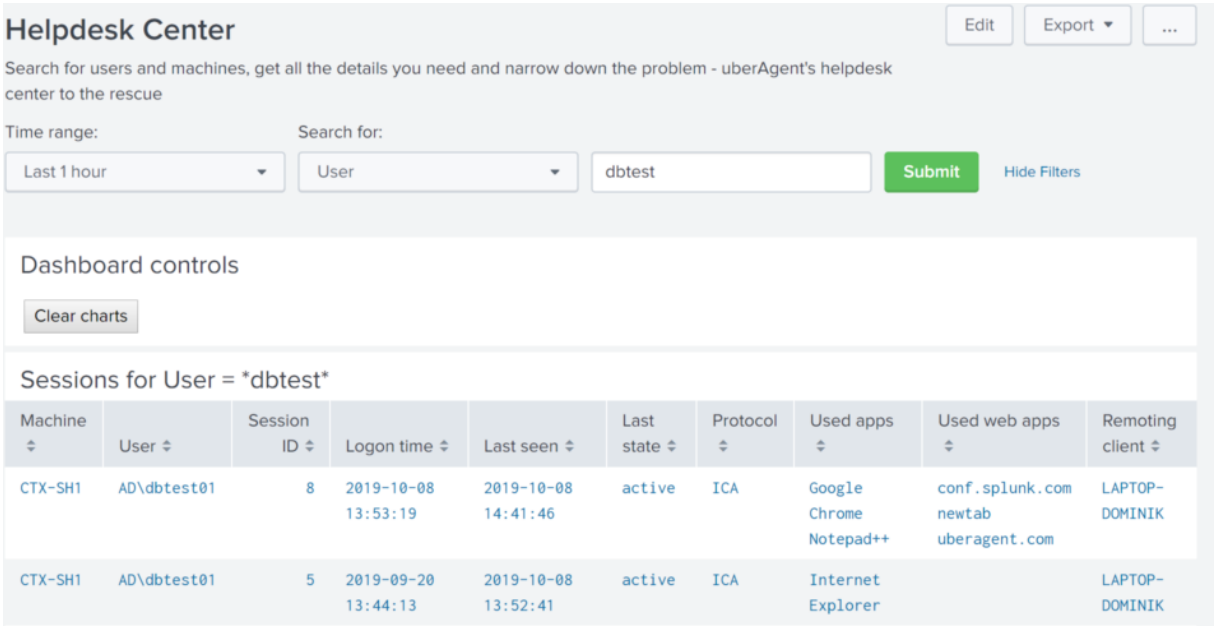
The uberAgent Helpdesk Splunk App is designed for helpdesk heroes who support virtual or physical desktops and who need quick answers to typical questions like the following:

- Why is my login so slow? It was fast yesterday.
- Why is my app constantly crashing?
- Citrix is slow!
- The website is not loading fast enough!

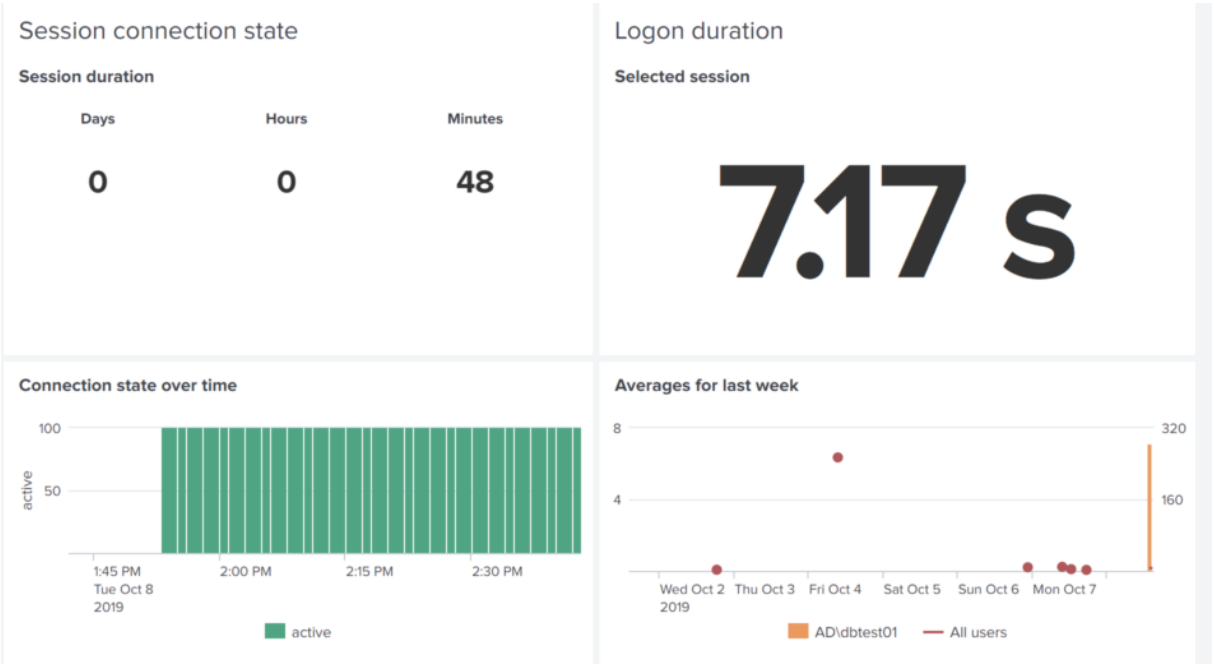
What Does the App Look Like

The app has just one dashboard, nice and easy. You start by searching either for a user or a machine. After selecting a session of interest detailed information will be provided.

