Liquidware CommandCTRL™

User Guide

Version 1.2.1

May 2, 2025

This guide has been authored by experts at Liquidware in order to provide information and guidance concerning CommandCTRL.

Liquidware Labs, Inc.

3600 Mansell Road
Suite 2000
Alpharetta, Georgia 30022
U.S.A.

Phone: 678-397-0450

Web: www.liquidware.com

Table of Contents

General Tasks

Side Navigation Panel and Common Components

The default CommandCTRL application has a side navigation panel. Each item in the side panel navigates you to a screen that has GUI components. The items on these screens provide you with a lot of information, real-time metrics about a user's machine, and more. Knowing how to interpret these metrics will help you to quickly resolve issues.

Side Navigation Panel

This briefly discusses each of the items listed in the side navigation panel, its use, and an explanation of the components that will provide you with the ability to do a task or get more information about the metric.

Dashboard

This displays all the widgets and components that provide functionality and information.

Task Manager

This displays all the Processes, Services, Performance, and Startup functionality and information. It provides information and control over processes and applications running on a machine. It allows the ability to monitor and manage the processes and applications running on a machine giving visibility and control over the processes, applications, and system performance of the operating system, helping to more efficiently monitor, manage, and troubleshoot a machine.

Tasks

This displays all the tasks that ran over time on that machine.

Diagnostics

This displays different diagnostics that can be run on a machine that will display performance and help you determine if any of the results are a factor in the reasons why there is an issue so you can identify, analyze, and resolve issues that may impact the performance, stability, or functionality of the machine or its components, allowing for efficient troubleshooting and problem resolution.

Machines

This displays all the machines connected to the machine. This displays the machine name, domain, the agent each machine is running, and when it last logged into the network. For more detailed information, see View a Machine's History via History Playback Mode

Blocked Machines

This displays all the machines that are currently being blocked. This displays the machine name, the machine ID, IP address, and how long the machine will be blocked. You can add or remove machines from the blocked list. For more detailed information, see Block or Unblock a Machine.

Scripts

This provides two pages, **Store** and **Results**. The **Store** page allows you to search for and view the scripts that are stored on that machine. The **Results** page allows you to search for and view scripts that have been run on the machine.

Triggers

This allows you to customize Trigger violations that occur in Real-Time and in History mode. The violations are visible with in Dashboard highlighting of the metric that is violation.

Shell

This allows you to search for and connect to a machine using Powershell, Command-Line (Cmd), or when available, Bash. As you type a letter the dialog box filters and lists the available machines. When you select a machine, it automatically begins connecting to the machine.

Tenant

This displays the tenant that is associated with the machine. Under the landing page is the **Company** tab, which lists the **Profile** screen that contains all the needed information about the tenant and who manages it.

Users

This displays all the users that are associated with the tenant, their role, when they were added, and the last time they logged in. You can view a user by clicking the icon. When the dialog box appears, you can change their email address and role, and delete the user from the tenant.

It also shows who has been invited to join the tenant and their status, such as Pending. You can Resend an Invite by clicking the icon and you can Delete the Invite by clicking the icon.

Roles

This displays the system roles for the owner, administrators, and users. You can Filter the Columns by clicking the icon and selecting from the drop-down the columns you want to appear.

You can Add a Role by clicking the icon. When the **New Role** dialog box appears, enter the **ID**, **Name**, **Description**, and **Permissions** and then click **Create** and the new role is added.

Site

This displays the **Scripts** and **API Keys** for the tenant.

For **Scripts**, you can enable the ability for **Agents to Hash Check if Not Signed**, clicking the icon so the switch moves to the right.

For **API Keys**, you can Filter the Columns by clicking the icon and selecting from the drop-down the columns you want to appear on the screen.

Install Agent

This provides information about the latest agent (e.g., Version, Hash, Tenant ID, and the API Key), the ability to enable or disable automatic updates, and allows you to download the latest agent or copy it for when you want to silently install the agent on a machine. For more detailed information, see Update the CommandCTRL Agent on a Single Machine or Update the CommandCTRL Agent on Multiple Machines.

Online Help

When you click the icon, a new browser window opens, and the CommandCTRL online help appears.

Support

When you click the icon, a new browser window opens, and the Liquidware Support page appears.

Common Components

This explains the components on a screen that display in many of the Side Navigation Panel screens.

General Tasks and Information Banner

When you click on any of the items listed in the Side Navigation Panel, the following components display at the top of the screen.

Recent

Clicking the RECENT down-arrow displays the most recent Pages and Machines you visited.

Search

Clicking the magnifying glass icon displays a search field.

User Profile

Clicking the user profile icon displays General information about the user and tenants, Settings, and allows you to log-out.

Toolbar

When you click Dashboard, Task Manager, or Diagnostics in the Side Navigation Panel, the following components display just above the widgets on the screen.

Machine Specific Information

This displays the name of the machine, date and time it last logged in, and the version of the agent running on the machine.

View History

The 

icon displays the daily history for that machine. Clicking any of the days displays the hours in a day. Clicking an hour displays a recording of the entire hour for that machine and all the metrics in the widgets as the timeline progresses. Speed controls, pause, and the time of the recording is located underneath the timeline.

Shell

For information about , see Shell.

Diagnostics

For information about , see Diagnostics.

Scripts

For information about , see Scripts.

Real-Time

This allows you to enable real-time metrics by clicking the icon so the switch moves to the right.

Agent Connected

This heartbeat icon displays if the agent is connected.

Dashboard Widgets and Metrics

The default CommandCTRL dashboard displays a dozen or more different widgets. Each widget provides you with a lot of information and metrics about a user's machine, their location, and more.

Knowing how to interpret these metrics and how to modify your Dashboard to provide you with real-time metrics in an easy-to-use interface will help you to more quickly resolve issues.

This discusses all the widgets that are available on the Desktop, their use, and an explanation of the items you can click on to get more information or perform functionality within the widget. The widgets that are display on the Desktop are:

- System Properties
- Location
- Current Sessions
- Top 5 CPU, RAM, Disk, and Net Consumers
- CPU
- Memory
- Disk 0 (C:)
- Ethernet
- Wifi
- GPU 0
- Display Protocol
- Battery

Basic Widgets

There are many widgets on the dashboard that are intuitive to most using CommandCTRL. Those widgets do not require a lot of explanation; however the following is a brief explanation of the functionality of each widget and the icons that allow you to customize the widget.

System Properties

This displays the name of the host, domain, last time the machine booted up; and all the hardware, software, and firmware details about the machine.

Actions

In the top right corner of the widget are the following icons:

- **Shutdown**: Clicking this icon will remotely shutdown the machine.
- **Restart**: Clicking this icon will remotely restart the machine.
- (**Widget Menu**): Clicking this icon displays a drop-down menu that allows you to select metrics that will display in the widget for that machine. Selecting/checking a box enables the metric to display in the widget and deselecting/unchecking a box disables the metric from displaying on the screen. Selecting **Remove** at the bottom of the drop-down list removes the widget from the Dashboard. If you remove the widget, you can restore it by clicking the (**Configuration**) icon in the bottom right corner of the screen and adding it to the Dashboard.

Location

This displays the location of the machine.

> **Note:** The ⋮ (**Widget Menu**) in the top right corner has no functionality at this time.

Current Sessions

This displays the name of the users that are connected to the machine and the protocol being used to connect to the machine (e.g., RDP). If a user was connected, but then disconnected, it will show "disconnected" next the user's name.

Widget Actions

In the top right corner of the widget are the following icons:

- **Logout All**: Clicking this icon logs out all users that are logged into that machine.
- **Remove**: Clicking this ⋮ icon removes the widget from the Dashboard.

User Actions

Next to each user within the widget are the following icons:

- **Connection**: This icon only appears if the user is logged into the machine that is currently showing metrics in the widgets on the hosted Desktop. The name of this machine can be seen in the top left corner of the Desktop. Hovering over this icon lets you know the name of the user's machine (source) that is connected to this machine (destination).

  Clicking the **Connection** icon advances you to the source machine the user is logged into. If the agent is installed on the user's machine, you can view the widgets and metrics for that user's machine.

  This **Connection** icon only displays if a user is logged into the machine being shown in the current hosted Desktop. Once the user logs off this machine, the **Connection** icon and the **Display Protocol** widget disappears.

  > **Note:** If more than one user is logged into the hosted Desktop, a check box appears next to each user's name. When that occurs, the metrics on the Display Protocol and all the "Top 5" consumers widgets are automatically altered to show the combined metrics for those users. You can select only the users you want to collect metrics in the Dashboard widgets. For more information, see Multiple Session Detection and Filter by User.

- **Environment Variables**: Clicking this icon displays a dialog box that shows pertinent information about the user's machine. You can scroll top to bottom and left to right through the information to find about all you would want to know about a user's machine. To view the Dashboard again, click **Close** or anywhere outside the dialog box.

- **Logout**: Clicking this icon logs out the user from the connection they made to the hosted Desktop.
- **Remote**: Clicking this icon allows you to remote into the user's machine.

Top 5 CPU, RAM, Disk, and Net Consumers

The following displays the top 5 applications on a machine that are:

- CPU Consumers: Using CPU resources.
- RAM Consumers: Using RAM resources and the amount of RAM each are using.
- Disk Consumers: Using hard drive resources and the speed of each write.
- Net Consumers: Using network bandwidth resources and the amount of bandwidth each are using.

Widget Actions

In the top right corner of the widget are the following icons:

- **Go to Processes**: Clicking this icon advances to the **Processes** screen (see below).
- **Remove**: Clicking this icon removes metrics from the widget or the entire widget from the Dashboard. If you remove the widget, you can restore it by clicking the (**Configuration**) icon in the bottom right corner of the screen and adding it to the Dashboard.

Process Screen Search and Filters

If you clicked on **Go to Processes** icon you are advanced to the Processes screen where it displays every process that is running on all machines that are listed under **Users**. Across the top of the screen are the following:

- **Users**: Clicking the drop-down arrow displays all the machines, domain, and users for the processes that are being shown on the screen.
- **Search**: Clicking within the field allows you to enter the name of a process. As you enter each character or number, the screen automatically filters.
- **Filter Columns**: Clicking this icon displays a drop-down menu that allows you to select processes that will display on the Processes screen for all machines that are listed under **Users**, such as CPU. Clicking a check box enables the process to display on the screen and unchecking a check box disables the process from displaying on the screen.
- **X**: Clicking the icon located to the far right of each process listed within the Processes screen stops/kills/terminates that process.

Widget User Actions

To the far right of each of the "Top 5" consumers widgets (e.g., CPU, RAM, Disk, and Net) listed within the widget is the following icon:

- **X**: Clicking the ✕ icon located to the far right of each process listed within the widget stops/kills/terminates that process.

CPU

This displays detailed information about the CPU and the percentage of the CPU that is being used on this machine or in the cloud.

Actions

In the top right corner of the widget is the following icon:

- ⋮ (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the CPU:

- **CPU**: This is the brand, model, and speed of the CPU in the machine or in the cloud.
- **Utilization**: This is the percentage of the CPU that is being used in real-time.
- **Sockets**: This is the number of physical sockets attached to the motherboard in which the CPU is plugged into.
- **Cores**: This is the number of cores within the CPU or the number of virtual cores that been assigned to that machine.
- **Processors**: This is the number of processors within the CPU or the number of virtual processors that been assigned to that machine.
- **Base Speed**: This is the clock speed frequency at which this processor is currently operating. Some processors support dynamic frequency scaling so it can adjust its clock speed based on various factors, such as workload, power management settings, and thermal conditions. This means the base speed and processor clock speed may be different. For example, the processor clock speed might be 2.4GHZ, but the base speed is currently reporting 2.9GHZ, which indicates the processor supports dynamic frequency scaling since it is running at a higher clock speed frequency.

Memory

This displays detailed information about the RAM memory and the amount that is in use and available on this machine or allocated in the cloud.

Actions

In the top right corner of the widget is the following icon:

- ⋮ (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the RAM that is installed in this machine or allocated in the cloud:

- **Total RAM**: This is the amount of RAM.
- **In Use**: This is the amount of RAM that is currently being used.
- **Available**: This is the amount of RAM that is available for use.

Disk 0 (C:)

This displays detailed information about the hard drive or Disk installed, connected to the machine, or disk space allocated in the cloud; the percentage it is active, average response times, and read and write speeds.

> **Note:** For every hard drive or Disk installed, connected to the machine, or disk space allocated in the cloud; a widget will appear. For example, if a second Disk was connected to a machine, a widget would appear as Disk 1 (D:), however if Disk 0 (C:) was partitioned then Disk 1 would be labeled the next logical letter, such as Disk 1 (E:). If a Disk widget skips a letter(s) then it indicates the previous Disk was partitioned. Each Disk widget provides the same information, but it is specific to that hard drive or disk space allocated in the cloud.

Actions

In the top right corner of the widget are the following icons:

- **View Partition Layout**: Clicking the magnifying glass icon causes a **Partition Layout** dialog box to appear that shows the Recovery Partition, EFI System Partition, and Basic Data Partition for the hard drive in that machine or disk space allocated in the cloud. It also shows the format type (e.g., exFAT) for that Disk. The Disk might be partitioned so that the operating system can reside in a separate space from all other files. Each Disk widget on the desktop will show partition information for that hard drive and the total size of the Disk.
- (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the hard drive or Disk installed, connected to a machine, or disk space allocated in the cloud:

- **Storage Type**: This information is located directly underneath the Disk label. It displays the type of storage being used, whether it is a physical hard drive or virtual space.
- **Active Time**: This is the percentage of how much time the Disk is performing data operations, such as reading or writing data, as opposed to being idle or idle time. Monitoring the active time of a Disk can provide insights into its performance and workload. It can be useful for assessing the

health, efficiency, and workload of a Disk, as well as identifying potential performance bottlenecks or issues related to data access or transfer.

- **Average Response Time**: This is the time in milliseconds (ms) it takes for the Disk to complete a data access operation, including the time it takes to locate the requested data, transfer it to the system, and confirm the completion of the operation. Average response time is an important performance metric for assessing the efficiency and effectiveness of a Disk in meeting data access requirements. It can be used for benchmarking, comparing different Disks or storage systems, and identifying potential performance issues or bottlenecks related to data access speed. It is worth noting that average response time can vary depending on factors such as the type of hard drive (HDD vs. SSD), the storage capacity, the workload, and the system configuration, among others.
- **Capacity**: This is the total capacity of the Disk (hard drive). To see if the Disk was partitioned and the size of each partition, see View Partition Layout.
- **Formatted**: This is how much of the total capacity of the Disk was formatted.
- **Read Speed**: This is the amount of data that can be read from the Disk in a given amount of time. Read speed is an important performance factor for assessing the efficiency and effectiveness of a Disk in providing data to the system or other devices. A lower read speed may indicate slower performance, which can impact the overall performance of the system that relies on the Disk for data retrieval. Read speed can depend on various factors, including the type of hard drive (HDD vs. SSD), the storage capacity, the rotational speed (for HDDs), the interface used (e.g., SATA, SAS, NVMe), and other factors such as caching technology or system configuration. It can be useful for evaluating storage performance requirements for specific applications or workloads that involve frequent data access or retrieval.
- **Write Speed**: This is the amount of data that can be written to the Disk in a given amount of time. The same factors described in "Read Speed" apply.
- **System Disk**: This is the primary Disk that contains the operating system and other essential system files required for a machine to boot up and operate. The System Disk is also sometimes referred to as the "boot drive" or "C: drive." If "Yes" is in this field, the main Disk was partitioned into one or more logical drives, with the "C:" drive being the default drive letter assigned to the partition that contains the operating system. Having a fast and reliable System Disk is important for overall system performance, as it affects the boot time, responsiveness, and stability of the machine.
- **Page File**: This is the file that is used by the operating system as virtual memory. It is also known as a "paging file" or "swap file." If "Yes" is in this field, a Page File is being managed by the operating system to store data that is not actively being used by running programs or the operating system itself. The size of the Page File can be set by the user or managed automatically by the operating system based on system usage patterns. Properly managing the Page File can help optimize system performance and prevent issues related to low memory situations.
- **Type**: This is the Disk using the interface, such as Serial ATA (SATA), Serial Attached SCSI (SAS), PCIe (PCI Express), Non-Volatile Memory Express (NVMe), Fiber Channel (FC), Thunderbolt, or USB (Universal Serial Bus).

Ethernet

This displays detailed information about the Ethernet protocol, send and receive speeds, and latency on this machine.

Actions

In the top right corner of the widget is the following icon:

- ⋮ (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the Ethernet connection:

- **Ethernet Type**: This is the type of Ethernet the machine is using to connect to networks and machines, such as Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, 40 Gigabit Ethernet, or 100 Gigabit Ethernet.
- **Send**: This is the speed of the data packets being sent from this machine to a destination device over an Ethernet network using Ethernet frames and the appropriate signaling method for the Ethernet type and data rate being used.
- **Receive**: The same as above, only it is the speed of the data packets being received.
- **IP Address**: This is the internet protocol address that is being used to connect the machine to networks and machines.
- **Gateway IP**: This is the internet protocol address that is being used to connect the gateway, which is a network node acting as a bridge or a router that connects different network segments, allowing devices on one network to communicate with devices on another network.
- **Gateway Latency**: This is the amount of time it takes for a data packet to travel from the source device to the destination device over a network. High gateway latency can be caused by a variety of factors, including the processing time required for the gateway device to examine and route data packets, queuing delays if multiple data packets are waiting to be processed, network congestion, or other factors that may affect the performance of the gateway device. High gateway latency can impact the overall performance and responsiveness of a network, as it can increase the time it takes for data packets to reach their destination, resulting in increased communication delays or decreased network throughput. Therefore, knowing the Gateway Latency can help you determine if the problem you are trying the resolve is related to latency, and if so, direct your attention to a resolution, which might include a better network design and optimization to ensure efficient and low-latency communication between different networks or sub-nets.

Wi-fi

This displays detailed information about the Wi-fi adaptor, send and receive speeds, and latency on this machine.

Actions

In the top right corner of the widget is the following icon:

- (Widget Menu): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the Wi-Fi connection:

- **Wi-Fi adaptor type**: Indicates the type of Wi-Fi hardware the machine uses to connect to networks, which can affect the range, speed, and reliability of the wireless connection.
- **Send**: Represents the rate at which data packets are transmitted from this device to another over a Wi-Fi network, utilizing Wi-Fi frames and the corresponding signaling techniques suitable for the specific type of Wi-Fi and its data rate.
- **Receive**: Reflects the rate at which data packets are received by this device from another over the Wi-Fi network, using similar technology and methods as the sending process.
- **IP Address**: This is the internet protocol address that is being used to connect the machine to networks and machines.
- **Gateway IP**: This is the internet protocol address that is being used to connect the gateway, which is a network node acting as a bridge or a router that connects different network segments, allowing devices on one network to communicate with devices on another network.
- **Gateway Latency**: This is the amount of time it takes for a data packet to travel from the source device to the destination device over a network. High gateway latency can be caused by a variety of factors, including the processing time required for the gateway device to examine and route data packets, queuing delays if multiple data packets are waiting to be processed, network congestion, or other factors that may affect the performance of the gateway device. High gateway latency can impact the overall performance and responsiveness of a network, as it can increase the time it takes for data packets to reach their destination, resulting in increased communication delays or decreased network throughput. Therefore, knowing the Gateway Latency can help you determine if the problem you are trying the resolve is related to latency, and if so, direct your attention to a resolution, which might include a better network design and optimization to ensure efficient and low-latency communication between different networks or sub-nets.
- **Strength**: Indicates the signal strength of the Wi-Fi connection, which affects the quality and stability of the connection. Higher strength generally means better performance and fewer disruptions.
- **Link Speed (Rx/Tx)**: Shows the current reception (Rx) and transmission (Tx) speeds that the Wi-Fi adapter is capable of handling, which can vary based on distance from the router, interference, and the capabilities of the Wi-Fi network.
- **SSID**: Displays the Service Set Identifier, which is the name of the Wi-Fi network the device is connected to. This helps users identify and connect to the correct network.
- **Protocol**: Describes the Wi-Fi protocol in use, such as 802.11n or 802.11ac, which dictates the performance characteristics and compatibility with other devices.
- **Security**: Specifies the type of security protocol in use (e.g., WEP, WPA, WPA2) to protect the network from unauthorized access and ensure data privacy.
- **Band**: Indicates whether the connection is using a 2.4 GHz or 5 GHz frequency band. The choice of band can affect the network's range, interference susceptibility, and data transmission speed.

Enable/Disable Gateway Ping on Agents

This allows the ability to Enable/Disable Pinging on the agent machines default gateway. This allows the administrator to disable the pinging of the machine gateway every 10 seconds when recording history and every 3 seconds when in real time mode. This is useful when most of the machines are within the same network and pinging the default gateway in mass is not desired. To view the agents current ping settings, complete the following steps:

1. In the side navigation panel, go to **Settings > Site**.
2. In the **Enable/Disable Gateway Ping on Agents** section, click the toggler to the desired enable (displays in red) or disabled state (displays in grey).

GPU 0

This displays detailed information about the Graphics Processing Units (GPU) installed, connected to the machine, or GPU space allocated in the cloud; how much RAM is being shared with the GPU, and the percentage of the GPU that is being utilized.

Actions

In the top right corner of the widget is the following icon:

- ⋮ (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the GPU:

- **GPU Type**: This is the type of GPU being used for this machine. The GPU being used could be Integrated, Discrete, Mobile, Workstation, Server, or virtual GPU in the cloud.
- **Utilization**: This is the percentage of the GPU that is being used in real-time.
- **Dedicated**: This is the total amount of RAM that is dedicated to the GPU and how much of that RAM the GPU is using in real-time. Most likely, the RAM is "dedicated" VRAM from a physical video adapter. In that situation it is probably not being shared with other tasks running on that machine.
- **Temp**: This is the temperature of the GPU in real-time.
- **Shared**: This is the total amount of RAM that is being shared with the GPU and how much of that RAM the GPU is using in real-time. Most likely, the RAM is "shared" from a virtual machine. The RAM might be shared with other tasks running on that machine.

Battery

This displays detailed information about the battery in a laptop, such as the percentage of the battery remaining, its capacity, and more.

> **Note:** This widget only displays if the machine you are viewing is a laptop.

Actions

In the top right corner of the widget is the following icon:

- ⋮ (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The widget displays the following static and real-time information about the battery:

- **Battery remaining**: This displays the percentage of the battery that is remaining for use.
- **State**: This displays the state of the battery. For example, this displays **Full** if **Battery remaining** displays **100%**.
- **Current capacity**: This is the total amount of amperage in the battery displayed in mW. This shows you the health of the battery if you compare the measurement to other measurements displayed in the widget, such as **Design capacity**.
- **Design capacity**: This is the total amount of amperage capacity according to its design by the manufacturer displayed in mW.
- **Current capacity**: This is the total amount of voltage in the battery displayed in mW. This shows you the health of the battery if you compare the measurement to other measurements displayed in the widget, such as **Design voltage**.
- **Design voltage**: This is the total amount of voltage capacity according to its design by the manufacturer displayed in mW.
- **Current charge rate**: This is the rate of amperage that the battery is drawing when it is being charged displayed in mW. If **0mV** is displayed then most likely the battery is not being charged at that time so the laptop is not plugged into an AC charger and is running on battery power.

Advanced Widgets

There are some widgets on the dashboard that are more advanced. The following is an explanation of the functionality of those widgets that are more advanced and the icons that allow you to customize the widgets.

Display Protocol

This displays detailed real-time and historical information about a machine that you are remotely logged into. That machine could reside anywhere in the world, whether it is in the cloud, in a data center, or on your local network.

Display Protocol metrics are captured by creating a pipe between the physical machine and the hosted desktop using Citrix HDX, VMware PCoIP, VMware Blast, and Microsoft RDP, Microsoft RFX, Microsoft CloudPC, Microsoft AVD, or VMware RDP. The widget will auto-detect the protocol that is being used.

When a user connects to the machine (destination) that is showing metrics within the widgets on the Desktop; the protocol (e.g., RDP) being used displays next to the user's name in the **Current Sessions** widget, the **Connection** icon displays to the right of the user's name, and the **Display Protocol** widget appears on the hosted Desktop. Clicking the **Connection** icon advances you to the source machine the user is logged into. If the agent is installed on the user's machine, you can view the widgets and metrics for that user's machine.

When the user logs out of the machine that is showing metrics within the widgets on the Desktop; next to the user's name shows ***disconnected***, the **Connection** icon disappears in the **Current Sessions** widget to the right of the user's name, and the **Display Protocol** widget disappears from the Desktop.

Mirroring

Mirroring gives you the ability to mirror the hosted desktop's Display Protocol widget on the user's physical machine. This allows you to take a collection of metrics that are sourced on a remote hosted desktop and mirror them to your physical desktop. By allowing you to view all the real-time metrics coming from the hosted desktop on your physical machine you do not need to switch back-n-forth between hosted and physical machines. This feature makes troubleshooting metrics that might be causing an issue so much easier and quicker.

Multiple Session Detection

It is possible to have many users connecting remotely to one machine. In this situation, Display Protocol metrics would be displayed for each user, which would overwhelm a typical browser and the dashboard. To avoid this from occurring, when more than one session is detected, the Display Protocol widget will not display on the dashboard. To be able to view the Display Protocol metrics without overwhelming a browser and the dashboard, you are able to select which of the users you want to collect metrics. For more information, see Filter by User below.

Filter by User

When Multiple Session Detection occurs, as explained above, you are able to manually select which of the users you want to view their Display Protocol metrics. After you selected the users, metrics will appear for those specific users on the Dashboard by showing their metrics in each Display Protocol widget (one widget for each user) and all the selected user's metrics are combined into the "Top 5" consumers widgets (e.g., CPU, RAM, Disk, and Net). For example, if you selected three users, you will see three Display Protocol widgets and the combination of the metrics from all three users in each of the "Top 5" consumers widgets.

If you click the **Go to Processes** icon on:

- A Display Protocol widget for any of the users you selected, the tasks displayed on the **Processes** screen will only be those related to that user.
- Any of the "Top 5" consumers widgets (e.g., CPU, RAM, Disk, and Net), the tasks displayed on the **Processes** screen will only be those related to the users you selected.

> **Note:** The agent needs to be installed on the user's machine for you to be able to view their machine's widgets and metrics.

To filter by user, do the following:

Note: The number of users that you can successfully view their metrics at the same time on your physical machine will depend on the many factors that are based on your machine, such as RAM, etc. If your browser or the Desktop is overwhelmed, select fewer users until you are able to successfully view user metrics. A recommendation is to not exceed ten users.

1. In the **Current Sessions** widget, click the check box next to the user's name to select the users that you want to view their Display Protocol metrics.

   The **Display Protocol** widget for each user appears and the "Top 5" consumers widgets (e.g., CPU, RAM, Disk, and Net) display the metrics for all the users you selected. The data being displayed in these widgets is only for the users you selected.

2. Click the **Go To Processes** icon on any of the "Top 5" consumers widgets.

   The **Processes** screen displays. The data being displayed is only for the users you selected. You are able to see each of the usernames under the **User** column.

Actions and Information

Across the top of the Display Protocol widget is the following:

- **Connection**: This information is displayed directly underneath the name of the widget. It shows the name of the source machine that is logged into this machine and the protocol (e.g., RDP) being used to connect to the machine.
- **Go To (machine name)**: Hovering over this icon lets you know the name of the user's machine (source) that is connected to this machine (destination). Clicking the **Go To (machine name)** icon advances you to the source machine the user is logged into. This information can also be viewed by clicking the **Connection** icon in the **Current Sessions** widget.
- (**Widget Menu**): See Widget Menu for the functionality.

Information and Real-Time Data

The Display Protocol widget displays the following static and real-time information:

- **Send**: This shows the speed of the data packets that are being sent from the source machine to the destination device over the network.
- **Receive**: This shows the speed of the data packets that are being received by the source machine from the destination device over the network.
- **Client IP**: This shows the IP address of the user's machine (e.g., source: 172.17.21.6) that is logged into the machine and showing metrics within the widgets on the hosted Desktop. The IP address of the hosted Desktop (e.g., 10.30.41.156) is shown in the **Ethernet** widget.
- **User**: This shows the name of the user, which is also displayed in the **Current Sessions** widget.

- **Latency**: This shows the time it takes to pass data between the hosted and destination machines. This is the amount of time it takes for a data packet to travel from the source device to the destination device over a network.
- **Frame Quality**: This shows the percentage of successful Ethernet frames being passed between the hosted and destination machines in real-time.
- **Loss Rate**: This shows the amount of dropped packets, unstable connection, etc. that is causing a data loss between the source and destination machines in real-time.

Customize the Dashboard

The default CommandCTRL dashboard can be customized in two ways: you can add and remove the widgets on the screen, and you can customize the metrics that appear in some of the widgets.

Adding and Removing Widgets

All widgets on the dashboard can be added or removed at will.

To remove a widget, complete the following steps:

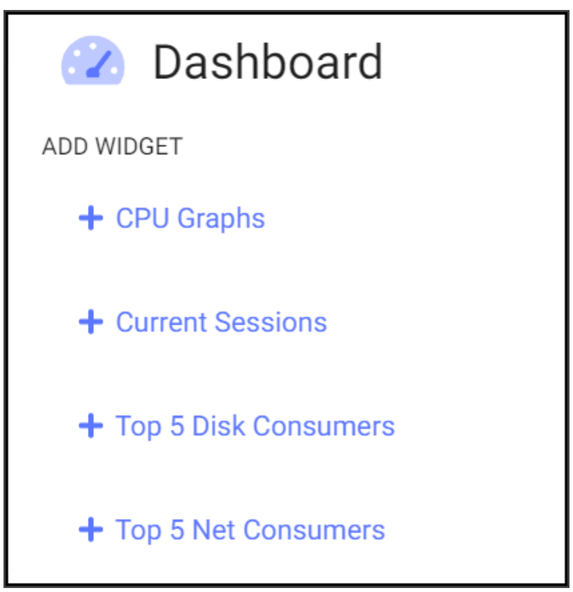
1. Click the ⋮ (**Widget Menu**) button in the top right corner of the widget.
2. Click the **Remove** option.

   The widget is then immediately removed from the dashboard.

To add a widget back to the dashboard, complete the following steps:

1. Click the (**Configuration**) icon in the bottom right corner of the screen.

   In the right sidebar menu that appears, all the widgets that have been removed from the dashboard appear under the **Dashboard** section.

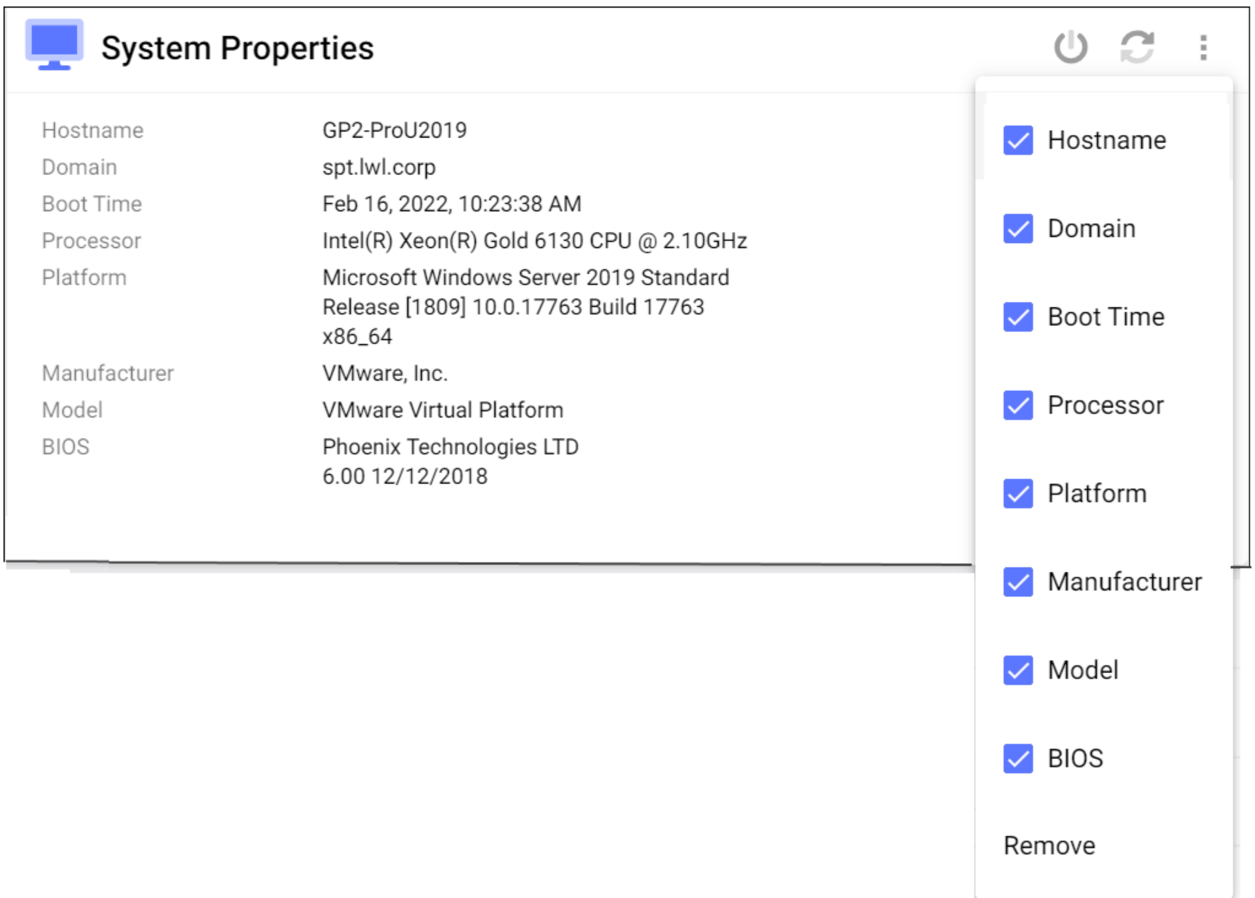
4. Click the name of each widget you want to add back to the dashboard.
   The corresponding widgets reappear immediately on the screen.

Customizing Widget Content

The contents of some widgets on the dashboard are customizable, allowing end users to view only the specific metrics in the widget that they want to see.

To customize the content of a widget, complete the following steps:

1. Click the ⋮ (**Widget Menu**) button in the top right corner of the widget.
2. A list of all of the widget's metrics appears.



> **Note:** If no metrics appear, the widget is not customizable.

5. Deselect each metric you want to hide and select each metric you want to display in the widget.
   The metrics are then immediately added to or removed from the widget.

Switch the Theme of the User Interface

To switch the theme currently displayed in the user interface, complete the following steps:

1. Click the (**Configuration**) icon in the bottom right corner of the screen.
2. In the right sidebar menu that appears, click the **Theme Style** you want to use for the user interface: **Light**, **Default**, or **Dark**.

Change the Display Density of the User Interface

To change the display density of the user interface in order to include more or less information in the same screen space, complete the following steps:

1. Click the (**Configuration**) icon in the bottom right corner of the screen.
2. In the right sidebar menu that appears, click the **Display Density** toggler to have the user interface display information in **Default** (normal spacing) or **Condensed** (narrow spacing) format.

Decline, Join, or Leave a Tenant

Decline an Invitation to Join a Tenant

While you are logged in to CommandCTRL, you can decline an invitation to join an additional tenant. To do so, complete the following steps:

1. Click your username in the top right corner of the screen.
2. Click **My Profile**.
3. In the **Tenants** field of the My Profile screen, locate the tenant you have been invited to join and click the **Decline** link.

Joining an Additional Tenant

When you are first invited to join CommandCTRL, you do not have access to the user interface, so you can only join it by accepting the email invitation you received. After you are granted access to the user interface, you can join additional tenants from within the CommandCTRL application.

1. Log in to CommandCTRL.
2. Look for a **Green Message** icon in the upper right and click it or click your **username** in the top right corner of the screen.
3. Click **My Profile**.
4. In the **Tenants** field of the My Profile screen, locate the tenant you have been invited to join and click the **Join** link.

Leaving a Tenant You Have Already Joined

After you are granted access to the user interface and more than one tenant, you can choose to leave any of the tenants you were granted access to from within the CommandCTRL application.

1. Log in to CommandCTRL.
2. Click your username in the top right corner of the screen.
3. Click **My Profile**.
4. In the **Tenants** field of the My Profile screen, locate the tenant you want to remove yourself from and click the **Leave** link.

Log In Using an Authenticator Application

CommandCTRL uses two-factor authentication (2FA) in the log in process and relies on an Authenticator application, such as Google Authenticator or Microsoft Authenticator, to grant users access to CommandCTRL.

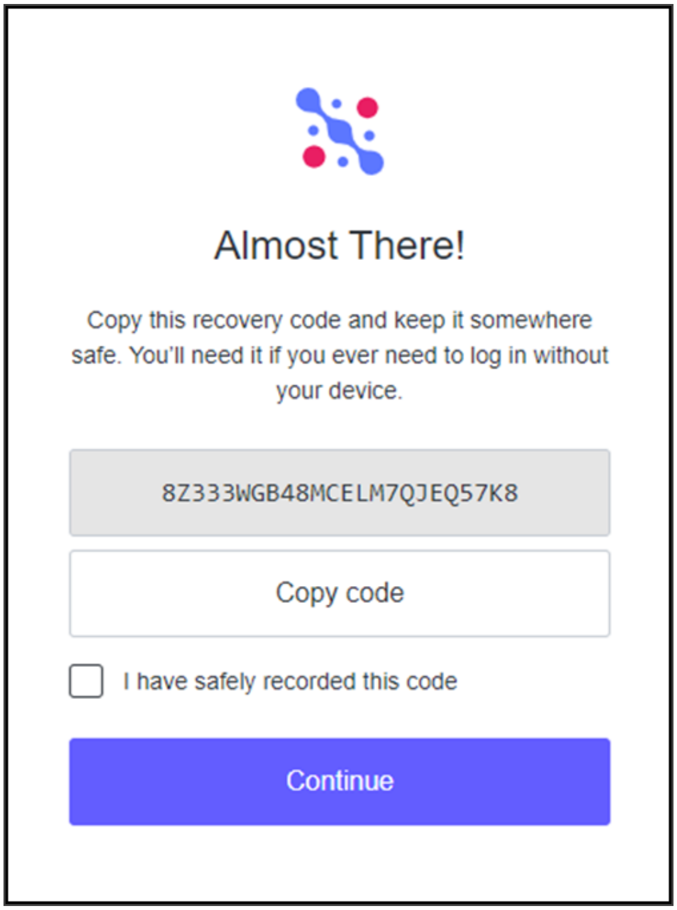
> **Note:** If you need to log in to CommandCTRL but you do not have access to the your mobile phone, you can log in using the recovery code that was generated for you when you first signed in to CommandCTRL. You could not complete that initial sign-in process without copying the code, so it should be located somewhere on your desktop or laptop.

To log in using an authenticator application, complete the following steps:

1. Click whatever link you use to launch CommandCTRL.
2. Enter your **email address** and **password**, then click the **Continue** button.
   The **Verify Your Identity** screen opens.
4. Open your authenticator app and note the current Liquidware access code displayed in it.
5. Enter the access code into the **Verify Your Identity** screen.
6. Click the **Continue** button.

Log In Using Your Recovery Code

If you want to log in to CommandCTRL but do not have access to your mobile phone in order to access the Authenticator app on it, you can log in using the recovery code that you were prompted to copy the first time you accessed CommandCTRL. The prompt you received at that time would have looked like the following:



To log in using your recovery code, complete the following steps:

1. Click whatever link you use to launch CommandCTRL.
2. Enter your **email address** and **password**.
3. Click the **Continue** button.
4. At the bottom of the **Verify Your Identity** screen, click the **Try another method** link.
5. On the Other Methods screen, click the **Recovery code** option.
6. On the updated **Verify Your Identity** screen that opens, enter your code, and then click the **Continue** button.

Agent-Related Tasks

View the Version Number and Hash for the Latest CommandCTRL Agent

To view the version number and hash for the latest CommandCTRL Agent, complete the following steps:

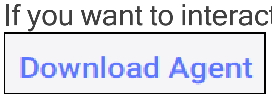
1. Open CommandCTRL.
2. In the side navigation panel, scroll down to the **Miscellaneous** section and click the **Install Agent** button.

   The latest version and latest hash are listed at the top of the screen in the **Latest Agent** field.

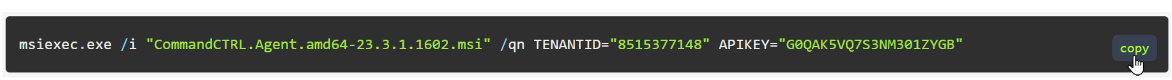
Install the CommandCTRL Agent on a Single Machine

Installing the Agent

The MSI installer allows for easy deployment using any software distribution solution like Microsoft End Point Manager or any other software distribution tools or solutions on the market. A command line for silent installation is also available under the install agent section. To install the CommandCTRL Agent on a single machine, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, scroll down to the **Miscellaneous** section and click the **Install Agent** button.
3. Search for the installation instructions for the Windows operating system.
4. In the **Windows** section, either:
   a. If you want to interactively (not silent) install the MSI on a machine, click 

   to save the MSI to your machine.
   b. If you want to silently install the MSI on a machine, click **Copy** to copy the MSI link. For example, `msiexec.exe /i "\\server-\share\CommandCTRL.Agent.amd64-xx.x.xx.xxxx.msi" /qn TENANTID="xxxxxxxxxx" APIKEY="xxxxxxxxxxxxxxx"`. Install = /i and quiet = /qn.



To enable or disable automatic updates, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Agent Settings** section, the enable/disable switch located to the far right. The default is set to enable. It is recommended to accept automatic updates; however, this switch allows users the ability to control when the agent is updated.
3. Either leave the switch enabled or slide the switch to the left to disable the agent from automatically updating.

Install the CommandCTRL Agent on Multiple Machines

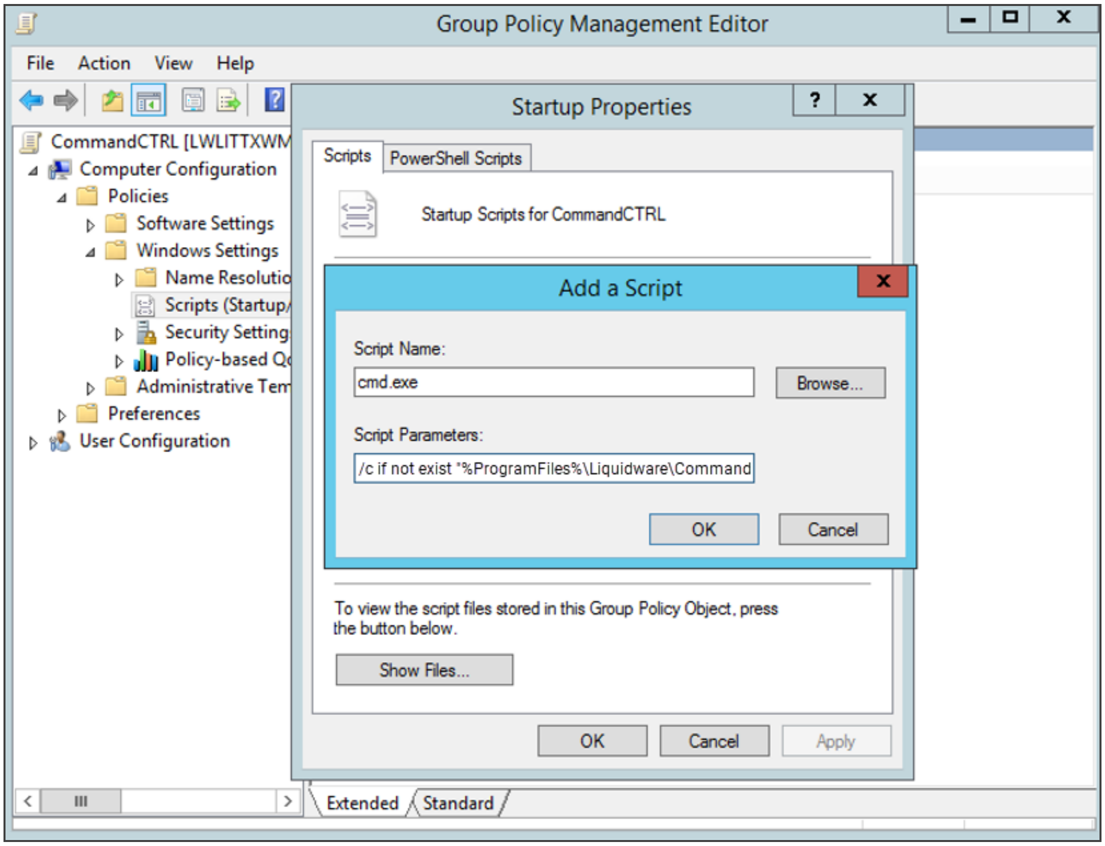
Installing the Agent

The MSI installer allows for easy deployment using any software distribution solution like Microsoft End Point Manager or any other software distribution tools or solutions on the market. A command line for silent installation is also available under the install agent section. To install the Agent on multiple machines simultaneously you would pick a method that allows for mass distribution like using the computer startup script method below. To accomplish this, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, scroll down to the **Miscellaneous** section and click the **Install Agent** button.
3. Search for the installation instructions for the Windows operating system.
4. In the **Windows** section, either:
   a. If you want to interactively (not silent) install the MSI on multiple machines, click Download Agent to save the MSI to your machine.
   b. If you want to silently install the MSI on a machine, click **Copy** to copy the MSI link. For example, `msiexec.exe /i "\\server-\share\CommandCTRL.Agent.amd64-xx.x.xx.xxxx.msi" /qn TENANTID="xxxxxxxxxx" APIKEY="xxxxxxxxxxxxxxx"`. Install = /i and quiet = /qn.

```
msiexec.exe /i "CommandCTRL.Agent.amd64-23.3.1.1602.msi" /qn TENANTID="8515377148" APIKEY="G0QAK5VQ7S3NM301ZYGB"        copy
```

5. After the MSI exists on the network, you can set this script to run at computer startup using the Group Policy Management Editor. Be sure the group policy object (GPO) exists in the computer organizational unit (OU) where you want the Agent to be installed. Go to:
   `Computer Configuration >Polices > Windows Settings > Scripts (Startup/Shutdown) > Startup - Add`
7. On the **Add a Script** screen that pops up, enter `cmd.exe` in the **Script Name** field.



9. In the **Script Parameters** field, enter:

   ```
   /c if not exist "%ProgramFiles%\Liquidware\CommandCtrl\ccagent.exe" msiex-
   ec.exe /i "\\server\share\CommandCTRL.Agent.amd64-xx.x.xx.xxxx.msi" /qn
   TENANTID="xxxxxxxxxx" APIKEY="xxxxxxxxxxxxxxx"
   ```

11. Install the Agent directly into the base image if it is a hosted desktop like VMware, Citrix, Frame, AVD. Or use the **GPO on startup script** option mentioned above.
12. Use Microsoft End point manager for deploying to machines in the field.

To enable or disable automatic updates, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Agent Settings** section, the enable/disable switch located to the far right. The default is set to enable . It is recommended to accept automatic updates; however, this switch allows users the ability to control when the agent is updated.
3. Either leave the switch enabled or slide the switch to the left to disable the agent from automatically updating.

Install the CommandCTRL Agent on a Mac Machine

Installing the Agent

This is for installing the agent on a single or multiple Mac machines.