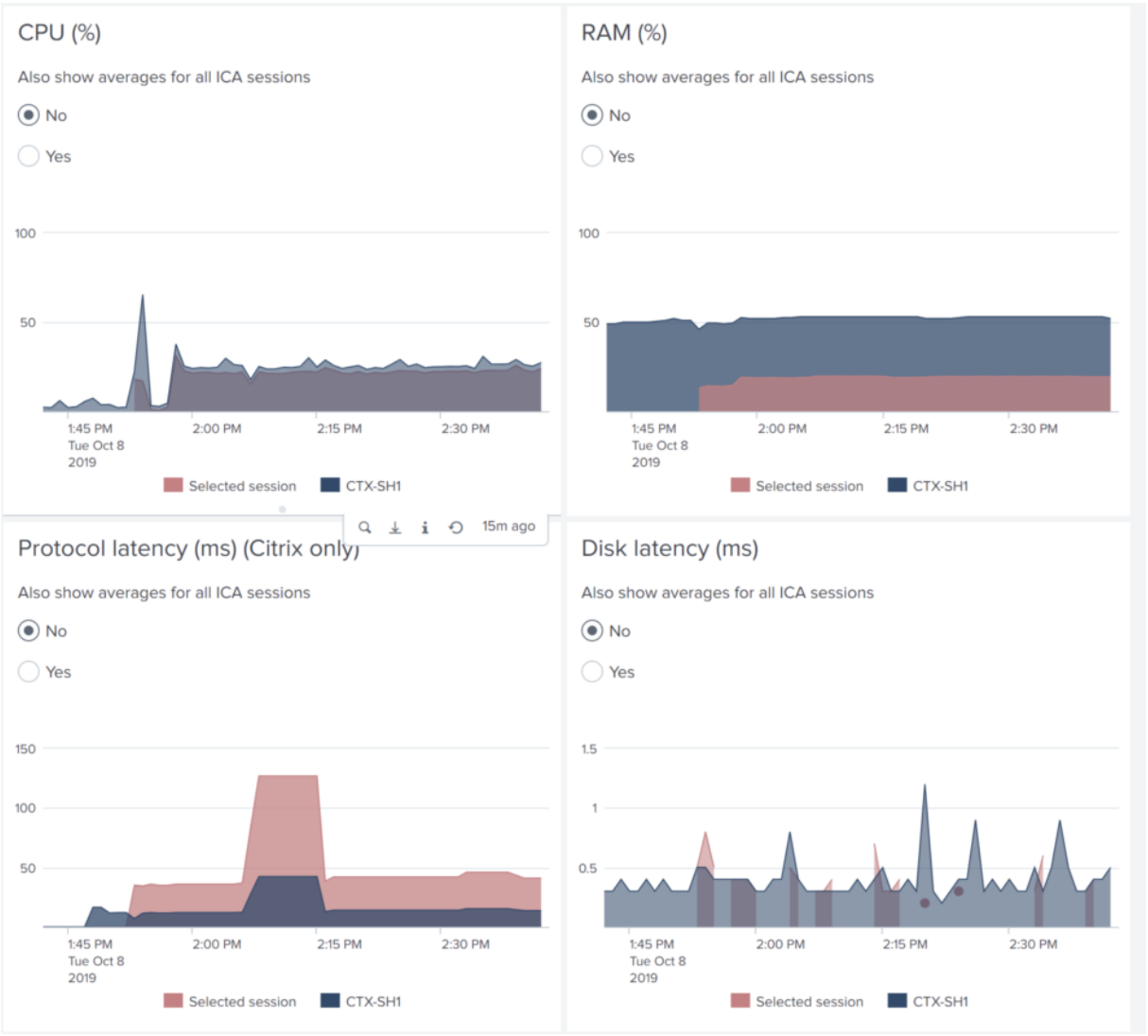
> Note: enter a * in the search field to see all user sessions or machines.



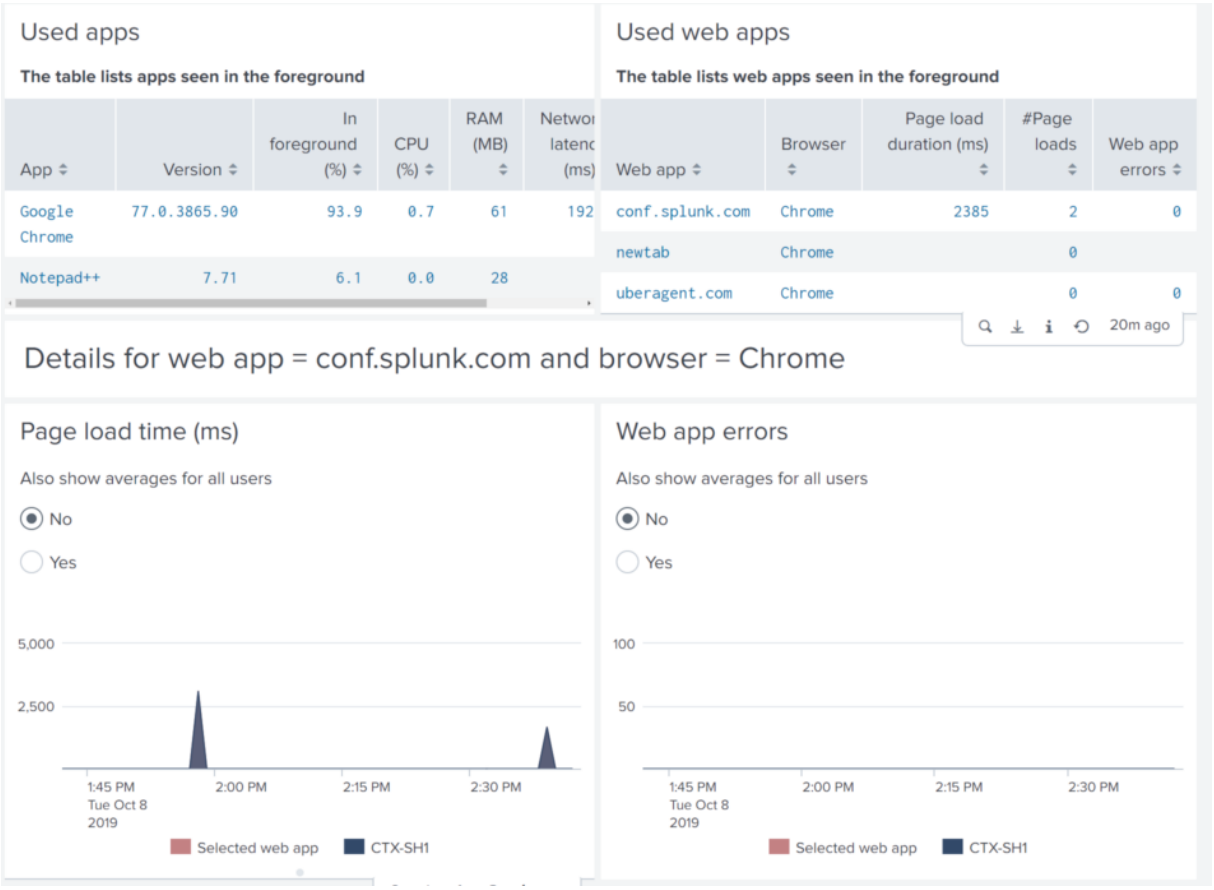
The dashboard gives you an overview of the user's session with helpful content like user and machine information, connection state over time as well as logon time compared to the previous week.