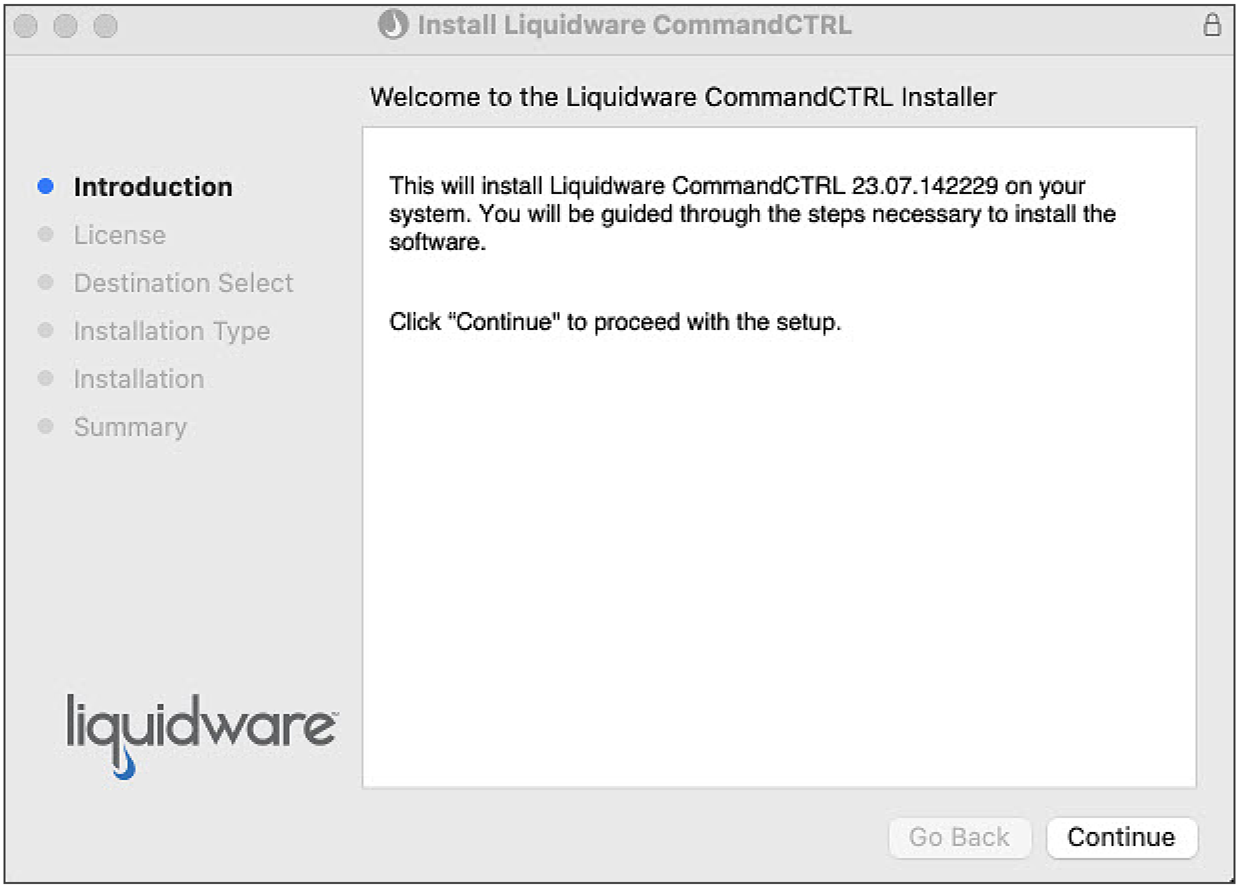
1. Download the most recent mac agent .DMG file from the CommandCTRL console.

The **CommandCTRL.pkg** appears on the desktop.

3. Launch the **CommandCTRL.pkg**.

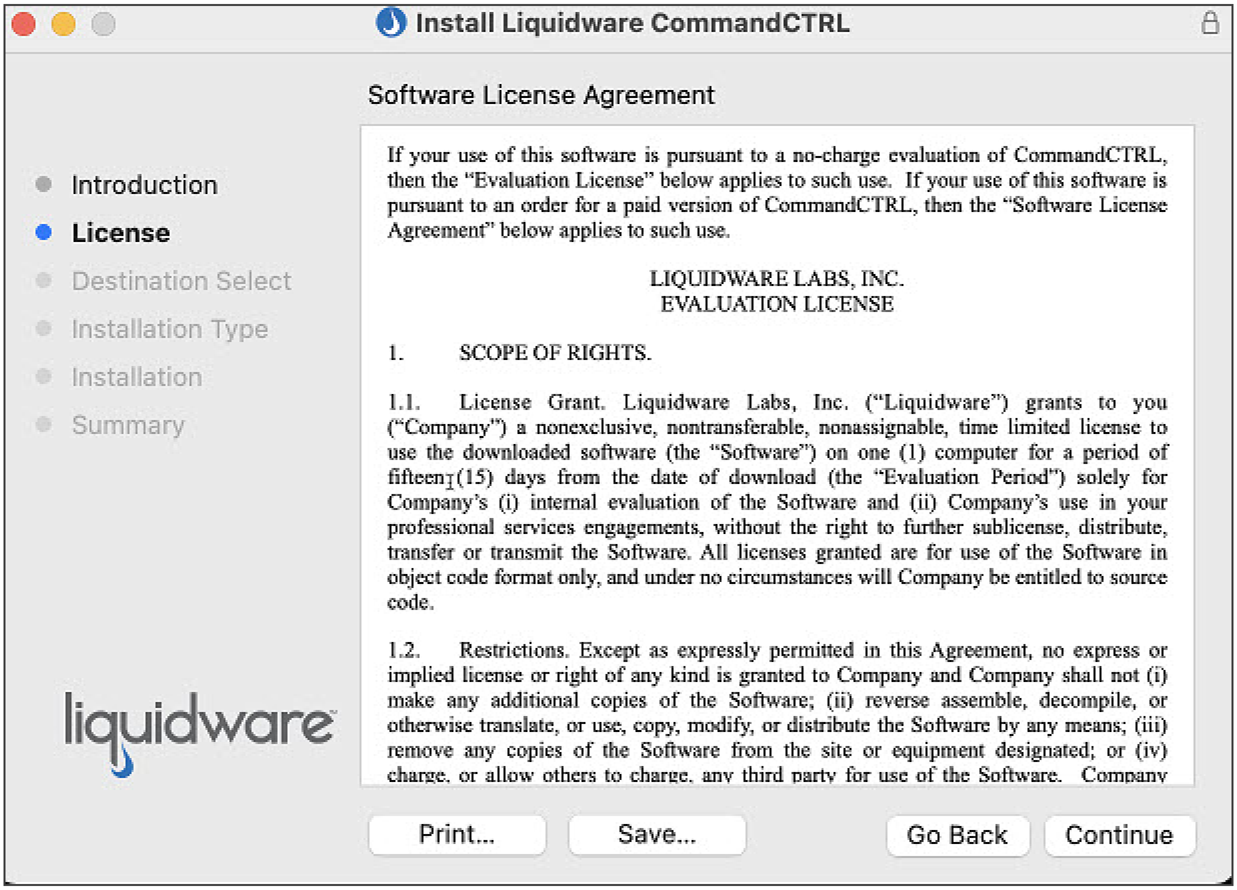
The CommandCTRL installer **Introduction** dialog box appears.

5. Click **Continue**.



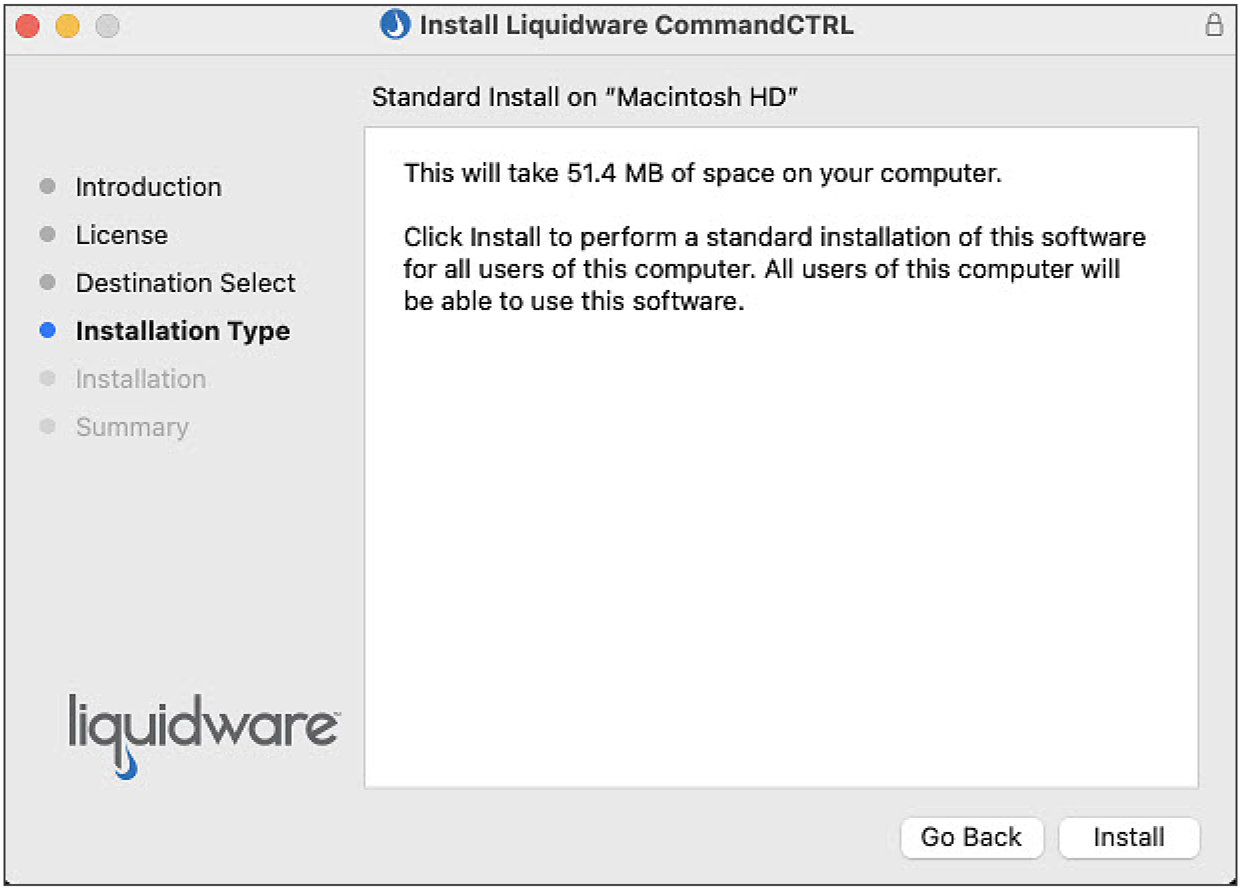
The CommandCTRL installer **License** agreement dialog box appears.

7. Click **Continue**.

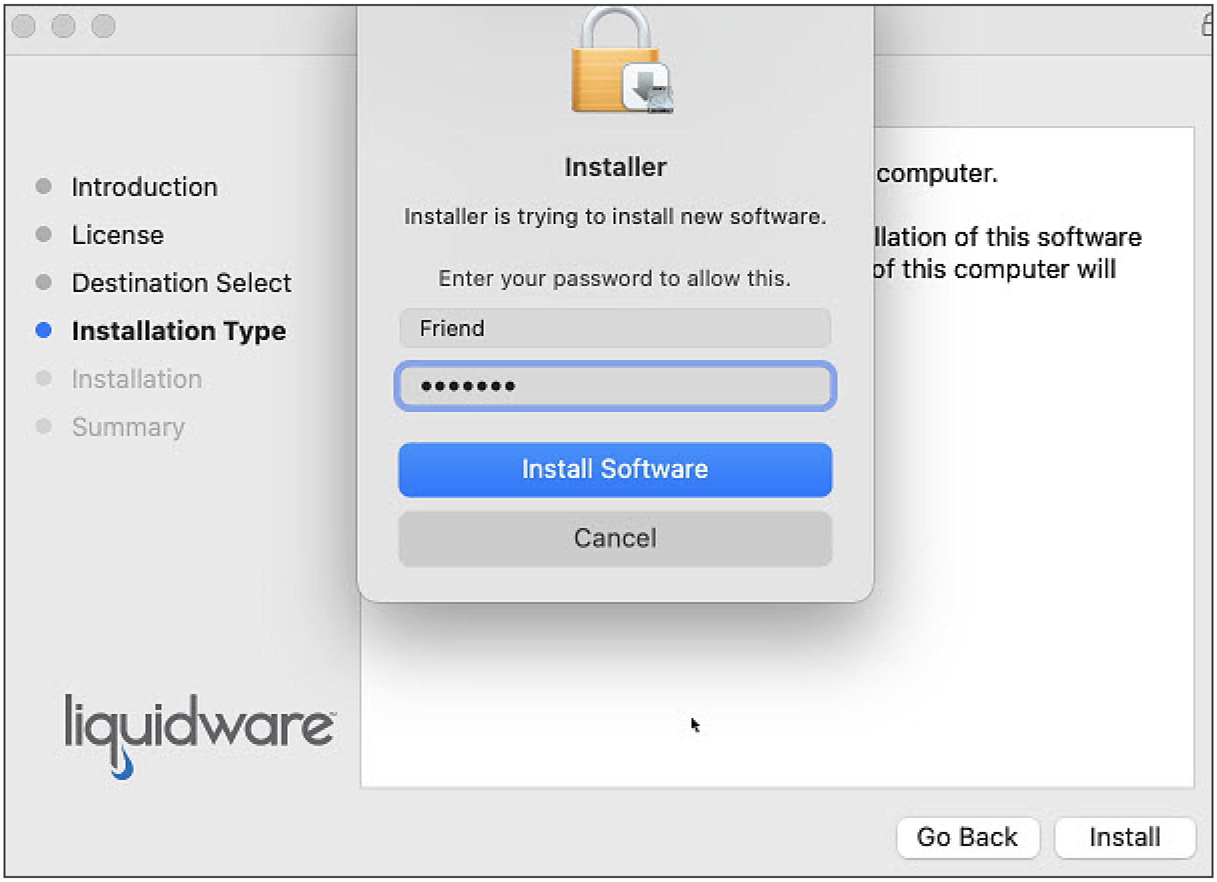


The CommandCTRL installer **Installation Type** dialog box appears.

9. Click **Install**.

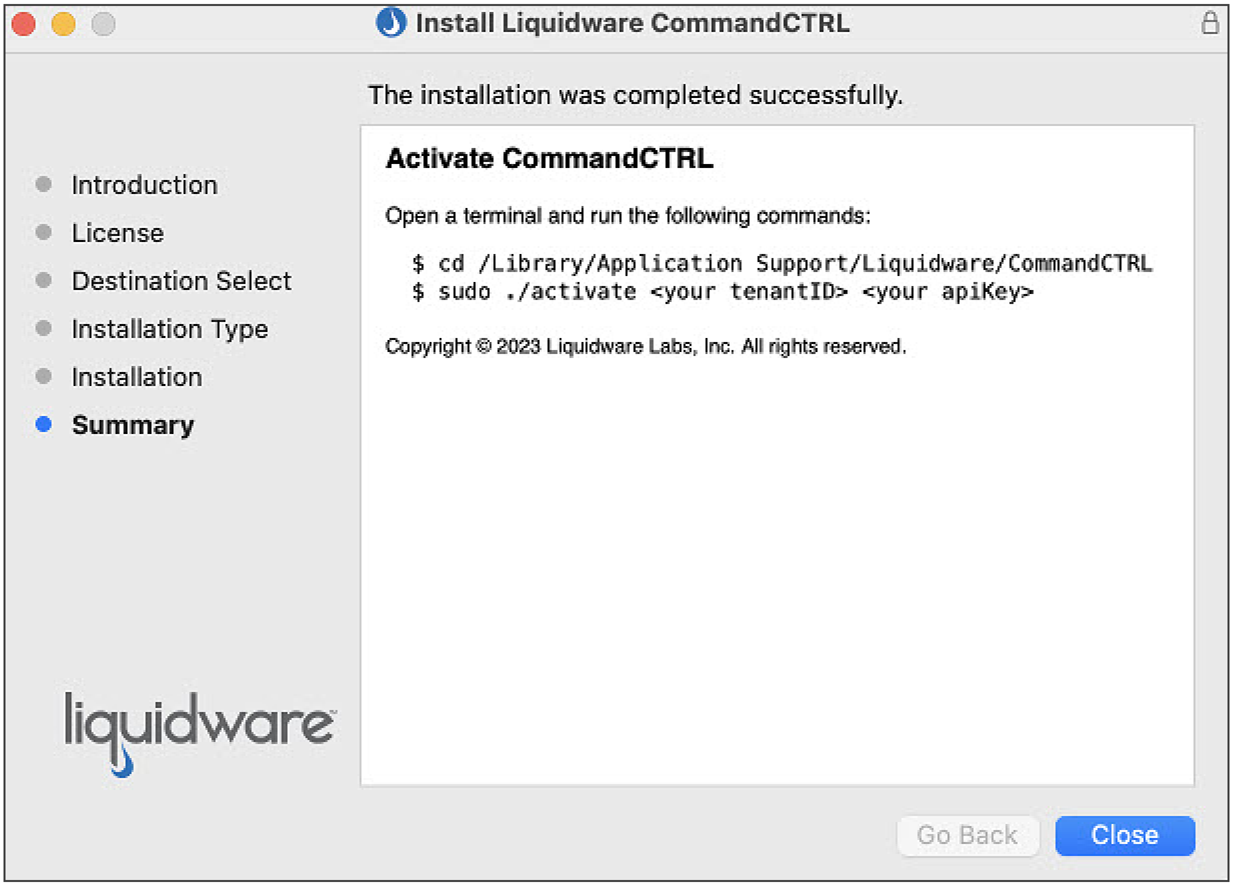


11. Enter the password you use to log into that machine.

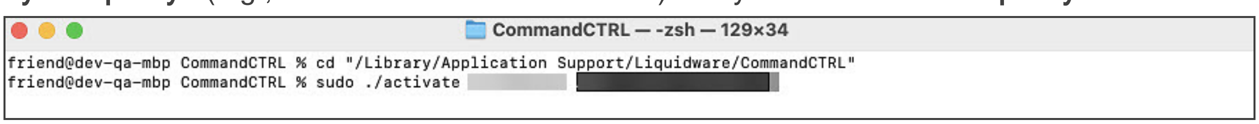


The CommandCTRL installer **Summary** dialog box appears.

13. Click **Close**.



15. Open a terminal window.
16. Change the CommandCTRL install path as shown in the first command line of the previous screen to where CommandCTRL resides in your environment.
17. Press the **Enter** key.
18. The second command line in the previous screen displays <your tenantID> and <your apiKey>. Install the CommandCTRL service as **Root** and replace **<your tenantID**> (e.g., 6274957583) and **<your apiKey>** (e.g., AWBCT2CUSR79AB7N8L9J) with your **tenant ID** and **api key**.



20. Press the **Enter** key.

    The command is executed and the following screen shows the agent was successfully installed.

```
CommandCTRL — -zsh — 129x34
friend@dev-qa-mbp CommandCTRL % cd "/Library/Application Support/Liquidware/CommandCTRL"
friend@dev-qa-mbp CommandCTRL % sudo ./activate [redacted]
Password:
[2023-08-17 18:55:20][INFO] Agent configuration process started
[2023-08-17 18:55:20][INFO] Successfully created agent configuration file
[2023-08-17 18:55:20][INFO] Successfully stopped agent
[2023-08-17 18:55:20][INFO] Successfully started agent
[2023-08-17 18:55:20][INFO] Agent configuration process finished
friend@dev-qa-mbp CommandCTRL %
```

To enable or disable automatic updates, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Agent Settings** section, the enable/disable switch located to the far right. The default is set to enable. It is recommended to accept automatic updates; however, this switch allows users the ability to control when the agent is updated.
3. Either leave the switch enabled or slide the switch to the left to disable the agent from automatically updating.

Update the CommandCTRL Agent on a Single Machine

Update the Agent

The MSI installer allows for easy deployment using any software distribution solution like Microsoft End Point Manager or any other software distribution tools or solutions on the market. A command line for silent installation is also available under the install agent section. To update the CommandCTRL Agent on a single machine, complete the following steps:

> **Note:** If you already have the agent installed on a machine and you are updating the agent interactively (not silent), the **Tenant ID** and **API Key** fields will automatically populate in the Settings dialog box.

1. Open CommandCTRL.
2. In the side navigation panel, scroll down to the **Miscellaneous** section and click the **Install Agent** button.
3. Search for the update instructions for the Windows operating system.
4. In the **Windows** section, if you want to either:
   - Interactively (not silent) install the MSI on a machine, click Download Agent to save the MSI to your machine.

- Silently install the MSI on a machine, click **Copy** to copy the MSI link. For example, `msiexec.exe /i "\\server\share\CommandCTRL.Agent.amd64-xx.x.xx.xxxx.msi" /qn TENANTID="xxxxxxxxxx" APIKEY="xxxxxxxxxxxxxxx"`. Install = /i and quiet = /qn.

```
msiexec.exe /i "CommandCTRL.Agent.amd64-23.3.1.1602.msi" /qn TENANTID="8515377148" APIKEY="G0QAK5VQ7S3NM301ZYGB"
```
copy

To enable or disable automatic updates, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Agent Settings** section, the enable/disable switch located to the far right. The default is set to enable. It is recommended to accept automatic updates; however, this switch allows users the ability to control when the agent is updated.
3. Either leave the switch enabled or slide the switch to the left to disable the agent from automatically updating.

Update the CommandCTRL Agent on Multiple Machines

Update the Agent

The MSI installer allows for easy deployment using any software distribution solution like Microsoft End Point Manager or any other software distribution tools or solutions on the market. A command line for silent installation is also available under the install agent section. If you initially installed the CommandCTRL Agent on multiple machines using the script provided by Liquidware, the Agent will update automatically whenever a new version is released. There is no need to manually update the software.

> **Note:** If you already have the agent installed on a machine and you are updating the agent interactively (not silent), the **Tenant ID** and **API Key** fields will automatically populate in the Settings dialog box.

To enable or disable automatic updates, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Agent Settings** section, the enable/disable switch located to the far right. The default is set to enable. It is recommended to accept automatic updates; however, this switch allows users the ability to control when the agent is updated.
3. Either leave the switch enabled or slide the switch to the left to disable the agent from automatically updating.

Update the CommandCTRL Agent on a Mac Machine

Update the Agent

This is for updating the agent on a single or multiple Mac machines.

To enable or disable automatic updates, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Agent Settings** section, the enable/disable switch located to the far right. The default is set to enable. It is recommended to accept automatic updates; however, this switch allows users the ability to control when the agent is updated.
3. Either leave the switch enabled or slide the switch to the left to disable the agent from automatically updating.

Uninstall the CommandCTRL Agent on a Single Machine

CommandCTRL collects historical metrics for each machine. After the CommandCTRL Agent has been uninstalled from a machine, no additional metrics will be collected.

Uninstall Using the Command Line Method

To uninstall the CommandCTRL Agent from a single machine, follow the Windows procedure for removing an application.

Uninstall Using the CommandCTRL Method

To use CommandCTRL to remove an agent from a single machine, follow the same procedure in Uninstall the CommandCTRL Agent on Multiple Machines.

Uninstall the CommandCTRL Agent on Multiple Machines

CommandCTRL collects historical metrics for each machine. After the CommandCTRL Agent has been uninstalled from a machine, no additional metrics will be collected.

Uninstall Using the CommandCTRL Method

To uninstall the Agent on multiple machines simultaneously, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, select the checkboxes beside each of the machines that you want to uninstall the Agent from.
3. In the top right corner of the header, click the (**Remove License**) button.

4. On the **Unlicense Machine** screen that pops up, select the **Block Indefinitely** radio button.
5. Click the **Do Not Uninstall Agents** toggler to switch it to **Uninstall Agents**.
6. Click the **Block Machines** button to uninstall the Agent on each machine and block them all from interacting with CommandCTRL.

Uninstall the CommandCTRL Agent on a Mac Machine

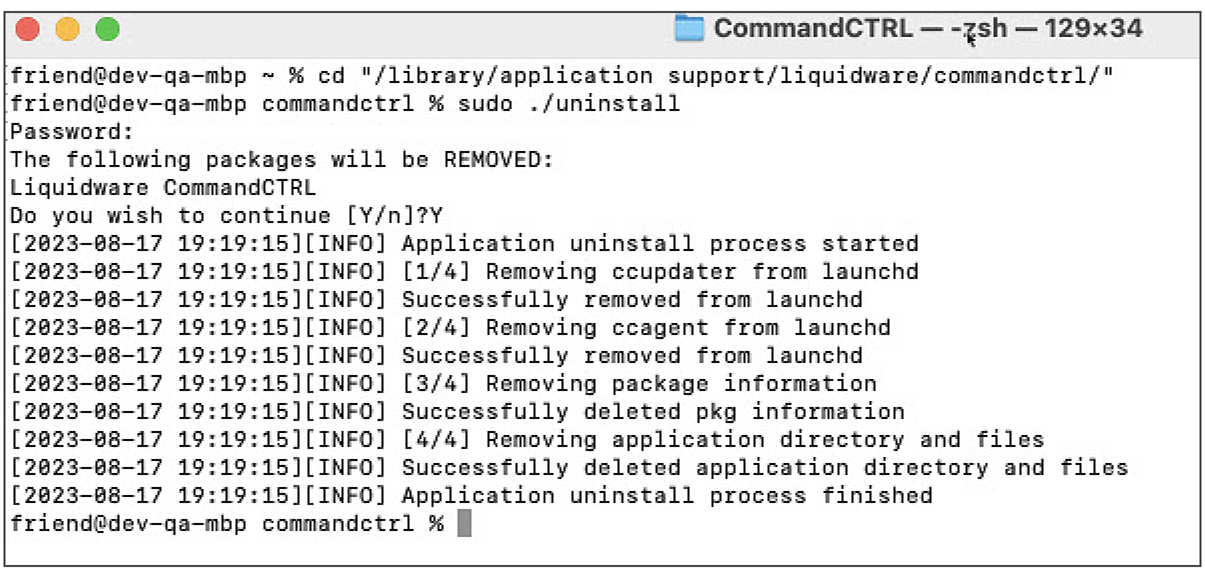
CommandCTRL collects historical metrics for each machine. After the CommandCTRL Agent has been uninstalled from a machine, no additional metrics will be collected.