Now dive into the session's performance and compare it to the entire machine or even to other sessions in the organization.



The user is reporting issues with a specific native application or SaaS app? Click on an item in the list and you will get details to solve the user's problem immediately!



Download

The app is available **for free** and can be downloaded from Splunkbase.

Requirements

The helpdesk app provides a different view of the regular dataset collected by uberAgent. As such it requires a working uberAgent infrastructure on Splunk. General uberAgent requirements apply.

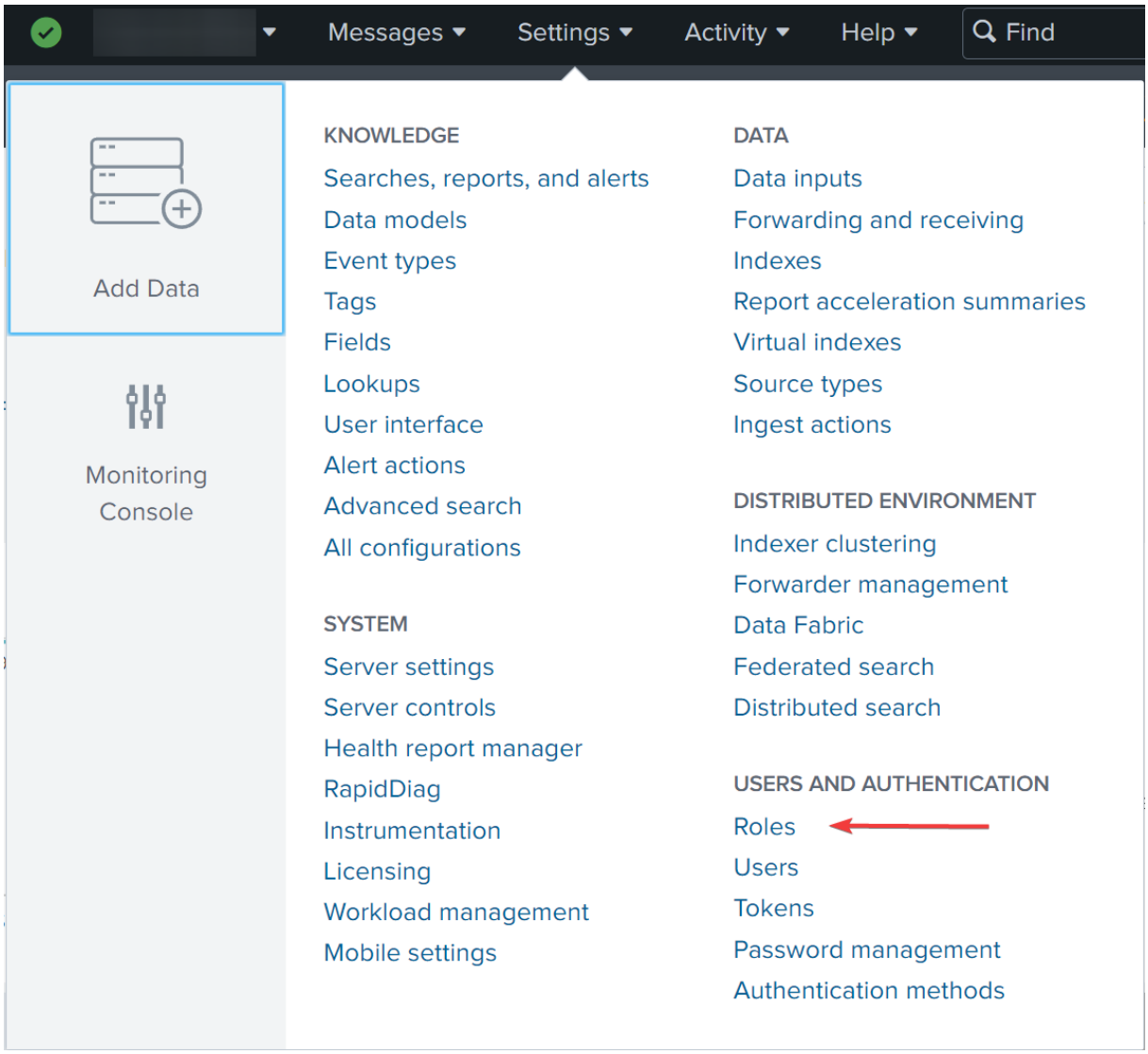