Uninstall Using the Command Line Method

This is for uninstalling the agent on a single or multiple Mac machines using a command line method.

1. Open a terminal window.
2. Navigate to the path where CommandCTRL is currently installed in your environment, as shown in the first command line of the following screen.
3. Press the **Enter** key.
4. Type the **uninstall** command as Root, as shown in the second command line of the following screen.
5. Press the **Enter** key.
6. Type **Y** (yes) to accept continuing to remove the agent.

   The command is executed and the following screen shows the agent was successfully uninstalled.




```
friend@dev-qa-mbp ~ % cd "/library/application support/liquidware/commandctrl/"
friend@dev-qa-mbp commandctrl % sudo ./uninstall
Password:
The following packages will be REMOVED:
Liquidware CommandCTRL
Do you wish to continue [Y/n]?Y
[2023-08-17 19:19:15][INFO] Application uninstall process started
[2023-08-17 19:19:15][INFO] [1/4] Removing ccupdater from launchd
[2023-08-17 19:19:15][INFO] Successfully removed from launchd
[2023-08-17 19:19:15][INFO] [2/4] Removing ccagent from launchd
[2023-08-17 19:19:15][INFO] Successfully removed from launchd
[2023-08-17 19:19:15][INFO] [3/4] Removing package information
[2023-08-17 19:19:15][INFO] Successfully deleted pkg information
[2023-08-17 19:19:15][INFO] [4/4] Removing application directory and files
[2023-08-17 19:19:15][INFO] Successfully deleted application directory and files
[2023-08-17 19:19:15][INFO] Application uninstall process finished
friend@dev-qa-mbp commandctrl %
```

Uninstall Using the CommandCTRL Method

To use CommandCTRL to remove an agent from a single machine, follow the same procedure in Uninstall the CommandCTRL Agent on Multiple Machines.

Administrative Tasks

Create a Custom User Role

Note: This functionality is only available to Admin and Owner users.

In CommandCTRL, it is possible to create a new user role and then assign a customized set of permissions to it. After the role is created, it persists in the system and can be assigned to other users.

To create a custom user role, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Roles**.
3. Click the (**Add Role**) button in the top right corner of the **Roles** screen.
4. On the **New Role** screen that pops up, enter an **ID** for the new role.
5. Enter a **Name** for the new role.
6. (Optional) Enter a **Description** for the new role. Although you do not have to fill in this field, the information in it can help other Admin/Owner users determine if the role should be assigned to any new users they are creating in the system or if they should create their own new role.
7. Click inside the **Permissions** field, and then click to select all of the permissions that you want to associate with the new user role.
8. When you are done, click the **Create** button.

   The new role then appears in the list on the **Roles** screen.

Modify a Custom User Role

Note: This functionality is only available to Admin and Owner users.

Within CommandCTRL, you can make changes to any custom role that has been created. You cannot, however, modify the out-of-the-box Owner, Administrator, or User roles.

To modify a custom user role, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Roles**.
3. Click the name of the custom role that you want to modify.
4. On the screen that pops up, make changes to any of the fields on the screen other than **ID**. The ID field cannot be modified after the role has been created.
5. When you are done, click the **Save Changes** button.
6. If the role **is not assigned** to any user in the system, the changes are implemented immediately.

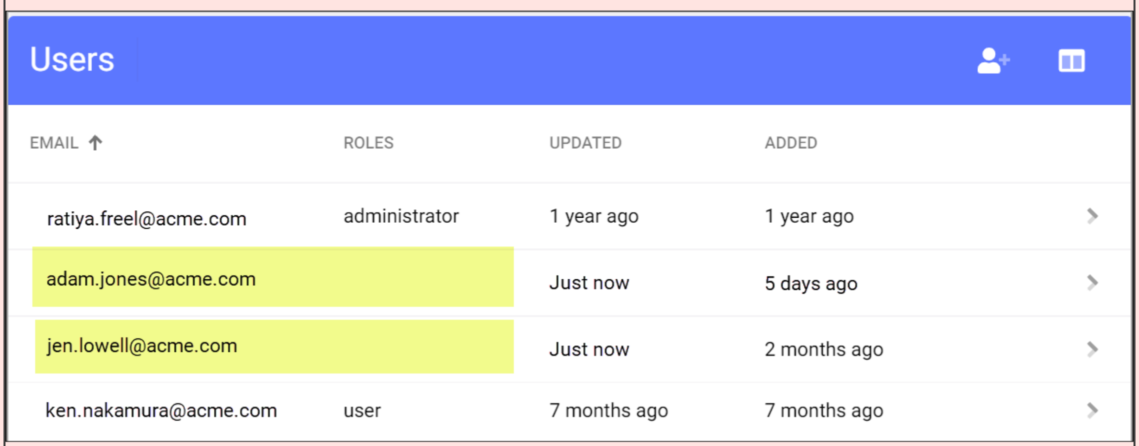
If the role **is assigned** to one or more users in the system, a screen pops up, informing you that "Doing this may influence users." Click **Confirm** to roll out the changes to the role. Users who are associated with the modified role will see the changes the next time they refresh their screen (if they are currently logged in to CommandCTRL) or the next time they log in (if they are currently offline).

Delete a Custom User Role

Note: This functionality is only available to Admin and Owner users.

In CommandCTRL, you cannot delete the Owner, Administrator, and User roles that are provided out-of-the-box. You can, however, delete any custom user roles that you or other Admins or Owners have created.

Important: If a user is assigned to only one role and you delete that role, the user loses the ability to do anything in the system. You can identify these role-less users by opening the **Users** screen and searching for blank entries in the **Roles** column.



To remedy this situation, click each user's name and then assign them to an existing role.

To delete a custom role, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Roles**.
3. Click the name of the role you want to delete.
4. On the popup screen that opens, click the **Delete** button.
5. A screen pops up, informing you that "Doing this may influence users." Click **Confirm** to proceed with the deletion of the role.

Invite a User to Join a Tenant

Note: This functionality is only available to Admin and Owner users.

To add a user to CommandCTRL, you first invite them via email and then they accept your invitation. To do this, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Users**.
3. On the **Users** screen that opens, click the (**Add User**) button in the top right corner of the header.
4. On the **New User** screen that pops up, enter the email address for the user you want to invite.
5. Select a role for the new user: **Administrator**, **User**, or one of the custom roles that has been created for your tenant. If the user is assigned the system Administrator role, that role contains all permissions, so it overrides all other roles and role restrictions that are assigned to the user.
6. Click the **Invite** button.

   An email is then sent to the user, inviting them to become part of the tenant.

Resend an Invitation to Join a Tenant

If a user has not yet replied to an invitation to join a tenant, you can resend the invitation by completing the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Users**.
3. In the Invites table that appears, locate the user you want to resend an invitation to and click the (**Resend Invite**) button to the right of their name.

Delete an Invitation to Join a Tenant

If a user has not yet replied to an invitation to join a tenant, you can rescind that invitation by completing the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Users**.
3. In the Invites table that appears, locate the user whose invitation you want to rescind and click the (**Delete Invite**) button to the right of their name.

Change a User's Role

Note: This functionality is only available to Admin and Owner users.

To change the role assigned to a user in CommandCTRL, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Users**.
3. In the Users table that appears, locate the user's email address and click it.
4. On the user details screen that pops up, do one of the following:
    - Click the **X** icon beside the user's current role to remove it, then select a new role from the **Roles** drop-down list.
    - Keep the user's existing role and add an additional one by clicking the **assign role...** link and selecting from the role list that appears. If the user is assigned the system Administrator role, that role contains all permissions, so it overrides all other roles and role restrictions that are assigned to the user.
5. Click the **Save Changes** button.

Change a User's Email Address

You cannot change a user's email address within CommandCTRL. If a user's email address changes, you must first delete the user from the system, then send them a new invitation using their new email address.

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Users**.
3. In the Users table that appears, locate the user's email address and click it.
4. On the user details screen that pops up, click the **Delete** button.
5. On the **Users** screen, click the  (**Invite User**) button in the top right corner of the header.
6. On the **Invite User** screen that pops up, enter the new email address for the user.
7. Click **Roles** and select an **Administrator**, **User**, or one of the custom roles that has been created for your tenant. If the user is assigned the system Administrator role, that role contains all permissions, so it overrides all other roles and role restrictions that are assigned to the user.
8. Click the **Invite** button.

    An email is sent to the user, inviting them to become part of the tenant again.

View the API Key for a Tenant

To view the API key associated with a tenant, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Site**.

The tenant's API key is listed in the **API Keys** table.

Share Usability Workflows

This allows the tenant to share usability workflows with Liquidware. This will allow Liquidware to better support the CommandCTRL application. To view the tenant's share usability workflows setting, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Site**.
3. In the **Share Usability Workflows** section, enable or disable the switch located to the far right.

> **Note:** It is recommended to leave the switch enabled so usability workflows are shared with Liquidware.

View the Number of Machine Licenses Used

Within CommandCTRL, licenses are assigned to machines, not to users. So a user who has CommandCTRL installed on three machines is using three licenses, not one.

Within the 30-day period, once a machine registers, the agent is installed and the machine is given its API key. The first time the machine calls home, a license is given to that machine. That license is deducted from the total number of licenses that are available.

As long as the machine is active, it will retain the license it was given. If the machine has not been active in 30 days (machine is turned off, offline, etc.), then CommandCTRL will release the license and add it back to the pool of available licenses for the tenant. The agent will still be installed on the machine. The next time the agent calls back to the CommandCTRL console, it will attempt to reclaim another license.

To view the number of licenses a tenant has used, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Tenant**.

   The **Company** tab is the landing page.

3. The **Subscription** line under **Profile** displays the:
   - Total number of licenses (**Claimed**).
   - Type of plan purchased (e.g., Standard Monthly Plan).
   - Next Billing date.
   - Limit, which is the total number of licenses purchased (e.g., 100).

- Status of the tenant (e.g., In-Trail).
- Number of days remaining in the subscription.

View the Renewal Date of a Tenant's Subscription

To view the renewal date of a tenant's subscription, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Settings** > **Tenant**.

   The **Subscription** line in the Profile field displays the **Next Billing** date of the tenant's subscription, which corresponds to the renewal date.

Add a Tenant

To add a tenant, complete the following steps:

> **Note:** You can add up to five tenants. The name of the tenant must be at least three characters and begin with a letter. The tenant you create is a trial. If the trial has expired, the tenant becomes inactive or your subscription has expired, the tenant will no longer be available after 90 days. Within the 90-day period, you can reactivate that tenant. After 30 additional days (90 + 30 = 120 days), the system purges the tenant and all agents that remain associated with that tenant will automatically be uninstalled.

1. Click your user profile icon in the top right corner of the CommandCTRL screen.
2. In the drop-down field that appears, click the **My Profile** option.
3. In the **Tenants** area, on the far right, click **New**.

   The **New Tenant** dialog box appears.

4. Click in the **Name** field.

   A drop-down appears with a list of names you can select.

5. Select a name from the drop-down or type a name in the field.
6. Click **Submit**.

Integrating CommandCTRL with OpenAI

CommandCTRL has been designed to allow integration with OpenAI’s API in order to leverage the large language models (LLMs) for more information on what is running on a machine in your environment. When looking at a list of processes on a machine, you can query OpenAI for the manufacturer and a description based on the process name. CommandCTRL currently utilizes four of OpenAI’s GPT models.

If you want to integrate CommandCTRL with one of the four OpenAI's GPT models you will need to have an OpenAI account. This will provide you with their API (Application Programming Interface) Key and Organization ID, which allows developers to integrate the model's natural language processing capabilities into applications or services. The cost of using OpenAI's API Key and Organization ID depends on various factors, such as the level of usage, the number of API requests, and the specific use case.

> **Note:** OpenAI charges a subscription and a fee for data (see OpenAI.com for their fee structure). Our integration was designed to help save you money by caching their information for 90 days. When anyone in your tenant clicks on the OpenAI icon, the information they provide is saved to cache and is available whenever anyone else in your tenant requests the same information within 90 days. After 90 days, it is assumed that the information needs to be refreshed since information is always changing.

> **Note:** These following procedures are intended to help you navigate OpenAI's website so you can open an account, get your Organization ID, and generate an API Key. At the time of publishing, these procedures were correct. Since Liquidware has no control over OpenAI's website, it is possible they might have changed their instructions and links.

Create an OpenAI Account

To create an OpenAI account, complete the following steps:

1. Navigate to OpenAI.com.
2. In the upper right corner of the page, click the Sign up ↗ icon.

   You are advanced to a **Create your account** page where you can enter all the necessary information needed to be able to open an account.

Retrieve your OpenAI Organization ID and API Key

This will guide you through the steps needed to retrieve your Organization ID, generate your API Key, and add both to CommandCTRL.

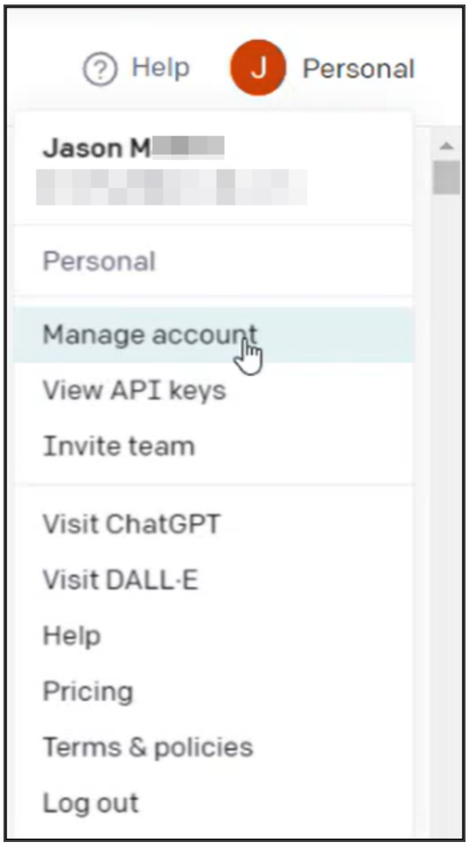
Get your Organization ID

To retrieve your Organization ID and add it to CommandCTRL, complete the following steps:

1. After completing Create an OpenAI Account, click your **User** icon in the upper right corner of the page.

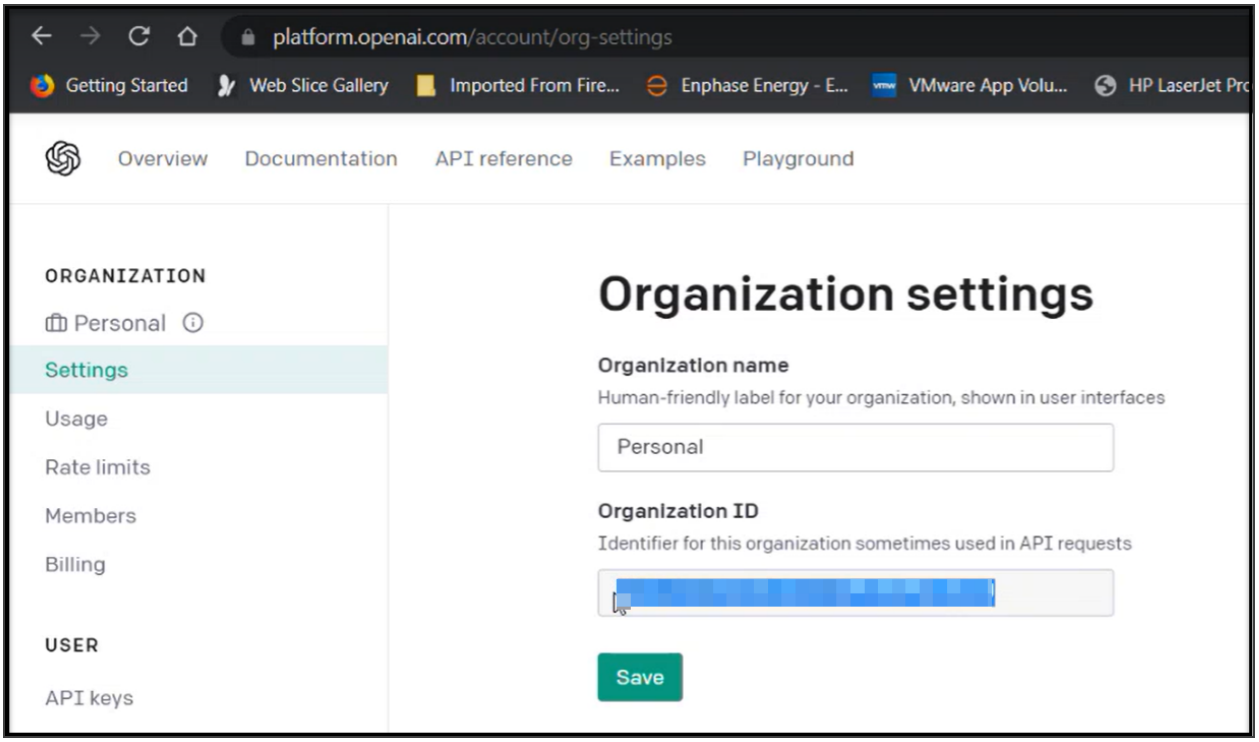
   A **User** account drop-down appears.

2. Select **Manage Account** from the drop-down list.



   The **Organization settings** page appears. Your **Organization ID** is in the field.

   You can also click this link to go directly to the **Organization settings** page but you will need to authenticate to access the page.



3. Click the **Save** button to copy your **Organization ID**.
4. Navigate to CommandCTRL.
5. In CommandCTRL's side navigation panel, go to **Settings** > **Site** and locate the **3rd Party APIs** widget.

6. In the **3rd Party APIs** widget, paste your OpenAI **Organization ID** in the field.

   The check mark to the far right of the field changes color from gray to green.

7. Click the check mark to accept the **Organization ID**.

   The check mark to the far right of the field changes color from green to gray and the **Clear** button highlights to show it accepted your **Organization ID**.

The **Organization ID** is hidden and replaced with text (i.e., OpenAI).

If you click the **Clear** button your **Organization ID** is removed from the field and the **Clear** button is no longer highlighted.

8. Pick your **OpenAI Model**:

   GPT-3.5-Turbo-0125

   Overview: This model is an intermediate version between GPT-3 and GPT-4, offering improved performance and cost-efficiency. It is particularly effective for applications requiring advanced language understanding but where the top-tier model (GPT-4) may not be necessary.

   Features: GPT-3.5-Turbo-0125 is designed to be faster and more cost-effective while still delivering significantly better performance than GPT-3, especially in tasks that involve nuanced language understanding and more complex problem-solving abilities.

   GPT-4

   Overview: GPT-4 is a large multimodal model (capable of processing both text and image inputs) that represents a major advancement in terms of reasoning and deeper contextual understanding compared to its predecessors.

   Features: Known for its broad general knowledge and problem-solving capabilities, GPT-4 can generate more relevant and contextually appropriate responses. It excels in tasks that require understanding intricate details and generating outputs that are coherent over long stretches of text.

   GPT-4-Turbo-Preview

   Overview: This is a preview version of the upcoming GPT-4-Turbo, designed to offer stakeholders a glimpse into the enhanced capabilities and optimizations of the full GPT-4-Turbo model.

   Features: While still in a preview phase, this model showcases improvements in processing speed and efficiency. The responses are quicker and may include optimizations in understanding and generating text, which are being tested for feedback before the final release.

GPT-4-Turbo

Overview: GPT-4-Turbo is an optimized version of GPT-4, designed to provide faster response times and higher efficiency while maintaining or improving the quality of output provided by GPT-4.

Features: This model integrates enhancements that make it suitable for high-demand environments where speed and accuracy are critical. It is ideal for enterprise-scale applications, providing quick, accurate responses and handling a high volume of requests seamlessly.

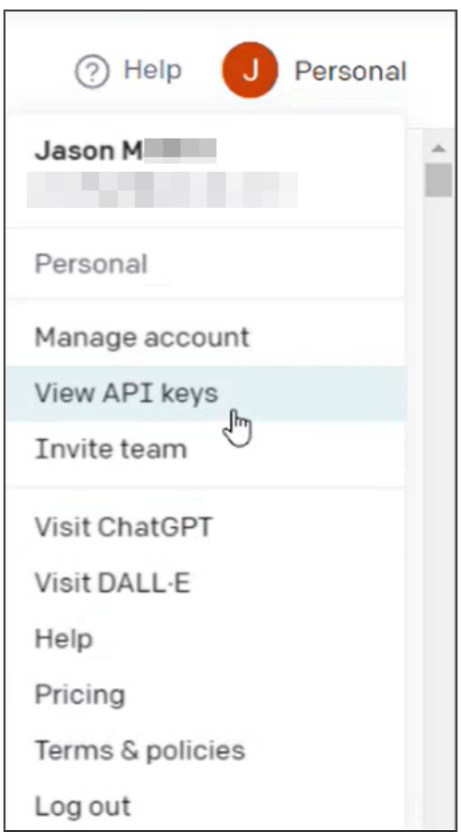
Generate your API Key

To generate your API Key and add it to CommandCTRL, complete the following steps:

1. After completing Create an OpenAI Account, click your **User** icon in the upper right corner of the page.

   A **User** account drop-down appears.

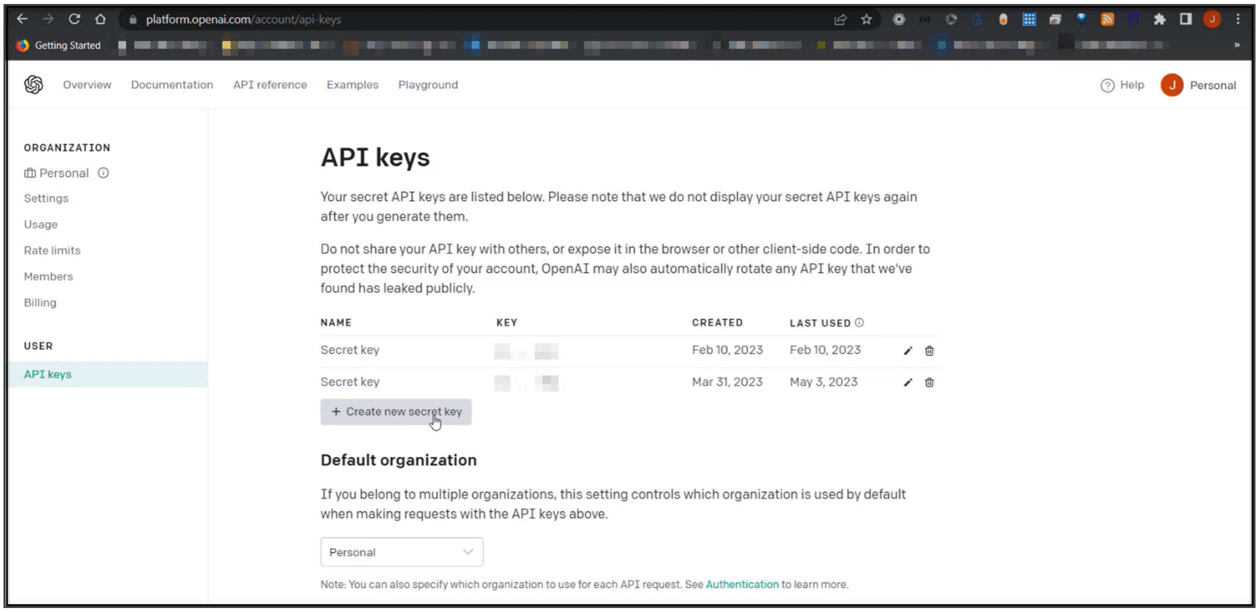
2. Select **View API keys** from the drop-down list.