uberAgent Version

- uberAgent UXM 6.0 or greater

Limit Helpdesk Employees to the Helpdesk App

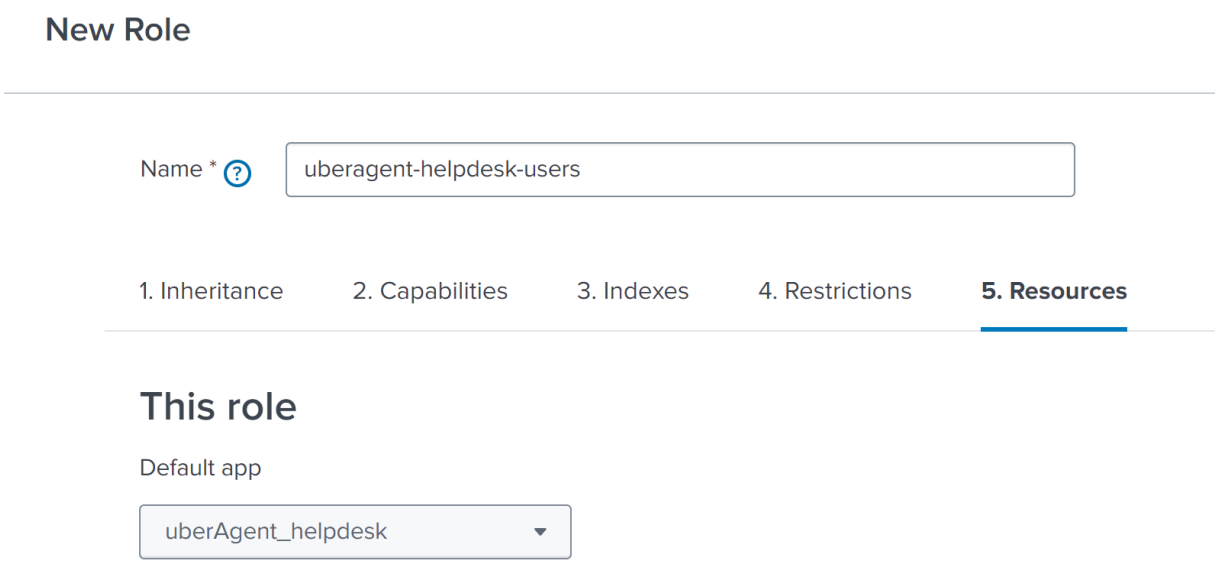
With role based access in Splunk, you can configure that helpdesk employees only see the helpdesk app and are automatically forwarded to the app after logging on to Splunk.

Navigate to **Settings -> Users and Authentication -> Roles**.



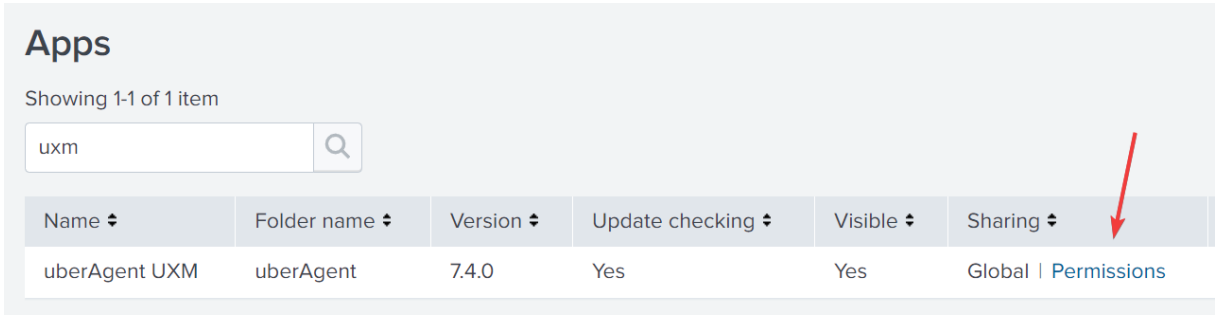
Create a new **user** role with a meaningful name like **uberagent-helpdesk-users**. More information on roles are available in Splunk's documentation.

In the last step, select the **uberAgent_helpdesk** app as default.