The **API keys** page appears. Liquidware recommends that you create a separate API key for

CommandCTRL.

You can also click this link to go directly to the **API keys** page but you will need to authenticate to access the page.



3. Click the **Create new secret key** button to generate a new **Key**.

> **Note:** OpenAI calls their **API Key** a **Secret Key**.

5. Copy your **API key** from the **Key** column.

> **Important:** OpenAI will allow you to only copy the **Key** once. If you want to change Keys periodically, you can create a new **Key** and rotate/replace the Key in CommandCTRL.

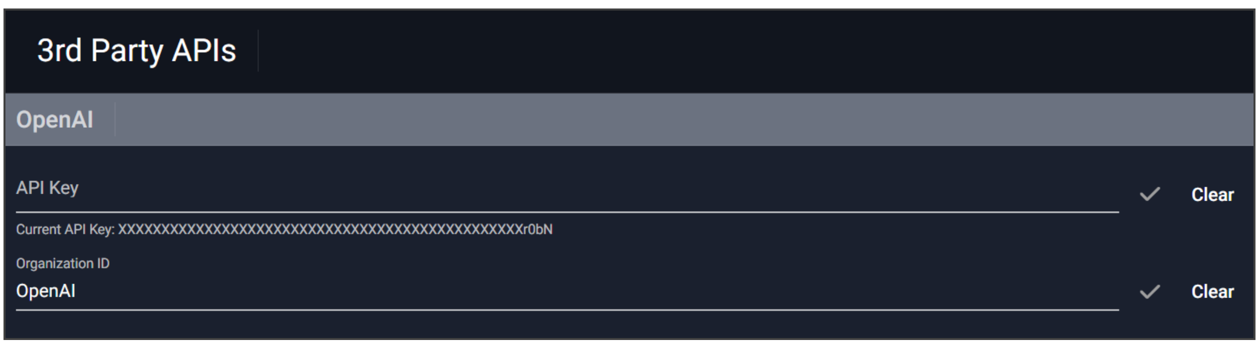
7. Navigate to CommandCTRL.
8. In CommandCTRL's side navigation panel, go to **Settings** > **Site** and locate the **3rd Party APIs** widget.

9. In the **3rd Party APIs** widget, paste your OpenAI **API Key** in the field.

   The check mark to the far right of the field changes color from gray to green.

10. Click the check mark to accept the **API Key**.

    The check mark to the far right of the field changes color from green to gray and the **Clear** button highlights to show it accepted your **API Key**.



    The **API Key** is hidden and replaced with text (i.e., xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx).

    If you click the **Clear** button your **API Key** is removed from the field and the **Clear** button is no longer highlighted.

Verify CommandCTRL is Connected to OpenAI

To verify CommandCTRL and OpenAI are connected, complete the following steps:

1. Follow the steps in Using OpenAI's API and verify you are able to see the (**OpenAI**) icon to the right side of the processes.
2. Click the (**OpenAI**) icon to the right side of a process.

   A dialog box opens that contains the **Process** (e.g., smss.exe), **Manufacturer** of that process (e.g., Microsoft), and a description of the process.

3. Click anywhere outside of the dialog box for it to close.

OpenAI Accuracy Statement

If you type "*statement regarding accuracy of openai information*" into ChatGPT's search field, you will receive the following statement:

"As an AI language model developed by OpenAI, my responses are generated based on patterns and associations learned from a vast amount of text data. While I strive to provide accurate and helpful information, my responses may not always be completely accurate or up-to-date, as the world is constantly changing and evolving. It is always a good idea to verify any information I provide with additional sources and consult with experts in the relevant field. Additionally, it is important to remember that OpenAI is a research organization, and the information provided by OpenAI, including by me as a language model, should not be used as a substitute for professional advice or guidance."

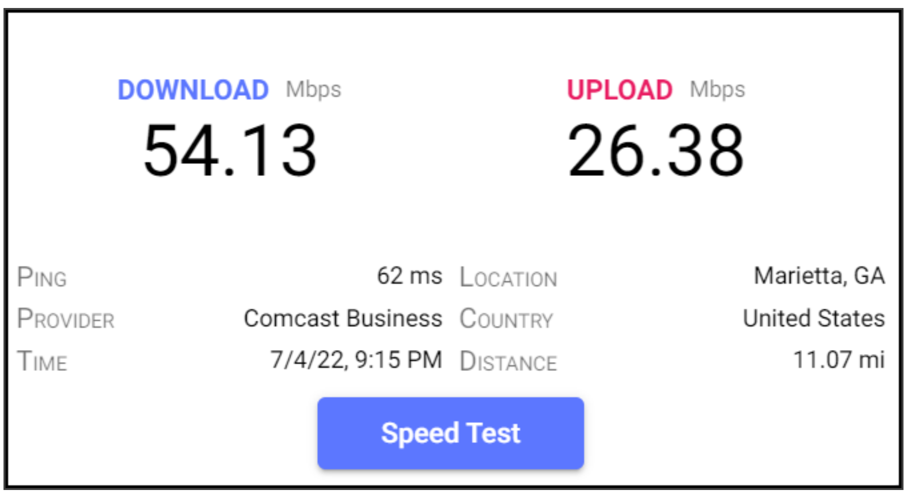
Diagnostic Tasks

Run a Speed Test on a Machine

The CommandCTRL application includes a number of Agent tools that provide you with just-in-time insight into the state of an end user's machine. One of these is a speed test, which measures the machine's upload and download speeds as well as the latency of the connection. To run a speed test, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine on which you want to run a speed test.
3. In the side navigation panel, click the **Diagnostics** link.
4. On the screen that opens, click the **Speed Test** button in the widget on the left.

   When the speed test finishes, the results are displayed on the screen, as shown in the image below



Ping Another Machine

The CommandCTRL application includes a number of Agent tools that provide you with just-in-time insight into the state of an end user's machine. One of these is the ping function, which allows you to send a request over the network to another machine to check whether the end user's machine is reach-able on that network. To ping another machine, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine you want to run a ping test.
3. In the side navigation panel, click the **Diagnostics** link.

4. On the screen that opens, in the widget that displays a **Ping!** button, enter the IP address of the machine you want to send the request to.
5. Click the **Ping**! button.

   If the ping is successful, the command field should display the following information:
   - The number of packets sent to the other machine.
   - The number of packets received from the other machine.
   - The number of packets lost.
   - The approximate round-trip time (in milliseconds) for the request to travel between the two machines.
7. (Optional) Click the **copy** link in the command field to copy the ping details.

Run Traceroute for a Machine

The CommandCTRL application includes a number of Agent tools that provide you with just-in-time insight into the state of an end user's machine. One of these is the traceroute function, which tracks the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all routers it pings in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination. To run traceroute for a machine, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine you want to run a traceroute.
3. In the side navigation panel, click the **Diagnostics** link.
4. On the screen that opens, locate the **Traceroute** widget, which is usually on the far right.
5. Enter the IP address of the machine you want to run.
6. Click the **Traceroute!** button.
7. (Optional) Click the **copy** link in the command field to copy the traceroute details.

Run IPConfig for a Machine

The CommandCTRL application includes a number of Agent tools that provide you with just-in-time insight into the state of an end user's machine. One of these is the ipconfig function, which allows you to get the IP address information of a Windows computer. To run ipconfig for a machine, complete the following steps:

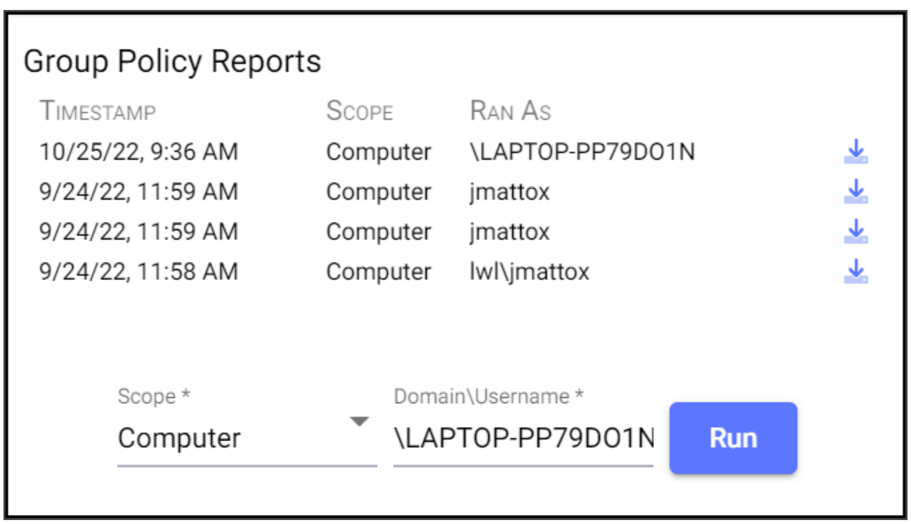
1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine you want to run an IPConfig.
3. In the side navigation panel, click the **Diagnostics** link.
4. On the screen that opens, locate the **Run IPConfig** widget, which is usually in the second row on the left.

5. In the widget, click the **Show All** toggler if you want to see *all* of the IP configuration details for the machine. If this is not enabled, the results only display the following ethernet adapter details:
    - Connection-specific DNS suffix
    - IPv4 address
    - Subnet mask
    - Default gateway
6. Click the **IPConfig** button.
7. (Optional) Click the **copy** link in the command field to copy the IPConfig details to your clipboard.

Run a Group Policy Report

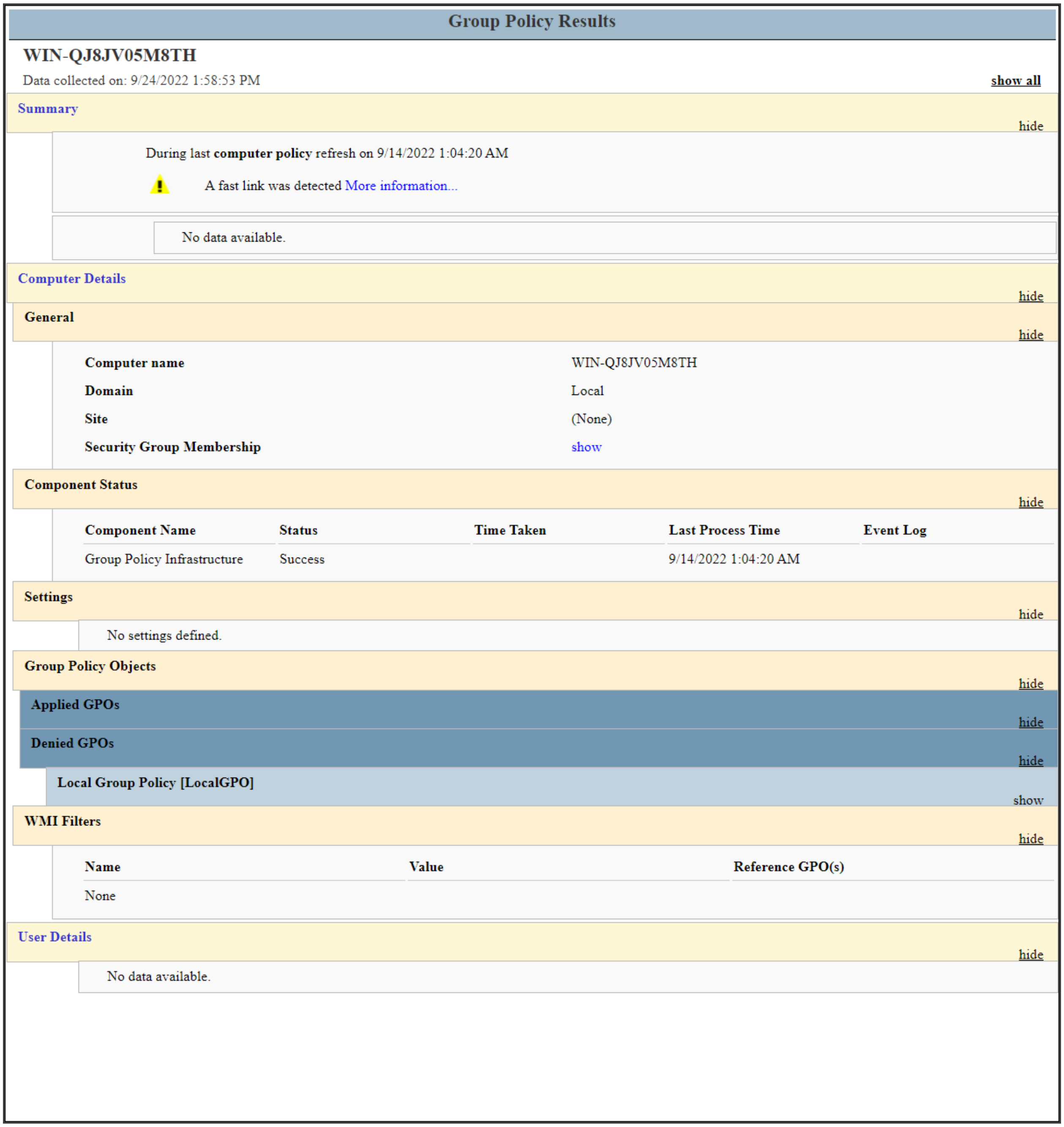
The CommandCTRL application includes a number of Agent tools that provide you with just-in-time insight into the state of an end user's machine. One of these is Group Policy report, which provides details on all the user and computer policies assigned to the machine. To generate one of these reports, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine for which you want to generate the Group Policy report.
3. In the side navigation panel, click the **Diagnostics** link.
4. On the screen that opens, locate the **Group Policy Reports** widget.
5. In the **Scope** field, select the scope for the report that you want to run:
    - **Computer**: Narrows the report to the specific computer you select.
    - **User**: Narrows the report to the specific user you select.
6. Click the **Run** button to view the report.



8. When the report is generated, click the (**Download Report**) button to the right of each report you want to download to your computer.

The following is an example of what a generated Group Policy Report looks like.



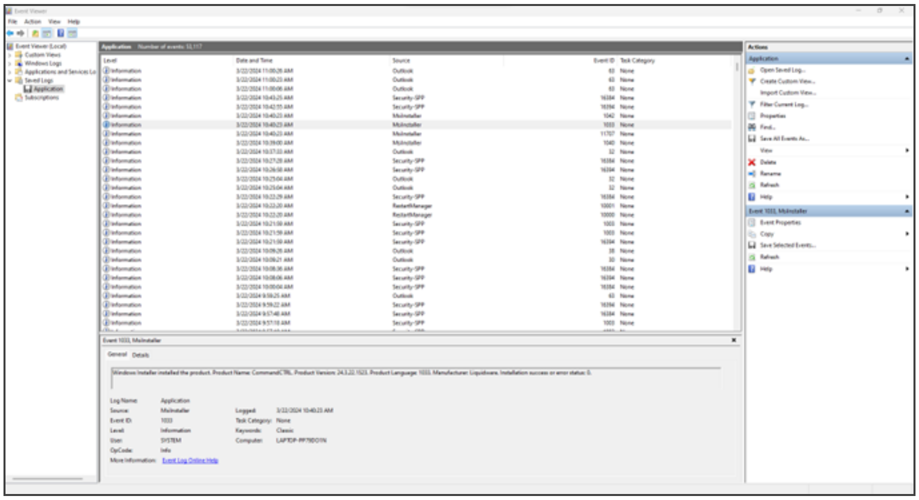
Create Event Log Archive

The CommandCTRL application includes a number of Agent tools that provide you with just-in-time insight into the state of an end user's machine. One of these is Event Logs Archive, which provides all the event logs on a machine for Application, Security and System. To generate one of these archives, complete the following steps:

1. In the side navigation panel, go to **Inventory > Machines**.
2. On the Machines screen that appears, locate, and click the name of the machine for which you want to generate the Event log archive.
3. In the side navigation panel, click the **Diagnostics** link.
4. On the screen that opens, locate the **Event Logs** widget.
5. In the Event Types field, select the event log type that you want to archive:
    - **Application**: The Windows Application Event Log records events from applications and services running on the system, including messages, warnings, errors, and critical notifications. It's used by administrators to troubleshoot issues, track software behavior, and diagnose problems affecting application performance and system stability.
    - **Security**: The Windows Security Event Log is a critical component of the Windows operating system, dedicated to recording security-related events such as authentication attempts, resource access, and security policy changes. It provides administrators with insights into system security, enabling them to monitor user activity, detect unauthorized access attempts, and investigate security incidents. By analyzing event details such as event type, timestamp, and user identity, administrators can effectively identify security threats, enforce security policies, and safeguard the integrity of the Windows environment.
    - **System**: The Windows System Event Log is an essential part of the Windows operating system, responsible for logging events related to system operation and hardware/software components. It records information about system startup, shutdown, device driver failures, and other system-level events. System administrators rely on this log to troubleshoot issues, diagnose hardware and software failures, and monitor system health. By analyzing event details such as event type, timestamp, and source component, administrators can efficiently identify and resolve system-related problems, ensuring the smooth operation and reliability of the Windows environment.
6. Click the **Archive** button to view the archive.

7. When the report is generated, click the (**Download Report**) button to the right of each archive you want to download to your computer.

    The following is an example of what an Event Viewer archive looks like.



To view a windows event log archive on a MAC OSx you have a few options.

1. Use an Online Windows Event Viewer - https://www.gigasheet.com/
2. Download a MAC application from the App Store called “EVTX Reader”.

Retrieve Agent Logs

The Agent Logging tool allows you to be able to use the agent to connect to a user's machine to capture real-time and historic data from that machine. This is similar to taking a recording of everything that is occurring or has occurred on that user's machine. The tool gives you two options for capturing data –the ability to capture the current log as-is and the ability to set a timer from 5 to 30 minutes, in 5-minute increments to only capture a log of that time period.

Downloading the log data as-is can provide a wide range of activity for when you want to view all the functionality of that machine in situations when you might not know exactly what the issue is, whereas setting a time limit can narrow the time-frame for when you have more information about the issue so you want to limit your troubleshooting to a few aspects of that machine, such as Speed Test, Ping!, etc.

Navigating to Agent Logging

To retrieve logs, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen, locate and click the name of the machine for which you want to retrieve the Agent logs.

   The **Dashboard** displays.

3. In the side navigation panel, click **Diagnostics**.
4. On the screen that opens, locate the **Agent Logging** widget.

Archiving a Log

To archive the logs, complete the steps in Navigating to Agent Logging above and then the following steps:

1. Click the **Archive Now** button.

   The agent reaches out to the user's machine, captures a log file, and then the log file appears in the widget with the current date and time.

2. Click the (**Download**) button.

   The .ZIP file begins to download.

3. Open the .ZIP file to view eight text files that contain data about that machine.

Setting Debug Mode

To set a time limit for capturing a log, complete the steps in Navigating to Agent Logging above and then the following steps:

1. Click the **Set Debug Mode** button.

   A **Select Duration** dialog box appears.

2. Click the **Duration** drop-down and select a time from 5 to 30 minutes, in 5-minute increments.

   > **Note:** You cannot type into this field.

4. Click the **Confirm** button.

   The dialog box disappears, and the clock (not viewable) begins counting down.

5. Run tasks, such as Speed Test, Ping!, or perform other operations in order to collect specific log data within the time limit you selected.

   The agent reaches out to the user's machine and captures a log file. At any time, you can click the **Archive Now** button to get a log file, however the task will continue for the designated time you selected.

   After the timer stops (automatically or manually), the log file appears in the widget with the current date and time.

6. Click the (**Download**) button.

The .ZIP file begins to download.

7. Open the .ZIP file to view eight text files that contain data about the machine.

Downloading Existing Logs

To download existing logs, complete the steps in Navigating to Agent Logging above and then the following steps:

1. Click the (**Download**) button.

   The .ZIP file begins to download.

2. Open the .ZIP file to view eight text files that contain data about the machine.

View the Performance Statistics for a Machine

To kill a process that is currently running on a machine, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine whose performance statistics you want to view.
3. In the side navigation panel, go to **Task Manager** > **Performance**.
4. On the screen that opens, click the tabs on the left to view real-time performance statistics for the following machine components:
   - CPU
   - Memory
   - Disk
   - Wi-Fi/Ethernet
   - GPU

View the CPU and GPU Statistics

There are two ways to view the CPU and GPU statistics. One method is to view this data in the Dashboard System Properties widget in "Live Mode" and the other method is to view the CPU and GPU in the Dashboard CPU and GPU widgets, which show live and historical data.

In the System Properties widget's "Live Mode" you will be able to view Load, Temperatures, and Fan Speed only in real-time. In the CPU widget you will be able to view the Utilization in real-time. In the GPU widget you will be able to view the Utilization and Temperature in real-time. Both the CPU and GPU widgets can display the history, which will allow you to view the data at various moments in time.

> **Note:** Fan Speed is only reported on desktop machines, and only in real-time in the Dashboard System Properties widget. Currently, the CPU and GPU widgets do not report Fan Speed.

Locating the Machine

To find the machine that you want to view the CPU and GPU statistics, complete the following steps:

1. Open CommandCTRL.
2. In the side navigation panel, go to **Inventory** > **Machines**.
3. On the **Machines** screen, locate and click the name of the machine for which you want to view.

   The **Dashboard** displays.

4. Proceed to any of the following sections to view the CPU and GPU statistics in either the System Properties and/or CPU and GPU widgets.

CPU

In the System Properties widget's "Live Mode" you will be able to view Load and Temperatures only in real-time. In the CPU widget you will be able to view the Utilization in real-time and in the history, which will allow you to view the data at various moments in time.

To view the CPU statistics, complete the following steps:

System Properties Widget

Real-Time Load or Temperature

1. Complete the steps in Locating the Machine above and then the following steps.
2. In the **System Properties** widget, located on the top right, click the **Hardware Information**  icon.

   The **Hardware Information** dialog box appears.

3. Click the drop-down next to the machine to expand it and view the hardware.
4. Click the drop-down next to the CPU.
5. Click either the **Load** or **Temperatures** drop-down to view all the load or temperature measurements in real-time.

> **Note:** The **CPU Total** displays the average **Load** in percentage of all the cores. The **CPU Package** displays the highest **Temperature** in degrees of all the cores. Both measurements are in real-time.

7. Click the **Close** button in the lower right corner to close the **Hardware Information** dialog box.

Enable/Disable Open Hardware Monitor On Agents

Real-Time Load or Temperature are dependent on http://openhardwaremonitor.org/. If this technology is not allowed in your environment, you can do the following to remove it from the agent.

To set up CommandCTRL to Enable/Disable Open Hardware, complete the following steps:

1. In the side navigation panel, go to **Settings > Site**.
2. In the **Enable/Disable Open Hardware Monitor On Agents** field, click the toggler so that it option is in the desired position, turned on (displays in red).

CPU Widget

Real-Time Utilization

1. Complete the steps in Locating the Machine above and then the following steps.
2. In the **CPU** widget, on the left side, view the real-time **Utilization** of the CPU.

Utilization History

1. To view the history of the CPU's **Utilization**, click the View History icon. This displays the daily history for that machine.
2. Click any of the days to display the hours in a day.
3. Click an hour to display a recording of the entire hour for that machine and all the metrics in the **Dashboard** widgets as the time-line progresses.

   You can click the turtle icon to slow down the speed, the rabbit icon to increase the speed, the pause icon to pause the recording, or the play icon, which only appears if the recording was paused, to play the recording.

GPU

In the System Properties widget's "Live Mode" you will be able to view Load and Temperatures only in real-time. In the GPU widget you will be able to view the Utilization and Temperature in real-time and in the history, which will allow you to view the data at various moments in time.

To view the GPU statistics, complete the following steps:

System Properties Widget

Real-Time Load and Temperature

1. Complete the steps in Locating the Machine above and then the following steps.
2. In the **System Properties** widget, located on the top right, click the **Hardware Information** icon.

   The **Hardware Information** dialog box appears.

3. Click the drop-down next to the machine to expand it and view the hardware.
4. Click the drop-down next to the GPU.
5. Click either the **Load** or **Temperatures** drop-down to view all the load or temperature measurements in real-time.

   > **Note:** The **GPU Total** displays the average **Load** in percentage of all the cores. The **GPU Package** displays the highest **Temperature** in degrees of all the cores. Both measurements are in real-time.

7. Click the **Close** button in the lower right corner to close the **Hardware Information** dialog box.

GPU Widget

The Dashboard GPU widget is able to access many different GPU manufacturers and models, however if no data is displayed in the widget, then most likely you will be able to view the real-time data in the System Properties widget since that widget has access to a database of many GPU manufacturers and models.

Real-Time Utilization and Temperature

1. Complete the steps in Locating the Machine above and then the following steps.
2. In the **GPU** widget, on the left side, view the real-time **Utilization** of the GPU.
3. In the **GPU** widget, on the right side, view the real-time **Temp** of the GPU.

Utilization and Temperature History

1. To view the history of the GPU's **Utilization** and **Temp**, click the View History icon. This displays the daily history for that machine.
2. Click any of the days to display the hours in a day.
3. Click an hour to display a recording of the entire hour for that machine and all the metrics in the **Dashboard** widgets as the time-line progresses.

   You can click the turtle icon to slow down the speed, the rabbit icon to increase the speed, the pause ⏸ icon to pause the recording, or the play ▶ icon, which only appears if the recording was paused, to play the recording.

Fan Speed

In the System Properties widget's "Live Mode" you will be able to view a desktop machine’s Fan Speed only in real-time.

> **Note:** Fan Speed is only reported on desktop machines, and only in real-time in the System Properties widget. Currently, the CPU and GPU widgets do not report Fan Speed or its history.

To view the Fan Speed statistics, complete the following steps:

System Properties Widget

Real-Time Fan Speed

1. Complete the steps in Locating the Machine above and then the following steps.
2. In the **System Properties** widget, located on the top right, click the **Hardware Information** icon.

   The **Hardware Information** dialog box appears.

3. Click the drop-down next to the machine to expand it and view the hardware.
4. Click the drop-down next to the CPU.

   > **Note:** If there are other fans inside the desktop, such as a case fan, it is possible to select the hardware and view the fan speeds and temperature inside the case.

6. Click **Fans** drop-down to view all the measurements in real-time.

   > **Note:** The **Fan Speed Total** is an average speed in percentage. The **Fan Speed Package** is an highest speed. Both are in real-time.

8. Click the **Close** button in the lower right corner to close the **Hardware Information** dialog box.

Using OpenAI's API

CommandCTRL has been designed to allow integration with OpenAI’s API in order to leverage the large language models (LLMs) for more information on what is running on a machine in your environment. When looking at a list of processes on a machine, you can query OpenAI for the manufacturer and a description based on the process name. CommandCTRL currently utilizes OpenAI’s gpt-3.5-turbo-0125 or gpt-4 or gpt-4-turbo-preview , which is the LLM that ChatGPT was originally based upon.

You can integrate CommandCTRL with OpenAI gpt-3.5-turbo-0125 or gpt-4 or gpt-4-turbo-preview through its API (Application Programming Interface) Key and Organizational ID. This guides you through how to use OpenAI's API in CommandCTRL to provide you with information.

> **Note:** Before you can use OpenAI's API, you will need to have an OpenAI account and CommandCTRL with OpenAI gpt-3.5-turbo-0125 or gpt-4 or gpt-4-turbo-preview. For more information, see Integrating CommandCTRL with OpenAI.
>
> OpenAI charges a subscription and a fee for data (see OpenAI.com for their fee structure). Our integration was designed to help save you money by caching their information for 90 days. When anyone in your tenant clicks on the OpenAI icon, the information they provide is saved to cache and is available whenever anyone else in your tenant requests the same information within 90 days. After 90 days, it is assumed that the information needs to be refreshed since information is always changing.

When you are viewing the list of processes, this API integration allows you to get information about a specific process from OpenAI. This can be helpful when you are troubleshooting a user's machine and you want to know more about a process that might be causing their machine to have an issue.

There are multiple ways to get to the **Processes** screen. This procedure assumes you noticed an issue displaying in one or more of the widgets on the **Dashboard** for a machine and want to navigate to the **Processes** screen to investigate. To view all the processes and get information from OpenAI about a specific process, complete the following steps:

1. In the side navigation panel, go to **Dashboard**.
2. Locate the issue in any of the "Top 5" consumers widgets (e.g., CPU, RAM, Disk, and Net). For example, the **Memory** widget is triggering an alert so you want to view the processes in the **Top 5 RAM Consumers** widget.
3. Click the **Go To Processes** icon on any of the "Top 5" consumers widgets.

   The **Processes** screen displays. The data being displayed is only for the machine you selected and the users on that machine. You are able to see each of the machine and user names under the **User** column.

4. On the **Processes** screen, scroll through the list or use the search field to locate the process in which you want information about that process.

   > **Note:** You can also click on any of the column headings (i.e., PID, CPU, Memory, Disk, Network, and User) to sort the columns in ascending or descending order. This can be useful when you are trying to find the process that is using the most resources.

6. Click the (**OpenAI**) icon to the right side of the process.

   A dialog box opens that contains the **Process** (e.g., smss.exe), **Manufacturer** of that process (e.g., Microsoft), and a description of the process shown in the **Website** field.

7. Click anywhere outside of the dialog box for it to close.

OpenAI Accuracy Statement

If you type "*statement regarding accuracy of openai information*" into ChatGPT's search field, you will receive the following statement:

"As an AI language model developed by OpenAI, my responses are generated based on patterns and associations learned from a vast amount of text data. While I strive to provide accurate and helpful information, my responses may not always be completely accurate or up-to-date, as the world is constantly changing and evolving. It is always a good idea to verify any information I provide with additional sources and consult with experts in the relevant field. Additionally, it is important to remember that OpenAI is a research organization, and the information provided by OpenAI, including by me as a language model, should not be used as a substitute for professional advice or guidance."

Tool Tasks

Note: The following is not applicable to Mac support.

View Script Lists and Script Details

The Tools section of the CommandCTRL application allows you to view a list of triggers and alarms that have been generated for machines you are able to view and lets you add actions to generate those triggers and alarms. The Tools section also displays a list of the scripts that have been installed on each machine and a separate list of scripts that can be installed on each one.

Note: The following is not applicable to Mac support.

View Installed and Recommended Scripts

To view the list of scripts that have been installed on a machine and to see the list of available scripts, go to **Tools** > **Scripts** > **Store**.

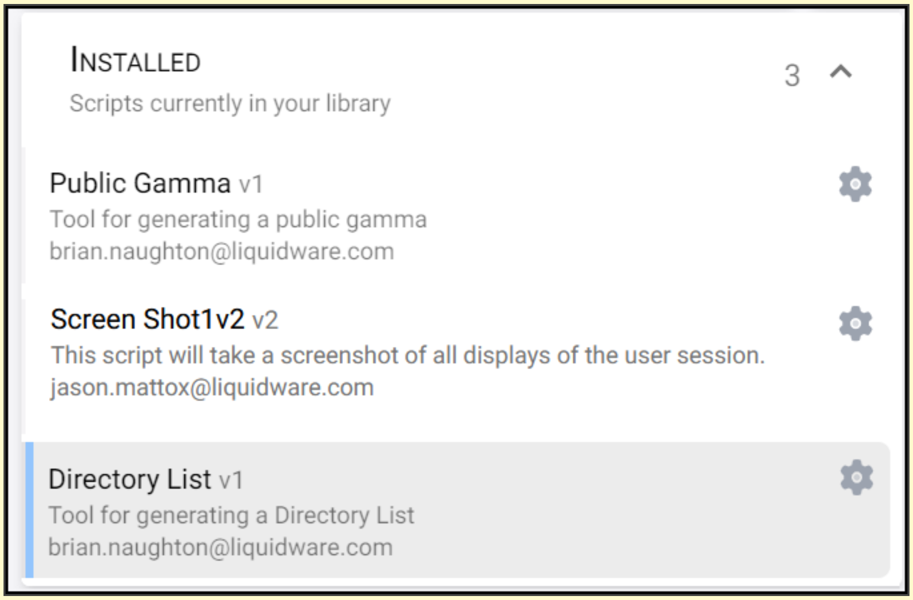
The upper section of the **Scripts** screen that appears lists the scripts that have already been installed. The bottom section of the pane displays a curated list of scripts that Liquidware recommends. Note that the recommended scripts are not installed, by default. In order to use them, you have to install them manually.

View Details of a Script

To view a description of a script, the script code, and the change log associated with it, complete the following steps:

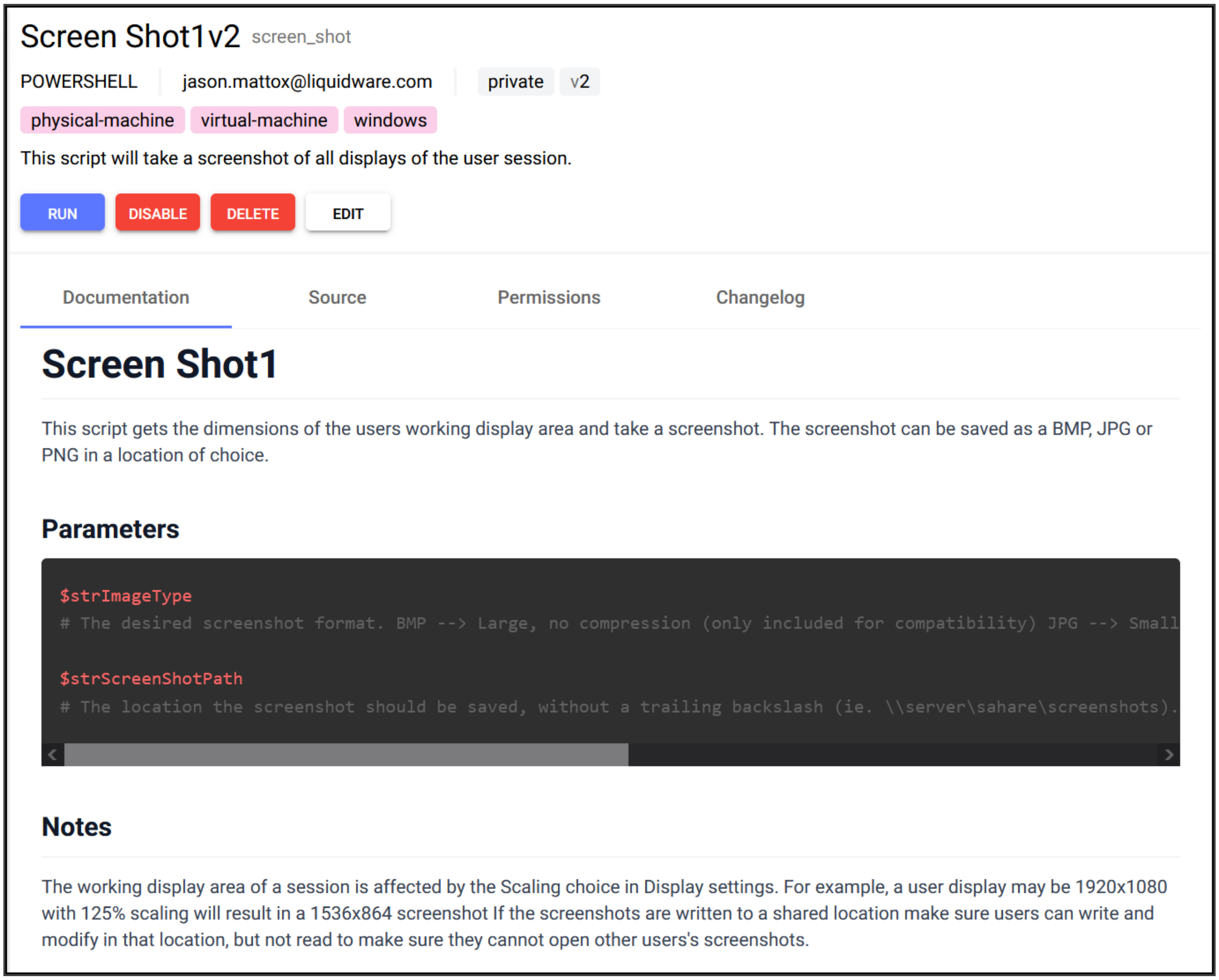
1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. Scroll through the **Installed** or **Recommended** fields on the screen to find the script whose details you want to view, or use the search engine if the script list is extensive.

Note: You can tell at a glance if a script in the **Installed** list was originally from the **Recommended** list of public scripts because a blue bar appears on the left edge of the script name, as shown in the image below for the **Directory List** script.



If you uninstall a public script, it returns to the **Recommended** list automatically.

4. Click a script name.
5. In the field that appears on the right, four tabs appear: **Documentation**, **Source**, **Permissions**, and **Changelog**.



7. The script **Documentation** tab is open by default, providing you with a description of the parameters that let you test different results and see the output in CommandCTRL. This tab also displays any notes entered when the script was created.
8. To view the script code, click the **Source** tab. If you want to copy the code, click the **copy** link in the bottom right corner of the field.
9. To view the change log, which includes a chronological list of all bug fixes and added features for the script, click the **Changelog** tab.

Allow or Disallow Unsigned Scripts to Be Uploaded

CommandCTRL can be set up to either allow or disallow users to upload unsigned scripts. If unsigned scripts *are* allowed, the CommandCTRL Agent does an online check to make sure the hashsum of the unsigned script file matches the hashsum of the same script in the library. If it does, the Agent executes the script.

> **Note:** In order to run unsigned scripts, the Agent requires an internet connection so that it can locate and compare the hashsums of the unsigned script and the script in the library.

> **Note:** The following is not applicable to Mac support.

Allow Unsigned Scripts

To set up CommandCTRL to allow unsigned scripts to be uploaded, complete the following steps:

1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Scripts** field, click the **Allow Agents To Hash Check If Not Signed** toggler so that it is turned on (displays in red).

Disallow Unsigned Scripts

To block the uploading of unsigned scripts into CommandCTRL, complete the following steps:

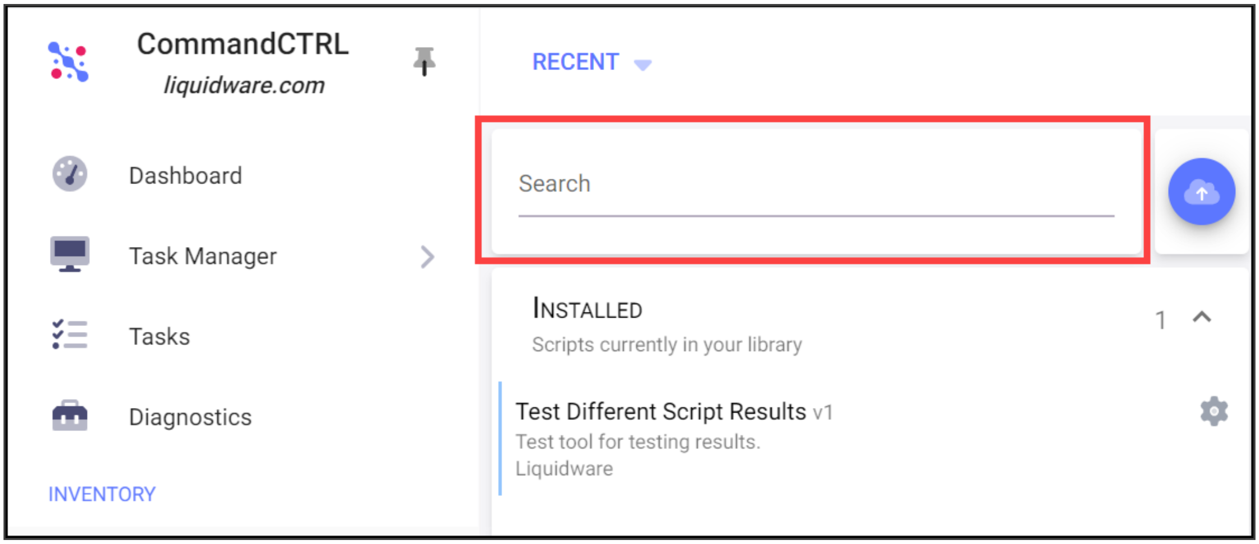
1. In the side navigation panel, go to **Settings** > **Site**.
2. In the **Scripts** field, click the **Allow Agents To Hash Check If Not Signed** toggler so that it is turned off (grayed out).

Search for a Script

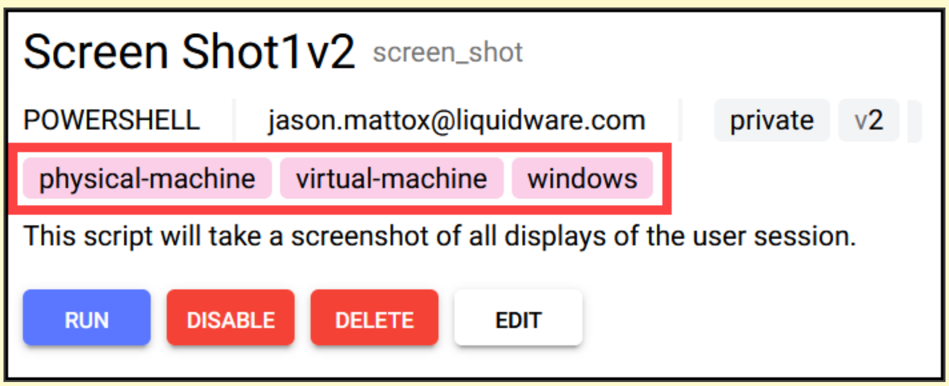
To search for a script that has been uploaded to CommandCTRL, complete the following steps:

> **Note:** The following is not applicable to Mac support.

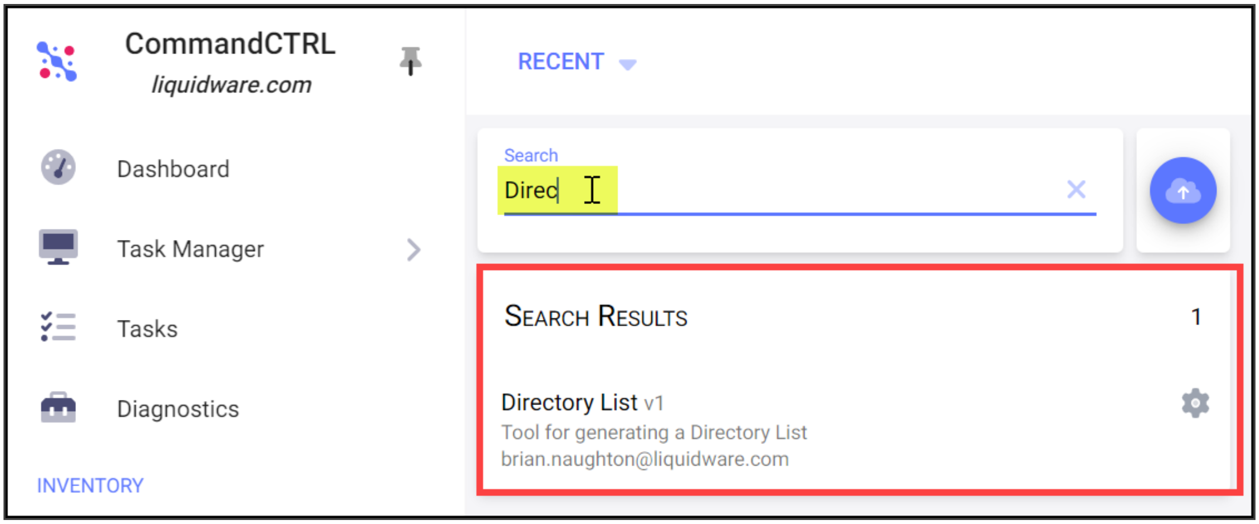
1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. In the **Search** field on the screen that appears, enter a word or phrase related to the script you want to access. Or enter the term `tag:` followed by a specific tag you want to search by. For example, you could enter `tag:windows` to search for all scripts that have been assigned the **windows** tag.



Note: You can also do a quick search for tagged scripts by clicking a tag that appears under a script name in the script details section of the screen. In the image below, for example, clicking **windows** would cause *all* scripts containing the **windows** tag to appear in the search results field. Clicking **virtual-machine** would cause *all* scripts containing that tag to appear in the search list, and so on.



5. As soon as you enter text in the **Search** field, the **Installed** field below it disappears and is replaced by a **Search Results** field. This results field refreshes dynamically to display all scripts that match the current search criteria. In the example below, the user has entered `Direc` in the Search field and the **Directory List** script has already appeared in the Search Results field.



7. As soon as the script you are searching for appears in the results list, click to open it.

Upload a Script

> **Note:** For security reasons, scripts should be signed prior to being uploaded into the system.

To upload a script to CommandCTRL, complete the following steps:

> **Note:** The following is not applicable to Mac support.

1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. In the right pane, click the (**Upload Script**) button.
3. On the **New Script** screen that opens, click the (**Upload**) button.
4. Navigate to and select the file you want to upload.
5. (Optional) Select the **Automatically use script comments to autofill fields** checkbox if you want to have the fields pre-filled for you. If you select this option, you can still enter your own comments in some or all of the fields, over-writing the pre-filled content.
6. Click the **Next** button.
7. In the **Detail** field, enter an ID for the script or accept the default. If you enter an ID manually, it can only contain lowercase alphanumeric characters, dashes, and/or underscores.
8. Enter a name for the script or accept the default.
9. Enter a description for the script or accept the default.
10. Enter at least three tags for the script or accept the defaults. These tags will be used to find the script when you or other users are searching for it using the search engine, so the tags should be relevant and descriptive.
11. Click the **Next** button.
12. In the **Parameters** field, review any existing parameters and modify or delete them if necessary.

13. (Optional) Click the + (**Add Parameter**) button at the bottom of the field to add one or more additional parameters.
14. Click the **Next** button.
15. In the **Documentation** field, use **Markdown** syntax to enter a detailed description of what the script does. This information will appear under the Documentation tab when the script details are viewed in CommandCTRL.

> **Note:** If you do not know Markdown syntax, click the link at the bottom of the screen to open a webpage that explains it in detail.

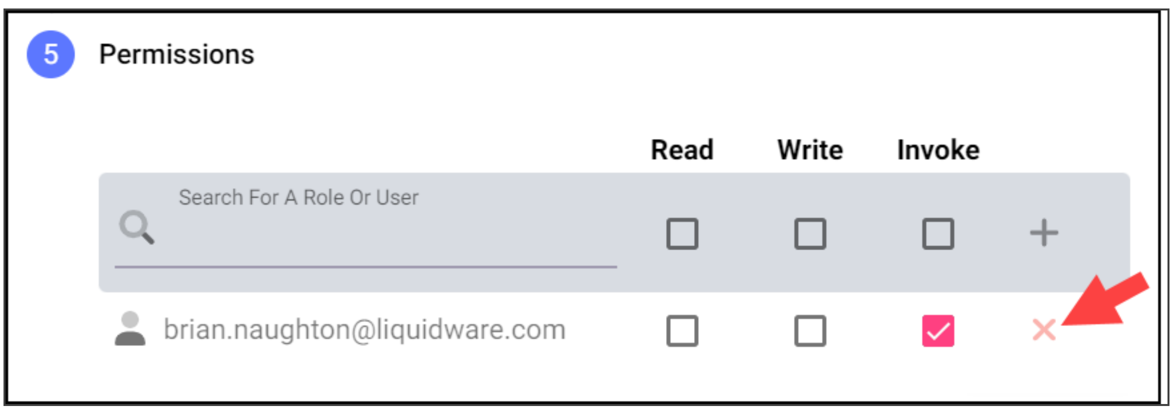
At any time, you can click the **Preview** button to see how the Markdown text you have written will appear online.