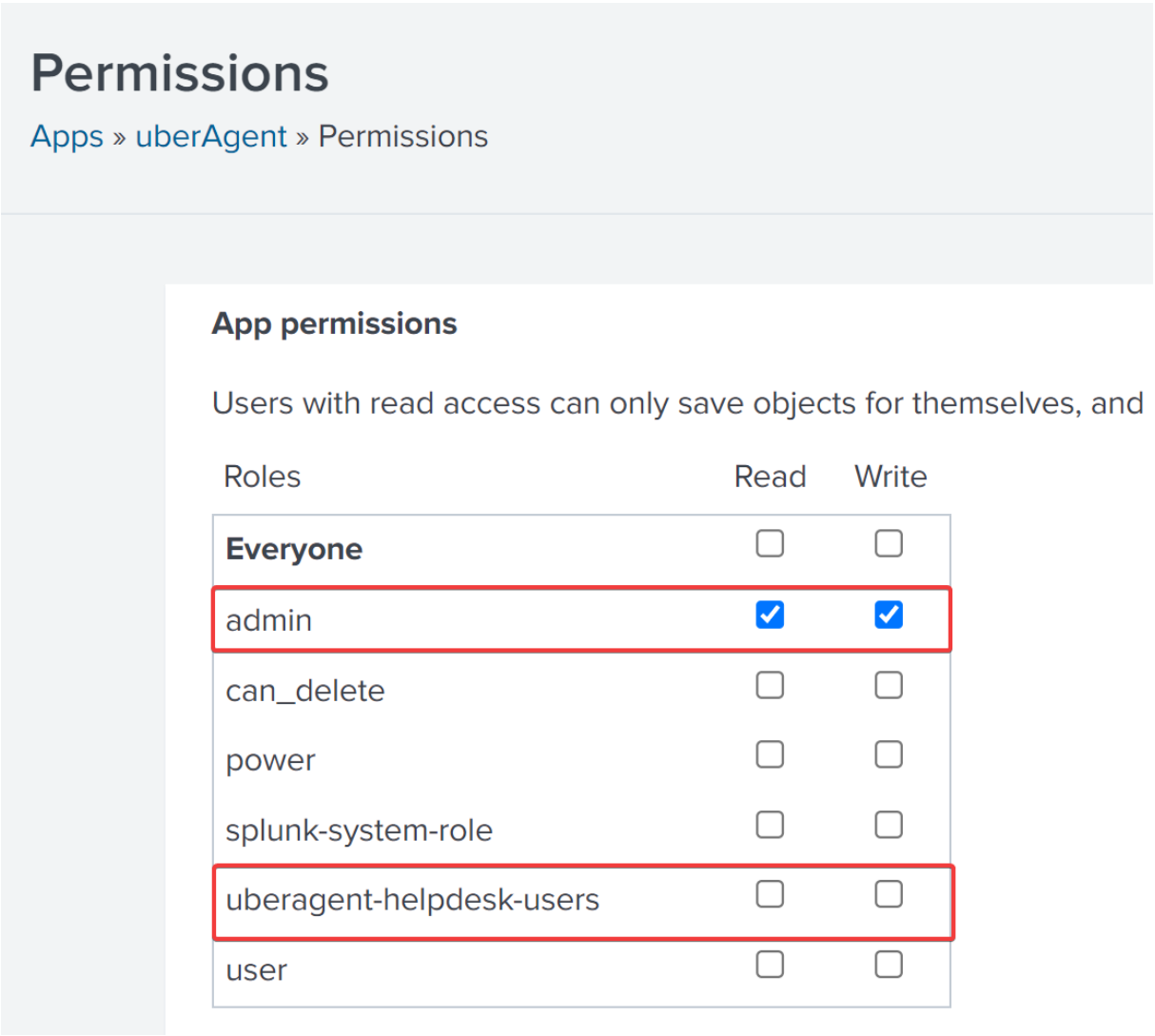


Put your helpdesk users in the new **uberagent-helpdesk-users** role.

Go to **Apps -> Manage Apps**, find the uberAgent UXM app, click on **Permissions**, and remove **Read** access for **Everyone**. Give **Read** access to admins only.

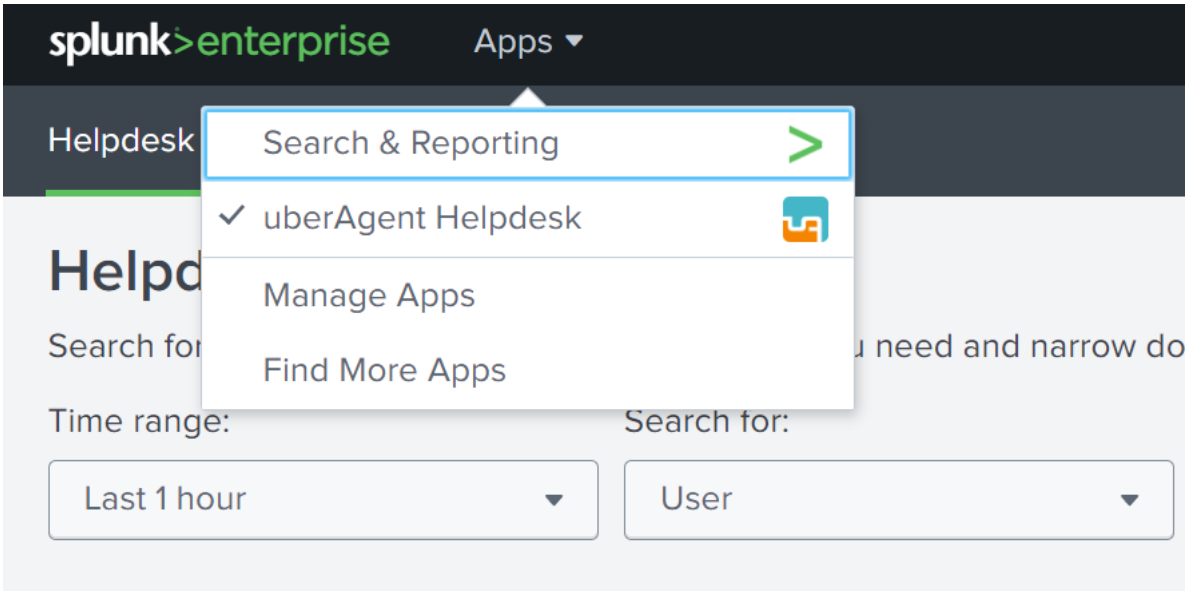


Note that the group **uberagent-helpdesk-users** does not have read access anymore.



Repeat the process for the uberAgent ESA app.

Now helpdesk employees only see the helpdesk app when logging on to Splunk.



This chapter was contributed by Antoin Carroll.

uberAgent® Log Collector Splunk App

April 22, 2026

The uberAgent Log Collector Splunk App is a powerful tool designed to help you monitor the health of your uberAgent deployment. It collects the data logged by uberAgent and sends it to Splunk, providing easy access through pre-build dashboards.

Features

- Automated collection of uberAgent log data
- Centralized logging and monitoring of uberAgent deployments
- Custom dashboards for quick health checks and troubleshooting
- Easy integration with existing Splunk environments

Quick Links

- Changelog and Release Notes
- Quickstart Guide

Getting Started

To get started with the uberAgent Log Collector App, please refer to our Quickstart Guide.

Related Tools

- uberAgent Config & Support Tool
- uberAgent Event Generator for Splunk
- uberAgent Helpdesk Splunk App

For a complete list of uberAgent addons and tools, visit our Addons and Tools page.

Changelog and Release Notes

April 22, 2026

Version 1.2.5

- Updated OS platform filter label.
- Updated regex extraction patterns to make some fields optional, improving log parsing robustness.

Version 1.2.4

- Added more granular permissions to the TA component to meet Splunk Cloud requirements.

Version 1.2.3

- Compatibility with the latest Splunk app packaging rules.
- No new features were added in this release.

Version 1.2.2

- Upgraded dashboards to version 1.1
- Added sc_admin permissions to meet Splunk Cloud requirements.
- Disabled index creation to meet Splunk Cloud requirements.
- Disabled data model acceleration to meet Splunk Cloud requirements.