18. Click the **Next** button.

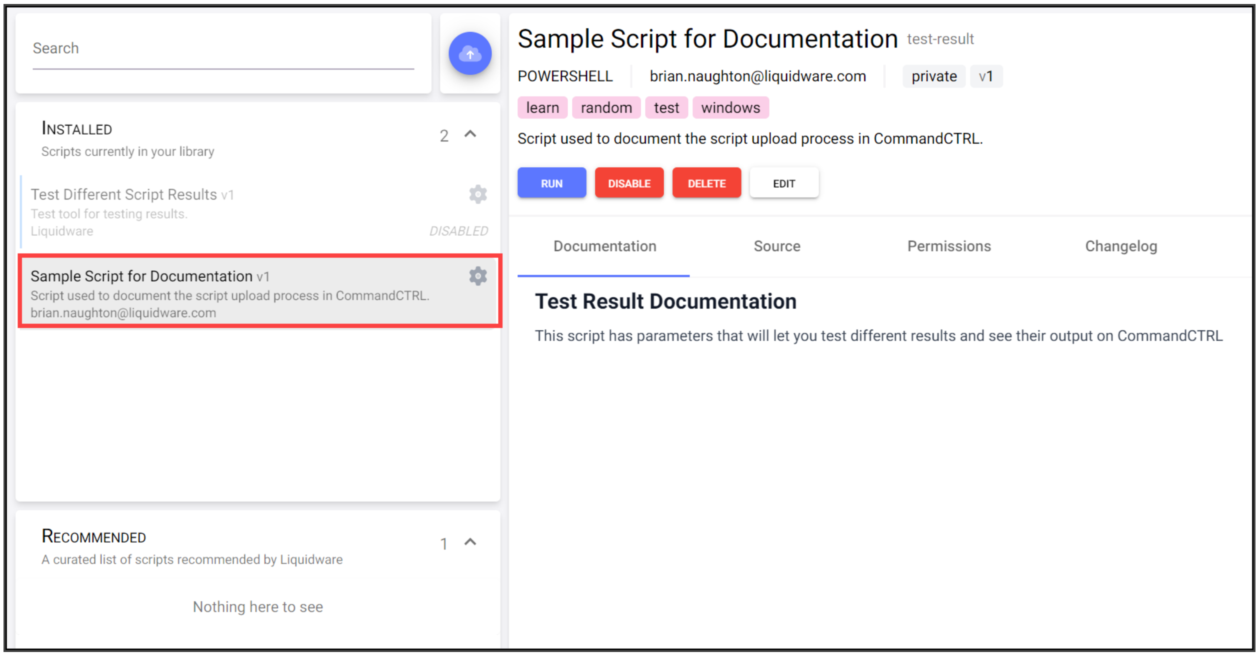
In the **Permissions** field, enter the name of all users and/or roles that you want to assign specific permissions to. For each user and role, select the permissions you want them to have: **Read**, **Write**, **Invoke**. Click the + (**Assign Permission**) button to add the permission to the script.

> **Note:** If you do not assign any permissions for specific users or roles, then *all* users and roles that have been assigned the **script:update** permission will have full access to the script by default.

After you add a permission, you can remove it easily by clicking the × (**Remove Permission**) button beside the user or role name.



23. When you are done setting script permissions, click **Create** to add the script to CommandCTRL. The script then appears in the list installed scripts on the Store screen.

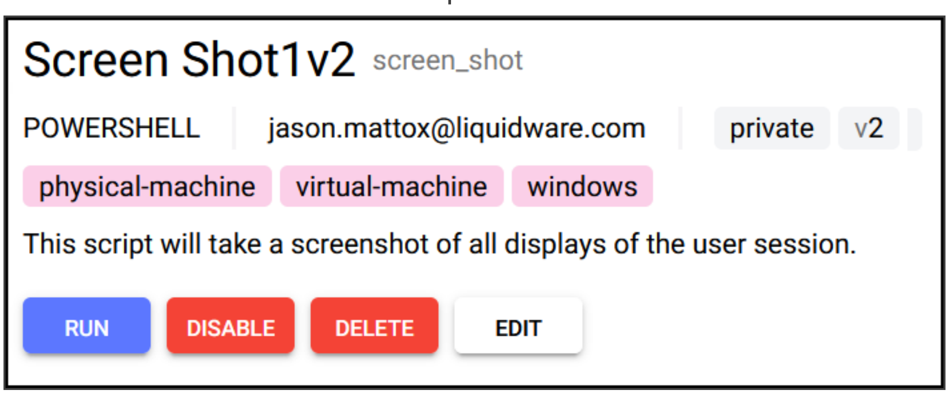


Edit a Script

If a user belongs to a role that has been assigned the permission **script:update**, they are able to edit the scripts in their tenant. To edit a script, complete the following steps:

Note: The following is not applicable to Mac support.

1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. Scroll through the **Installed** field on the screen to find the script you want to edit, or use the search engine if the script list is extensive.
3. Click the script name.
4. Click the **Edit** button below the script name.



The script details screen opens.

7. Click the **Next** button to move on from the **Upload** section that appears by default.

8. In the **Detail** section, make whatever edits you want to the Name, Description, and/or Tags field, then click the **Next** button.
9. In the **Parameters** section, make whatever edits you want to the existing parameters. You can change the text, delete individual parameters, or add new ones. When you have finished, click the **Next** button.
10. In the **Documentation** field, make whatever edits you want to the markdown syntax that exists.
11. Click the **Save Changes** button to complete the edit process.

Install or Uninstall a Script

The CommandCTRL application provides a tool that allows you to install and uninstall scripts quickly and efficiently.

> **Note:** The following is not applicable to Mac support.

Install a Script

There are two ways to install a script in CommandCTRL. The first way is covered in the Upload a Script section of this guide. The second way is to install it via the **Recommended Scripts** section of the default screen list field.

To install a recommended script, complete the following steps:

1. Click its name in the list.
   The script details then appear in the right pane.
3. Click the **Install** button.

Uninstall a Script

To uninstall a script, complete the following steps:

1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. In the **Installed** field that appears on the right, locate and click the script that you want to uninstall.
3. In the script details field that appears on the far right, click the **Uninstall** button.

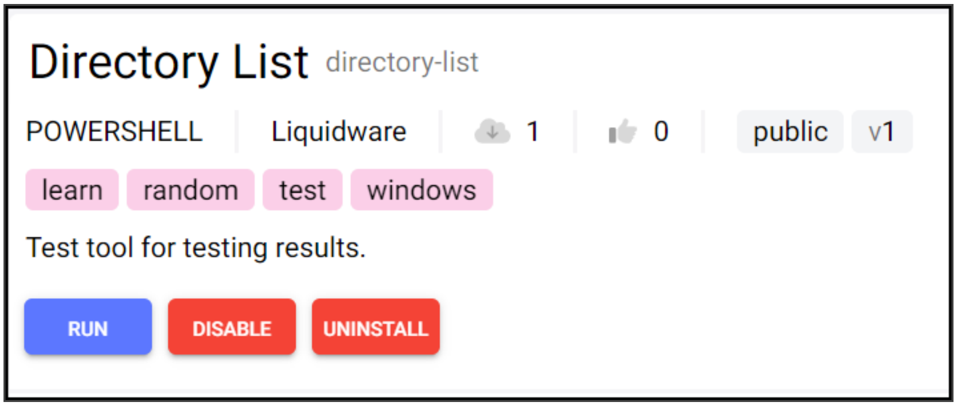
Run a Script

To run a script that has been uploaded to CommandCTRL, complete the following steps:

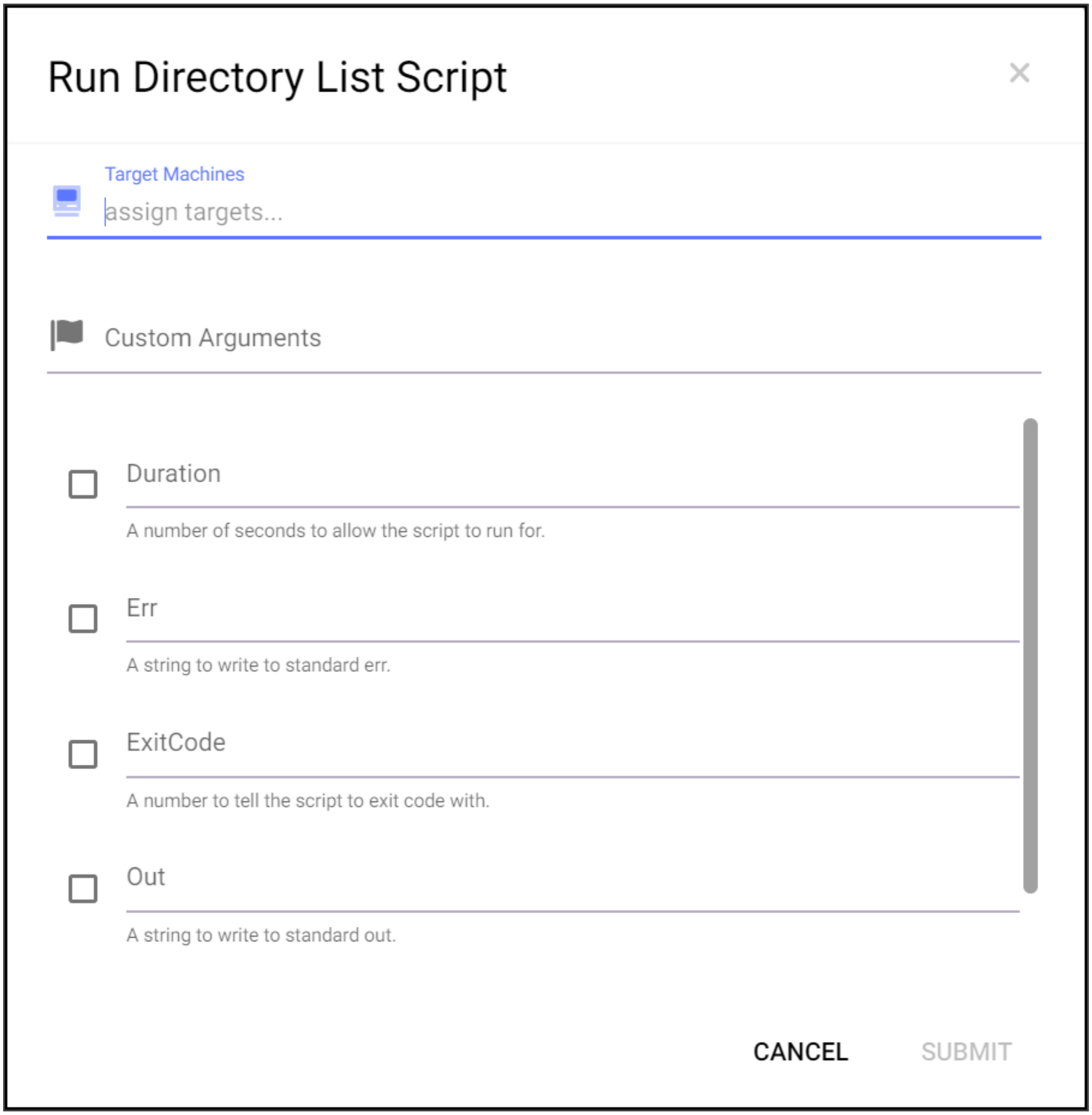
> **Note:** The following is not applicable to Mac support.

1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. Scroll through the **Installed** field on the screen to find the script you want to run, or use the search engine if the script list is extensive.
3. Click the script name.

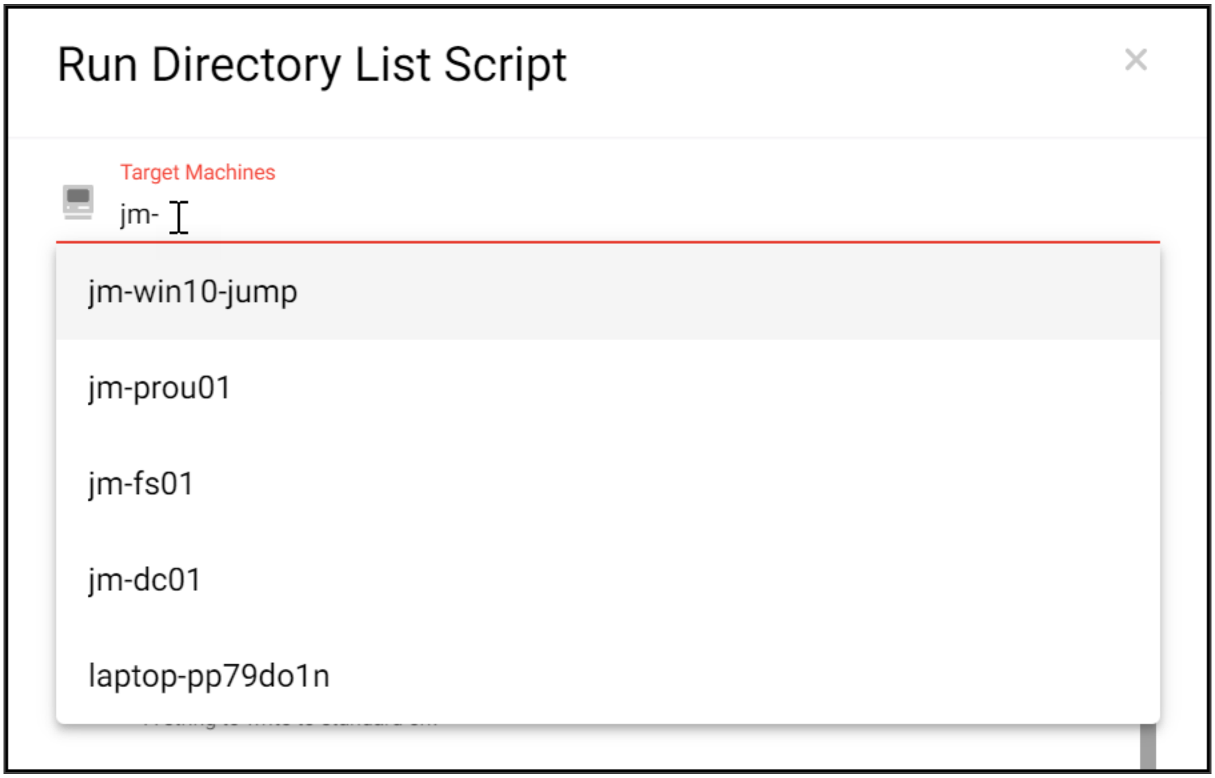
4. Click the **Run** button under the script name.



6. The **Run <script name> Script** screen opens.

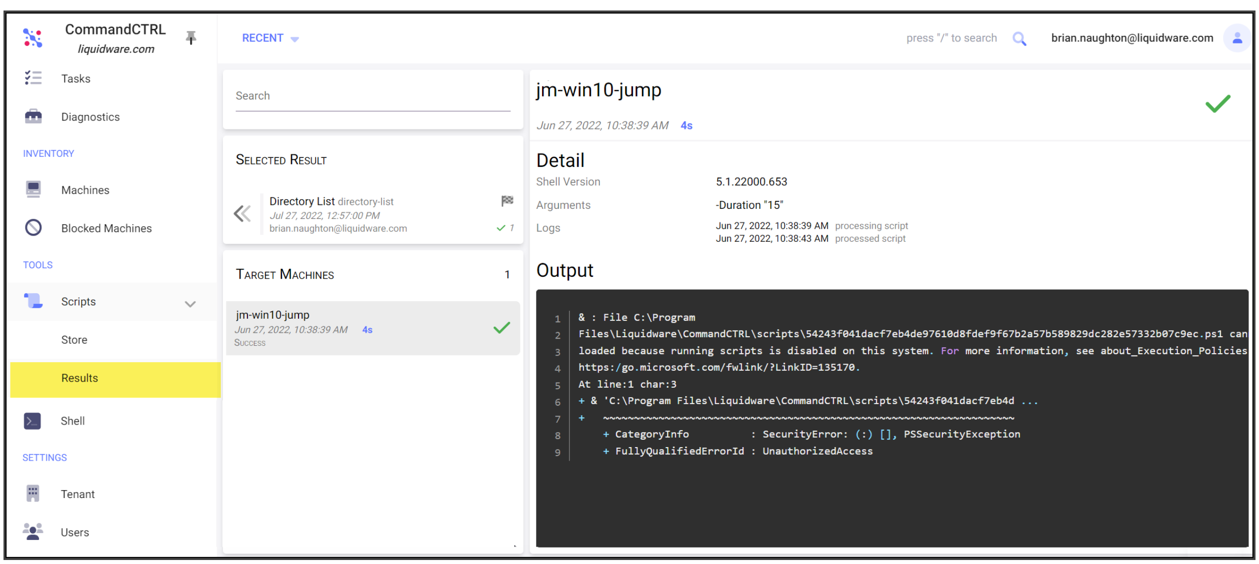


8. In the **Target Machines** field, enter the name of at least one computer on which the script will be run. If you are unsure of the exact name of a computer, start typing in the field and a list of computers that contain the characters you have entered so far will appear in a drop-down list below the Target Machines field.



10. (Optional) In the **Custom Arguments** field, add arguments to the existing script.
11. Select the checkboxes beside each of the parameters you want to include in the script, then add values to each of the parameters.
12. When you have finished, click **Submit** to run the script.

    When the script has finished running, the results are displayed on the **Results** screen located within the **Scripts** section of the left sidebar.

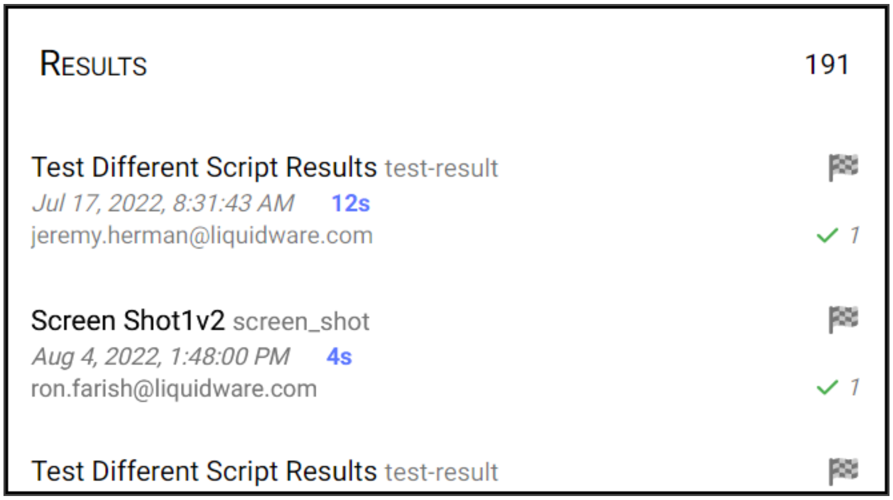


View Script Results

To view the results of a script that has been run in CommandCTRL, complete the following steps:

Note: The following is not applicable to Mac support.

1. In the side navigation panel, go to **Tools** > **Scripts** > **Results**.
2. The **Results** field on the right lists all the scripts that have been run.

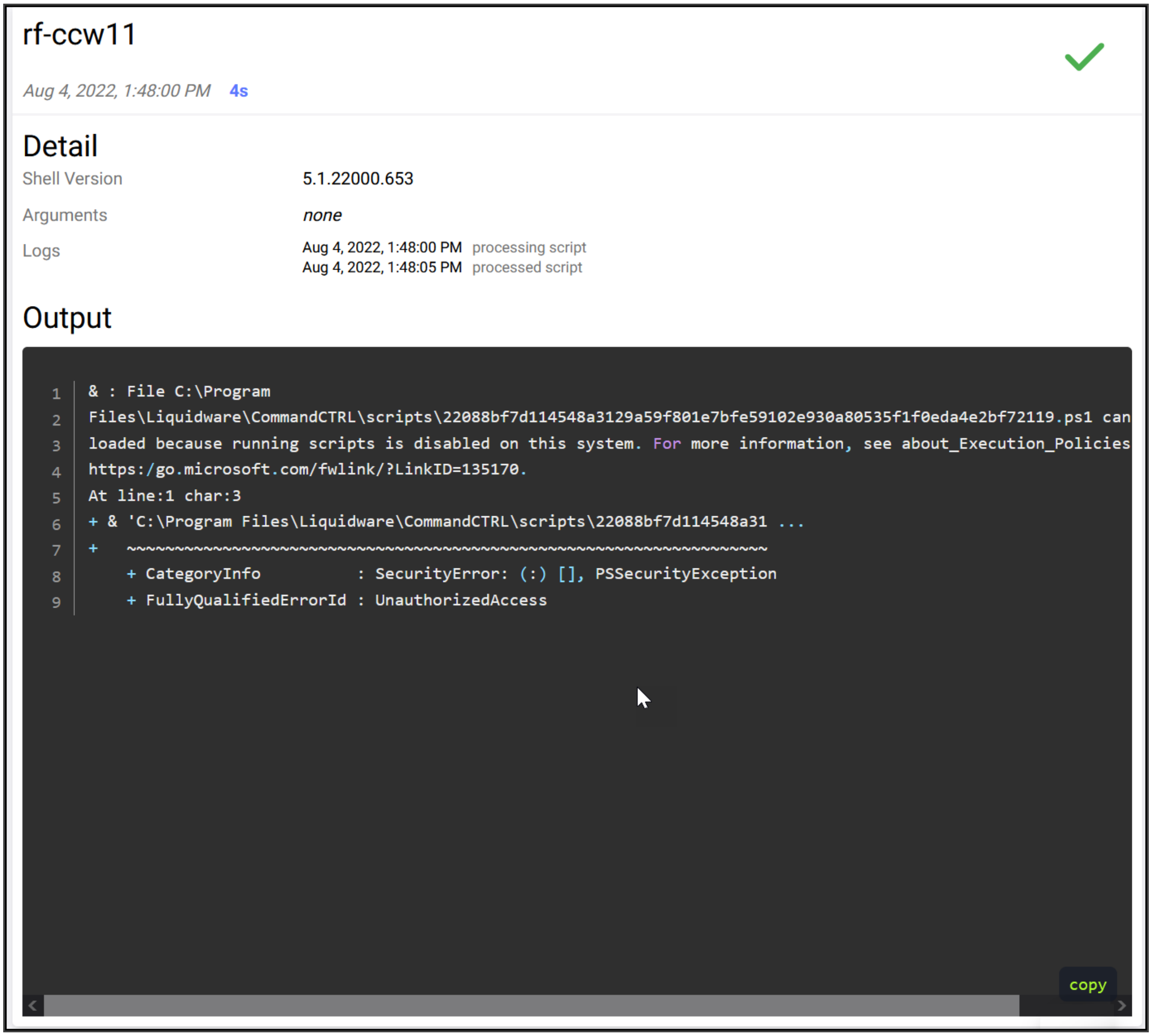


The following information is provided for each script:

- The name of the script and the version of the script. Note that version information is visible only if you hover your cursor over the script name.

- The time and date the script was created.
- The duration of the run.
- The name of the user who ran the script.
- The outcome of the script: whether it completed successfully or whether it timed out before completing.

5. Click the name of a script to view detailed results. The details of the script then appear in the far-right column.



In addition to the five pieces of information listed above, the following information appears for the script:

- The shell version.
- The arguments that were included in the script.
- The script logs.
- The output generated by the script.

Enable or Disable a Script

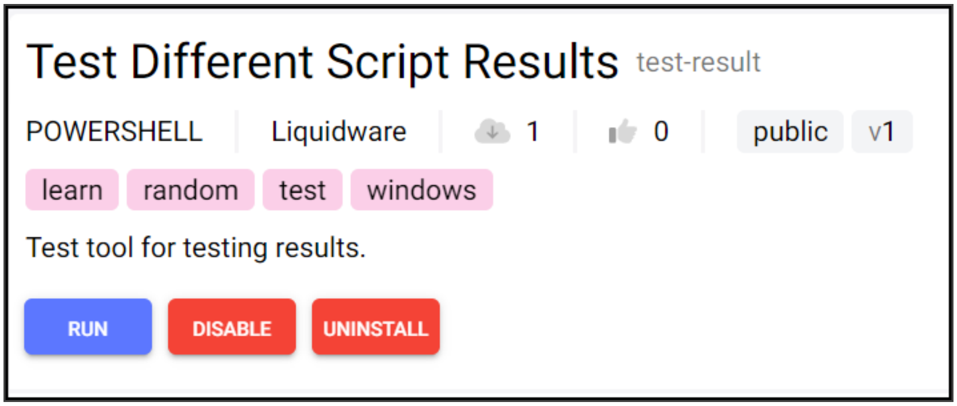
The CommandCTRL application allows you to disable a script to make in unavailable to other users. The same field also allows you to enable a script that has been disabled. Unlike uninstalling a script, disabling a script is a reversible process: you can re-enable it quickly without having to re-install it.

> **Note:** The following is not applicable to Mac support.