Version 1.2.1

- Disabled the truncation of lines greater than 10,000 bytes.

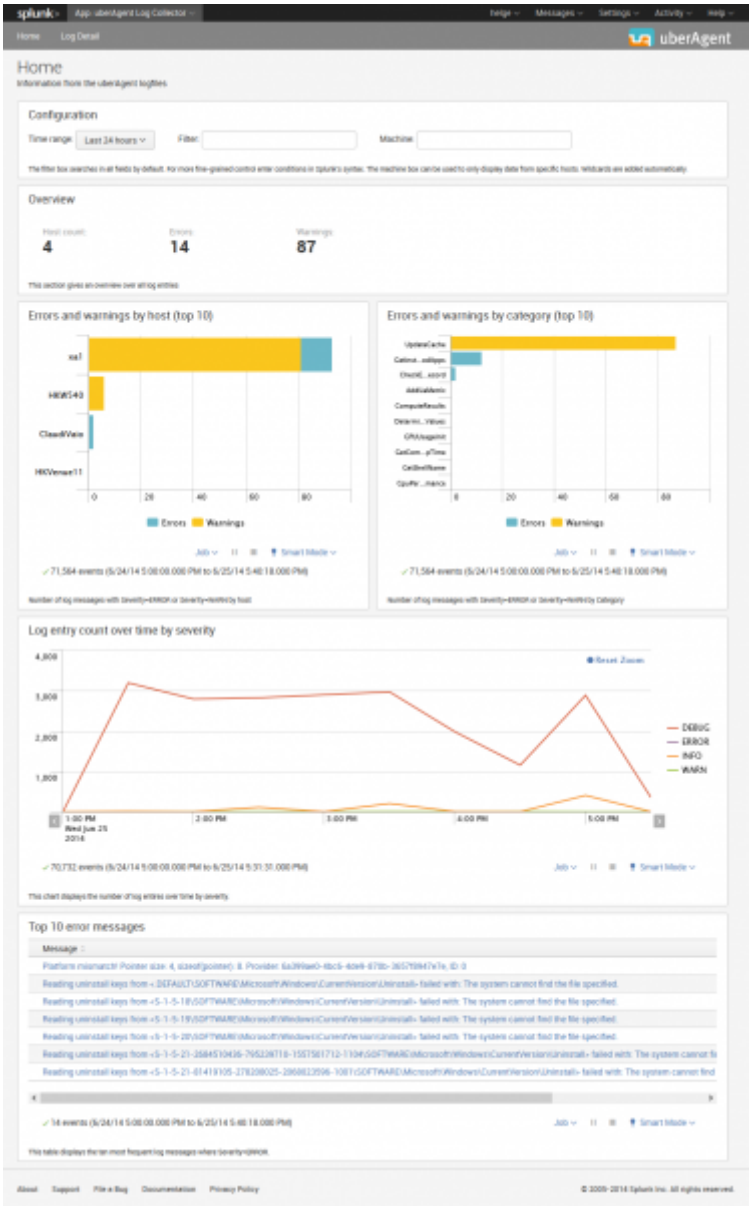
Version 1.2

- Complete dashboard redesign including various filtering capabilities
- Changed all dashboard searches from raw to pivot
- Added support for macOS log files
- Added Splunk data model `uberAgentMeta`
- Added additional logfile `uAInSessionHelper.log`
- Added new sourcetype `uberAgent:Meta:uAInSessionHelperLog`
- Added additional logfile `uberAgentIEExtension.log`
- Added new sourcetype `uberAgent:Meta:uAIEExtensionLog`
- Added additional logfile `uberAgentSandbox.log`
- Added new sourcetype `uberAgent:Meta:uASandboxLog`
- Changed the default index name from `uberagent_log` to `ua_meta_log`
- Added `macros.conf` to centrally rename the index
- Changed the sourcetype name from `uberAgent:log` to `uberAgent:Meta:uberAgentLog`

uberAgent® Log Collector Splunk App

April 22, 2026

uberAgent maintains a very detailed and informative log file that can tell you a lot not only about uberAgent's health but also about the machine uberAgent is running on. Naturally, the log file is stored locally on the computer uberAgent is running on which makes analysis and troubleshooting a bit difficult in large environments. But luckily it is very easy to solve that problem with Splunk!



What is it

uberAgent Log Collector is a set of associated Splunk apps that collect the data logged by uberAgent, send it to Splunk for indexing and provide dashboards for easy access.

Installation

uberAgent Log Collector consists of the Splunk app containing the dashboards and a technology add-on (TA) for collecting the data with Splunk's Universal Forwarder. These two components need to be installed on the following systems:

- **App:** search head(s)
- **TA:** endpoints where uberAgent and the Splunk Universal Forwarder are deployed

Splunk Index

You need to create the Splunk index `ua_meta_log` that stores the logs.

To add the new index `ua_meta_log` with the CLI run `splunk add index ua_meta_log`. The full documentation on creating Splunk indexes is available in the Splunk docs.

Configuration

Configurable Log Path

Since uberAgent 7.3, the log path is configurable. If you set a custom log path, you have to modify the **TA** app: copy the **`default`**`/inputs.conf` to `local/inputs.conf` and adjust the paths accordingly.

System Requirements

The TA requires Splunk's Universal Forwarder to be installed on the same machine.

Download

The *uberAgent Log Collector* apps are available in the Splunk App Directory:

- Download uberAgent Log Collector **app**
- Download uberAgent Log Collector **TA**

uberAgent Log Syntax Highlighter for Notepad++

April 22, 2026

We put a lot of effort into making uberAgent a product that just works. Sometimes, however, you might get to a point where you want to dig deeper and need more information about the product's inner workings. In such a case, of course, uberAgent's log files are your first stop.

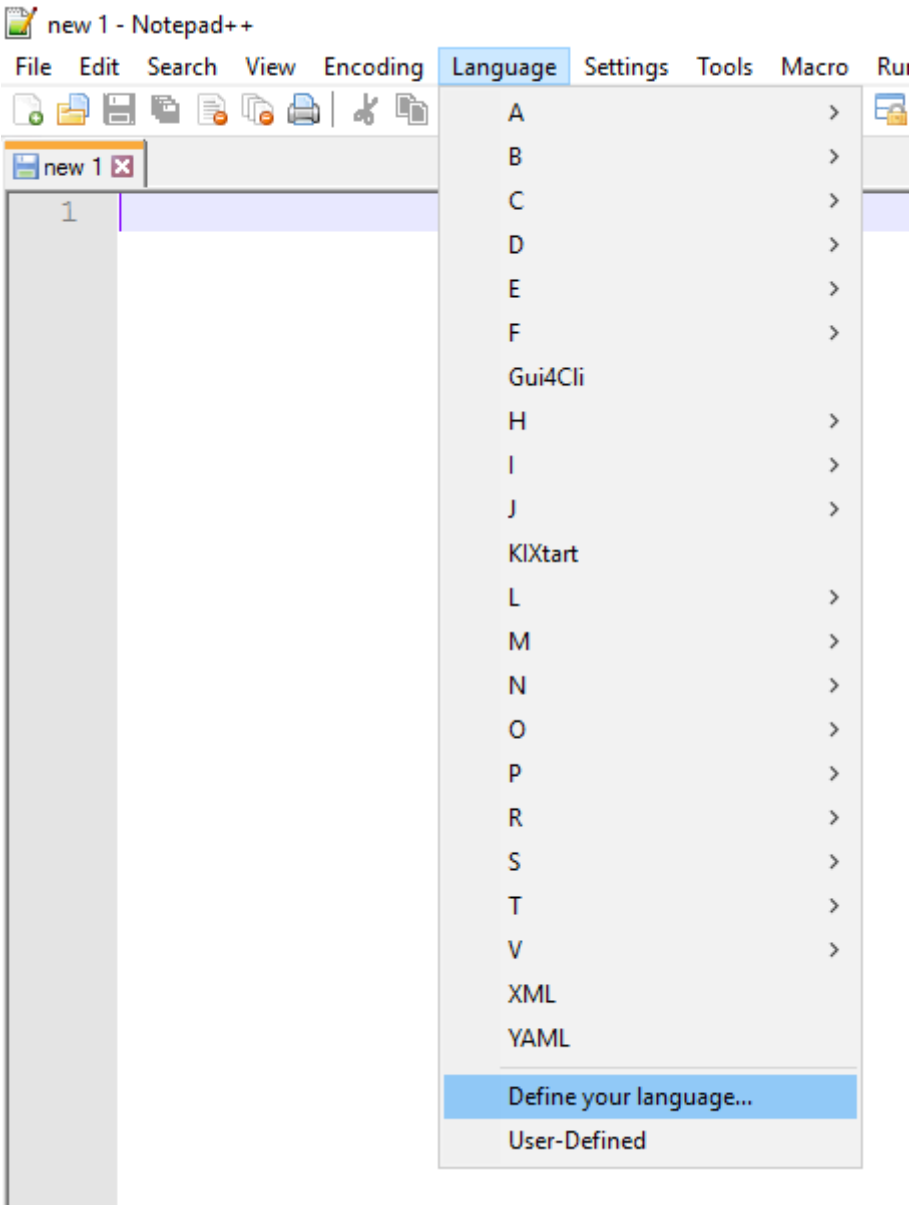
Finding The Cause More Easily

uberAgent logs all of its actions and a great number of relevant system events (e.g., process starts, or logons). That gives you the opportunity to easily identify the root causes of problems (side note: those are most often caused by configuration issues that are typically very easy to spot in the log file).

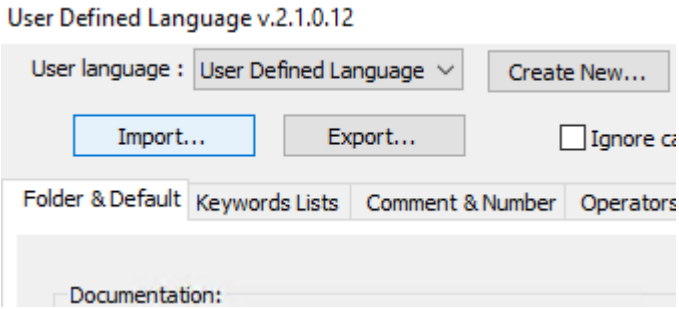
Even though we take great care to optimize the log for readability it is sometimes hard to find the needle in the haystack. That is why we created an uberAgent log syntax highlighter for Notepad++, our preferred text editor on Windows. It highlights the key information, making it easier to find what you are searching for.

Installing The Highlighter

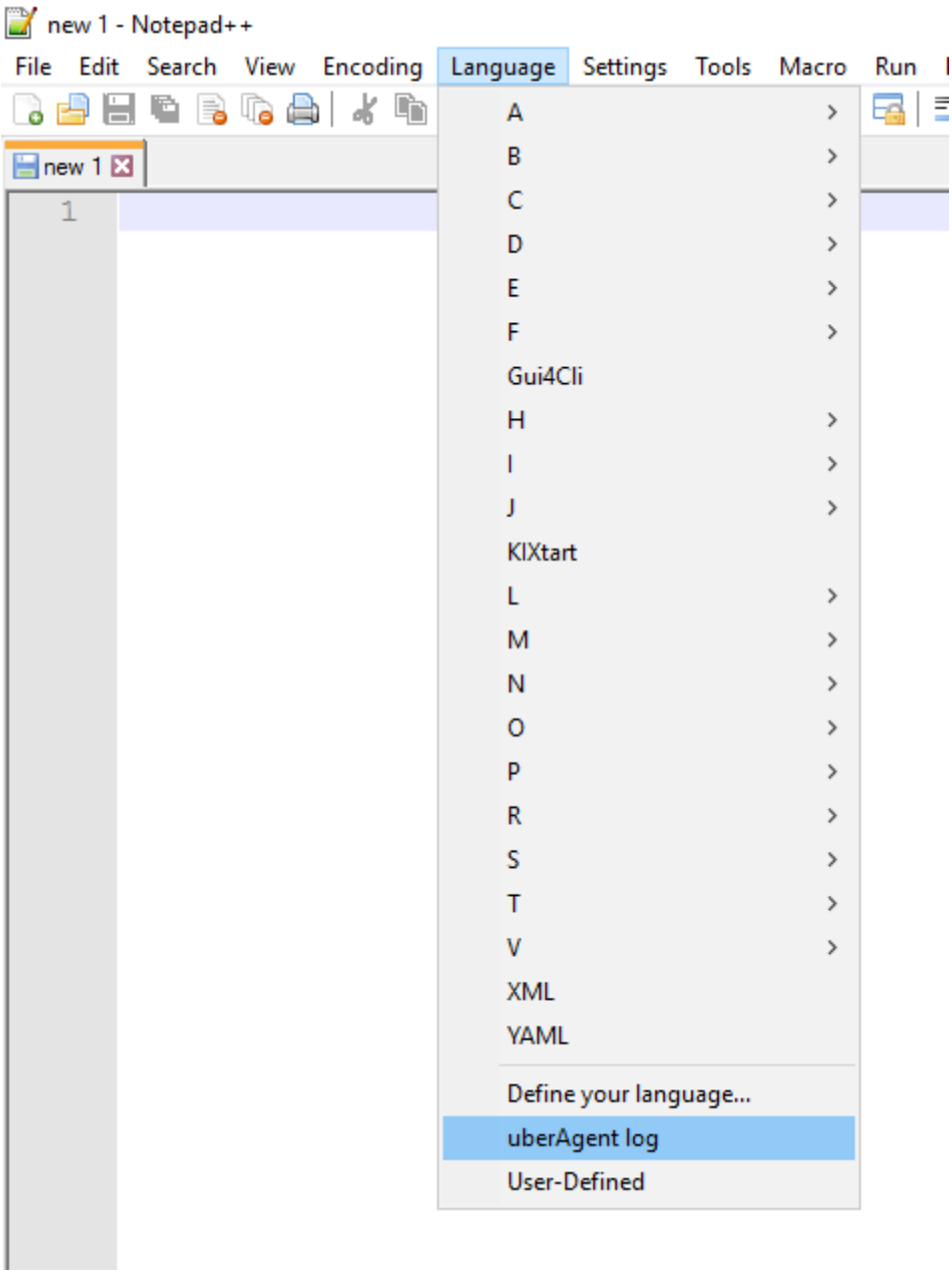
1. Download the highlighter and unpack it.
2. Open Notepad++ and go to *Language -> Define your language...*



3. Click on *Import*... and select the unpacked XML file.



4. Restart Notepad++
5. The uberAgent Log Syntax highlighter is now available as a language in Notepad++

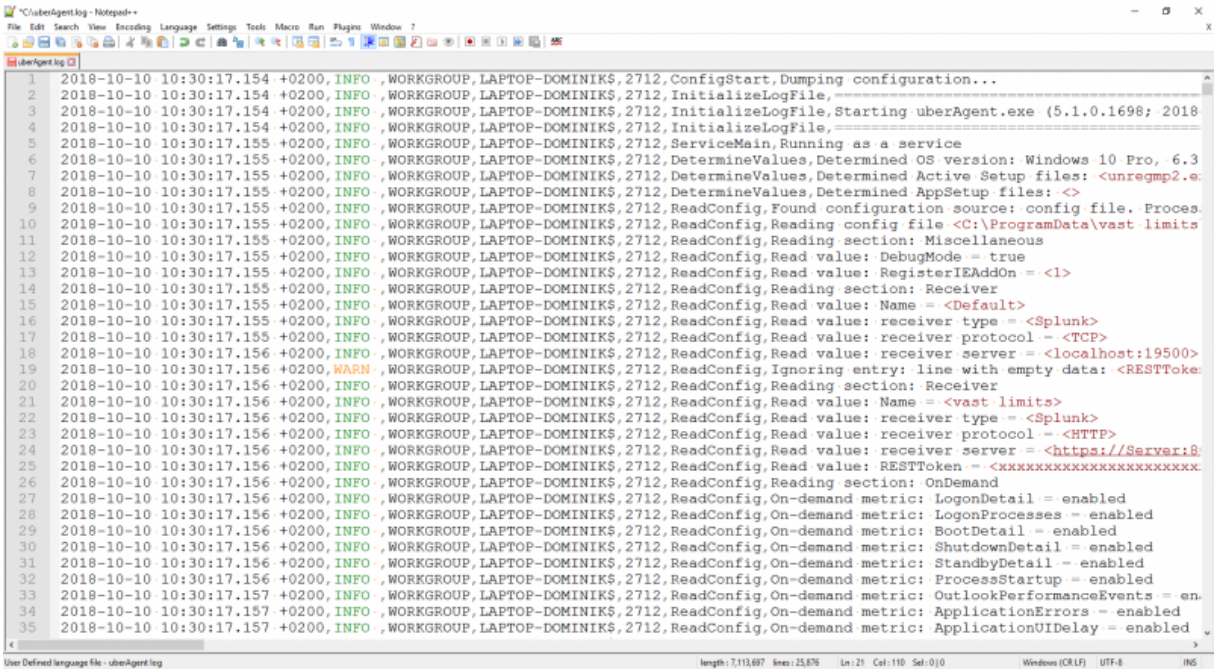


Using The Highlighter

The new language does the following things:

- It highlights the different severities in different colors
  - DEBUG = blue
  - INFO = green
  - WARNING = yellow
  - ERROR = red

- It colors the separators *comma* and *equal* in grey
- It highlights values enclosed in <> in red-brown



This should make troubleshooting with uberAgent's log file a lot more convenient. Enjoy!