Disable a Script

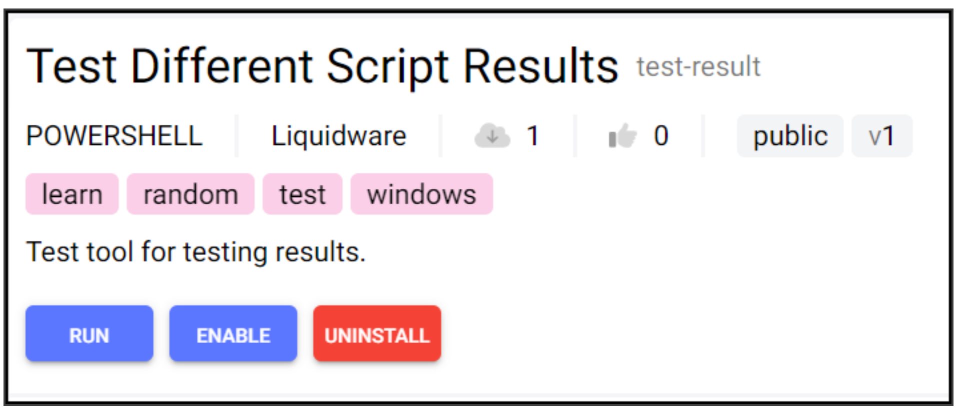
To disable a script, complete the following steps:

1. In the side navigation panel, go to **Tools** > **Scripts** > **Store**.
2. Scroll through the **Installed** field on the screen to find the script you want to disable or use the search engine if the script list is extensive.
3. Click the script name.
4. Click the **Disable** button under the script name.



Enable a Script

After a script has been disabled, the **Disable** button on the script details screen changes to an **Enable** button.

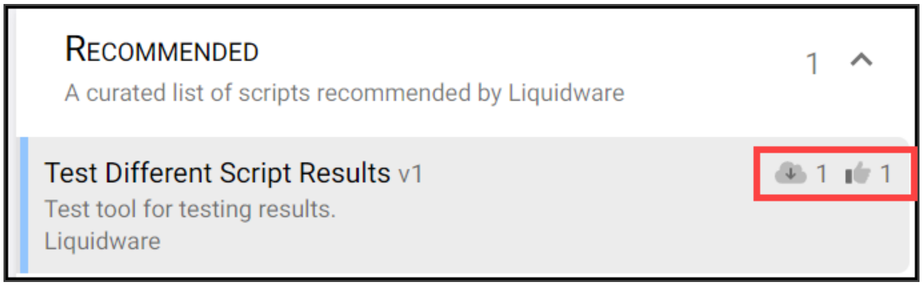


To re-enable the script, simply click the **Enable** button.

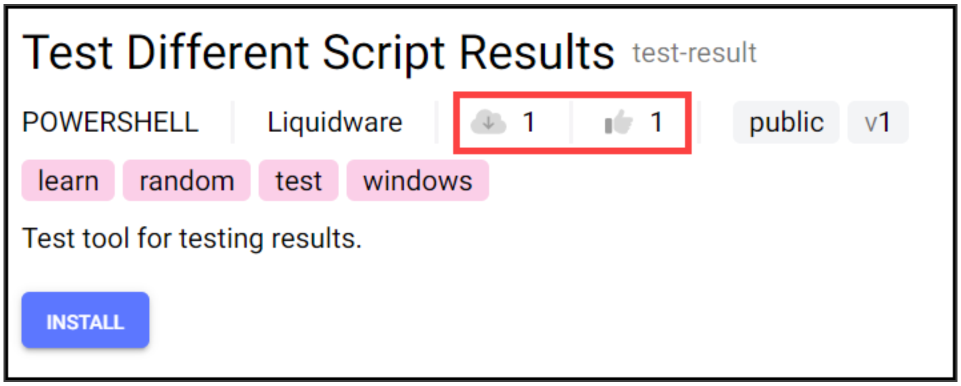
View Statistics for a Public Script

You can tell at a glance how often a public script has been installed and how many upvotes it has received by simply hovering your cursor over the (**Cloud**) or (**Thumbs Up**) icons on the left side of the script name in the **Recommended** or **Installed** list.

Note: The following is not applicable to Mac support.



or by hovering over the same icons under the script name in the script details field.



The first icon, the (**Cloud**), tells you how often the script has been uploaded.

The second icon, the (**ThumbsUp**), tells you how often the script has been upvoted (or "liked") by users in the system.

> **Note:** If the script is private (that is, if it was not originally a **Recommended** script), the two icons do not appear.

Managing Triggers and Alarms

The Tools section of the CommandCTRL application provides a comprehensive interface for monitoring and managing triggers and alarms associated with your machines. These triggers and alarms are visible in real-time and include historical data, enhancing your visibility and control over your environment.

Viewing and Customizing Triggers

Upon accessing the triggers, you may find that the default settings do not align with your specific needs. While system triggers cannot be modified directly (they can only be enabled or disabled), you can duplicate these triggers to create customizable versions. This allows you to tailor the conditions and behavior of the triggers to better suit your environment.

Editing and Creating Triggers

When you choose to edit an existing trigger or create a new one, you will be presented with several configuration options:

Details

- **Name**: Assign a name to the trigger, which will be displayed in the trigger list.
- **Description**: Provide a description for the trigger to clarify its purpose and conditions.

Conditions

- **Field**: Select the metric you wish to monitor, such as CPU usage, memory load, etc.
- **Operator (Op)**: Determine the condition to evaluate, such as whether the metric is greater than or less than a specified value.
- **Value**: Set the threshold that the metric must reach to activate the trigger. For instance, you might set this to 80% for CPU usage.
- **Interval**: Define how many consecutive times the condition must be met before an alarm is triggered. This setting helps differentiate between transient spikes and persistent issues. For instance, configuring a trigger with a value greater than 80% CPU usage over 6 intervals means:
  - **Real-Time**: While in Real-Time mode only one 3 second interval is honored. For example, if the CPU usage exceeds 80% for one 3 second sample the violation will be highlighted.
  - **History**: The condition persists for 60 seconds (6 intervals, each lasting 10 seconds), indicating a more consistent issue.

    > **Note:** Remember, system triggers are pre-defined and cannot be edited. They can only be enabled or disabled according to your monitoring needs.

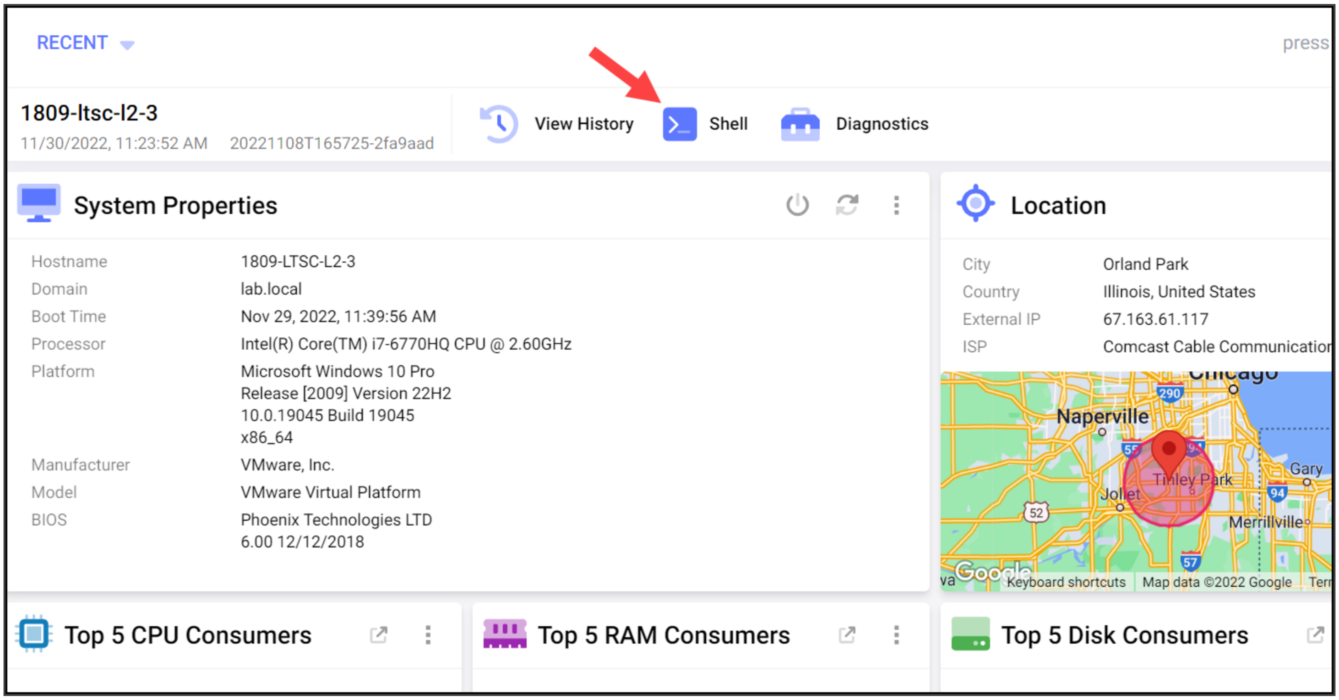
Connect to a Command Line Console Within CommandCTRL

CommandCTRL allows you to connect to an elevated command line Windows console without having to leave the application.

> **Note:** The following is not applicable to Mac support.

Connect from the Dashboard View

To access the command line from the Dashboard view of a machine, click the **Open Shell** button in the top row beside the machine's name.



The console then opens in a popup window.

Connect from the Tools Menu

To connect to the command line console from the Tools menu, complete the following steps:

1. In the side navigation panel, go to **shell** > **Shell**.
2. On the screen that appears, click the **Connect** button.
3. On the popup screen that appears, select the Windows **Powershell** option.
4. In the **Search For Machine** field, enter all or part of the name of the machine you want to install the agent on. As you type, relevant search results appear in a drop-down list below the field.
5. Click to select the machine name from the list.

   The Powershell console then opens.

Support Tasks

Switch Between Tenants

If you belong to more than one tenant, you can quickly switch between them without exiting the CommandCTRL application.

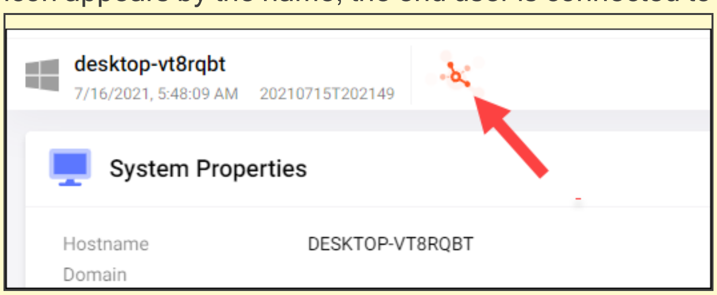
To switch between tenants, complete the following steps:

1. Click your user profile icon in the top right corner of the CommandCTRL screen.
2. In the drop-down field that appears, click the **Switch Tenant** option.
3. On the **Switch Tenant** dialog box that appears, click the name of the tenant you want to switch to.

   The **Switch Tenant** dialog box disappears and you are advanced to the tenant you chose.

Switch Between an End User's Physical and Virtual Machines

If an end user is connected to a physical machine and a virtual machine and both have the CommandCTRL Agent installed, you can switch between them quickly and easily within the CommandCTRL dashboard.

> **Note:** You can tell at a glance if an end user has remote sessions to other machines open by looking at the machine name in the dashboard. If an (**Other Connection**) icon appears by the name, the end user is connected to at least one other machine.
>
> 
>

In order to be able to switch between a physical and a virtual machine, you must be connected to the virtual machine via one of the following methods:

- Remote Desktop Protocol (RDP)

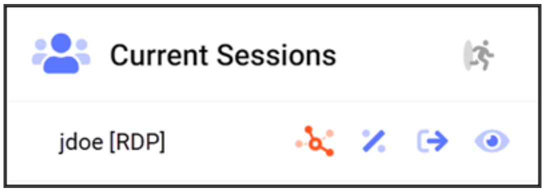
  > **Note:** Supporting Stand Alone RDP, Microsoft CloudPC, and Azure Virual Deskop.

- Citrix (HDX)
- VMware View (PCoIP & Blast)

This process does not currently support connections via Nutanix Frame and AWS Workspaces.

To switch between a physical and a virtual machine, complete the following steps:

1. Use the **Search** or **Recent** fields to locate the end user's machine.
2. In the dashboard view, go to the **Current Sessions** widget and click the (**Other Connection**) icon.



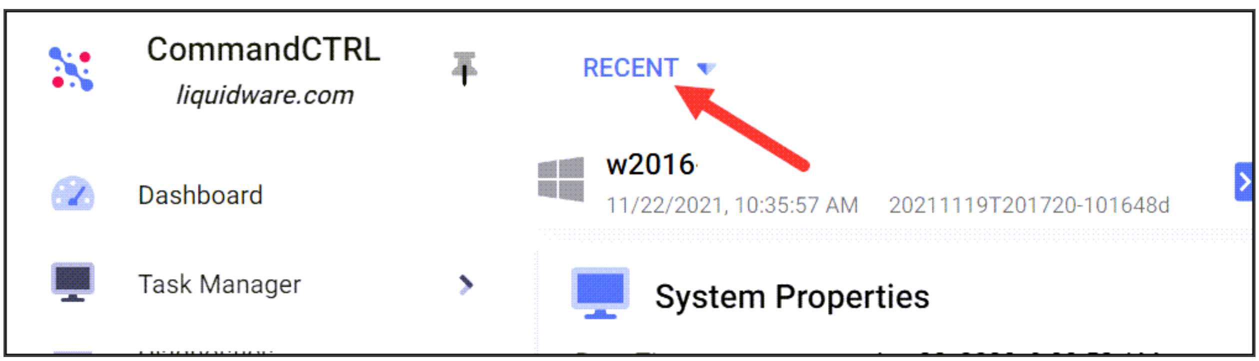
A new browser tab opens, displaying the CommandCTRL dashboard for the virtual machine.

5. To view the dashboard for the original machine again, either click the original browser tab that was open or click the (**Other Connection**) icon in the **Current Sessions** widget for the virtual machine.

Jump to a Page or Machine You Accessed Recently

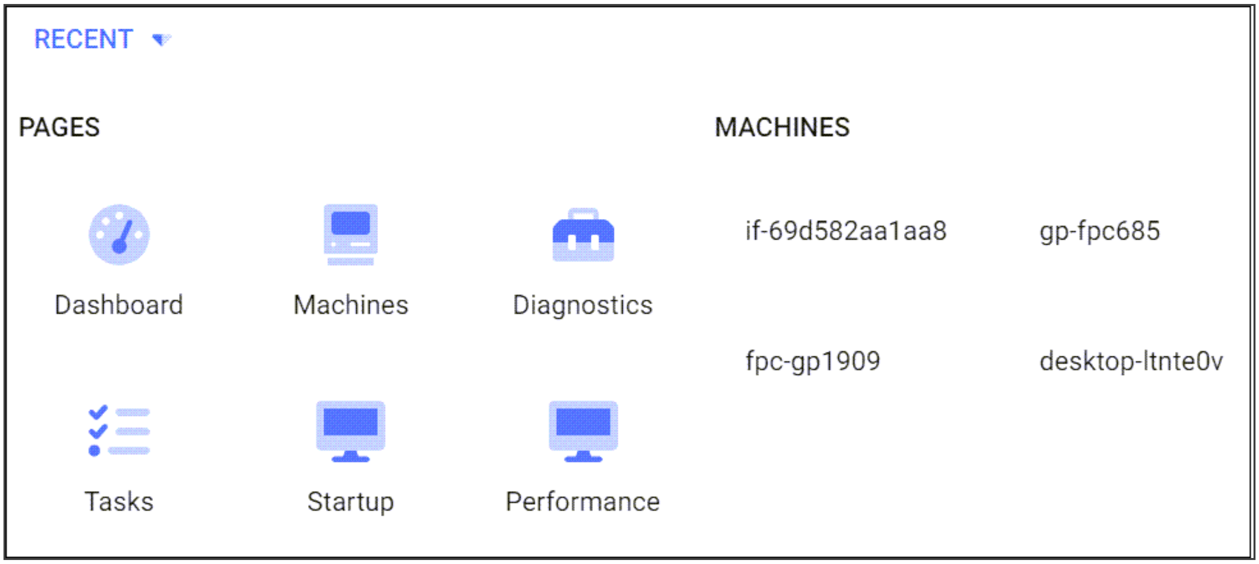
To jump immediately to recent pages or machines you accessed without having to run a search, complete the following steps:

1. Click the **Recent** drop-down link that appears in the top left corner of all CommandCTRL screens other than the shell popup screen.



3. In the expanded view of the **Recent** field that appears, click the page or machine that you want to

jump to.



Switch Between Real-time Mode and History Playback Mode

Real-time Mode Compared to History Playback Mode

By default, CommandCTRL shows the Real-time Mode of an end user's machine. In this mode, the Agent collects machine statistics every 10 seconds and writes them to the local disk. Every five minutes, the Agent compresses those statistics and uploads them to a database in cloud storage.

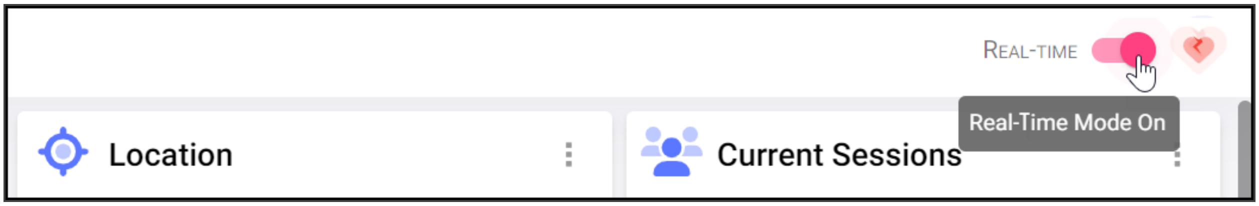
> **Important:** The Agent connects directly to the cloud without going through the control plane. As a result, if the entire control plane goes down, machine statistics continue to upload to cloud storage automatically every 5 minutes. When the control plane comes back online, the CommandCTRL app does an automatic sweep of cloud storage and downloads all of the statistics it missed while it was offline.

In contrast to Real-time Mode, History Playback Mode allows Support to access and review previously recorded sessions on the machine. In History Playback Mode, you can view a 10-second sample of the machine's history every 3 seconds when using normal playback speed or a 10-second sample every 1 second when using high speed playback.

Switching Between Real-time Mode and History Playback Mode

To switch between Real-time Mode and History Playback Mode from within the CommandCTRL user interface, complete the following steps:

1. Use the **Search** or **Recent** fields to locate the machine for which you want to switch the view.
2. In the top right corner of the machine dashboard, click the (**Real-time Mode On**) or (**Real-time Mode Off**) icon.



Note: For a detailed explanation of how to use History Playback Mode, refer to the View a Machine's History via History Playback Mode section of this guide.

View a Machine's History via History Playback Mode

You can view a machine's history using the History Playback Mode feature of CommandCTRL. In History Playback Mode, you can view a 10-second sample of the machine's history every 3 seconds when using normal playback speed or a 10-second sample every 1 second when using high speed playback.

CommandCTRL only tracks machine statistics while the machine is being used. When the machine is turned off or when it is locked, no statistics are collected. Because of this, the history you see might include gaps corresponding to weekends, holidays, or times during the day when the machine was not being used.

Note: When using the History Playback Mode of a machine, all times displayed are determined by the **local time of the Agent**, not the local time of the end-user's machine. So when CommandCTRL users are trying to review events that occurred on machines in other time zones, the CommandCTRL users must calculate what time the event happened in his or her local time. For example, to find an event that happened at noon in Honolulu, a CommandCTRL user accessing an Agent based in New York City would need to view the 6pm block of the timeline because Honolulu is six hours behind New York City.

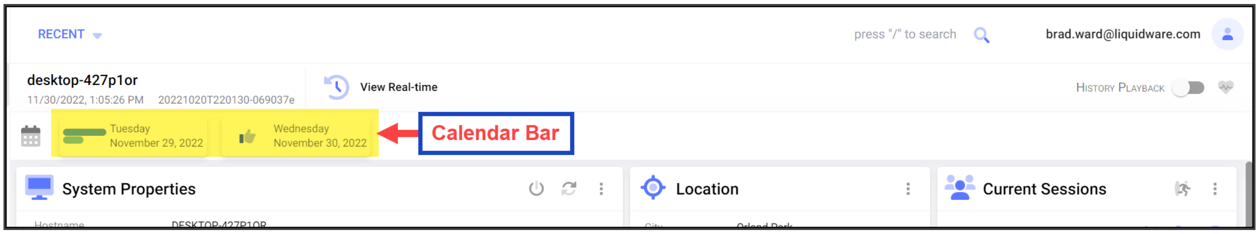
To access the history of a machine, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the Machines screen that appears, locate the machine whose history you want to view, then either click the:
   - Name of the machine.
   - Right-arrow icon located to the far right of the machine.

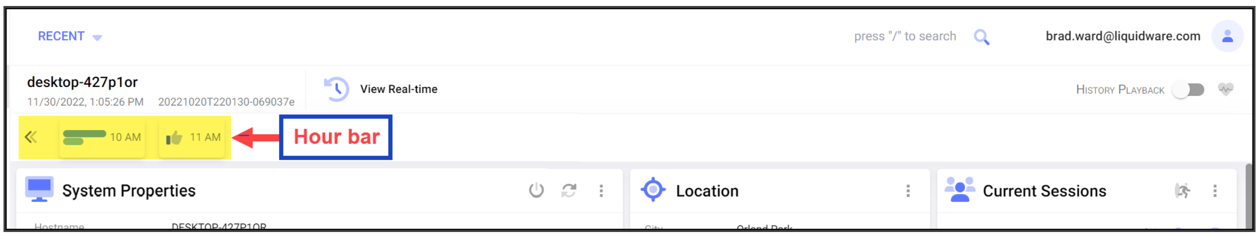
   The dashboard for that machine appears.

3. In the top right corner of the machine dashboard, click the (**Real-Time Mode On**) icon in order to switch Real-time Mode off and to turn History Playback Mode on.

   When History Playback Mode is turned on, a calendar bar appears below the machine name on the dashboard.



6. If the calendar bar already displays the date you want to review, click the **date**. Otherwise, click the (**Calendar**) icon on the left side of the calendar bar and then use the popup calendar screen to select another date range.
7. After you select a date, the calendar bar is replaced by an hour bar that shows all of the hours within the date you selected that you can review the history of. Click one of the hour blocks.

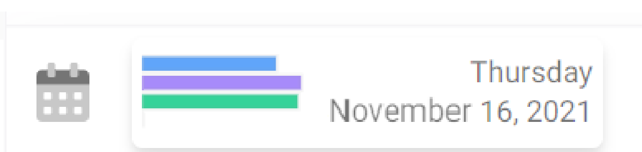


   If there were incidents during the hour block you selected, a color-coded bar or set of bars appears in the hour field.

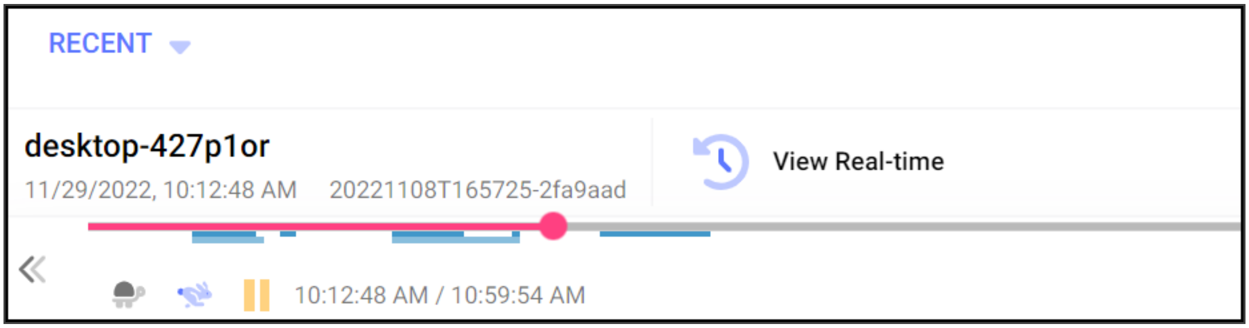
Color	Incident Type
Blue	CPU
Red	Network
Purple	RAM
Green	Disk

   The length of the bar represents the approximate amount of time during the hour that the incident occurred.

   In the example below, a **CPU** incident occurred for approximately 50 minutes of the hour block, while **RAM** and **disk** incidents occurred for the whole hour.



14. After you click an hour bar, it disappears and is replaced by a video control bar.

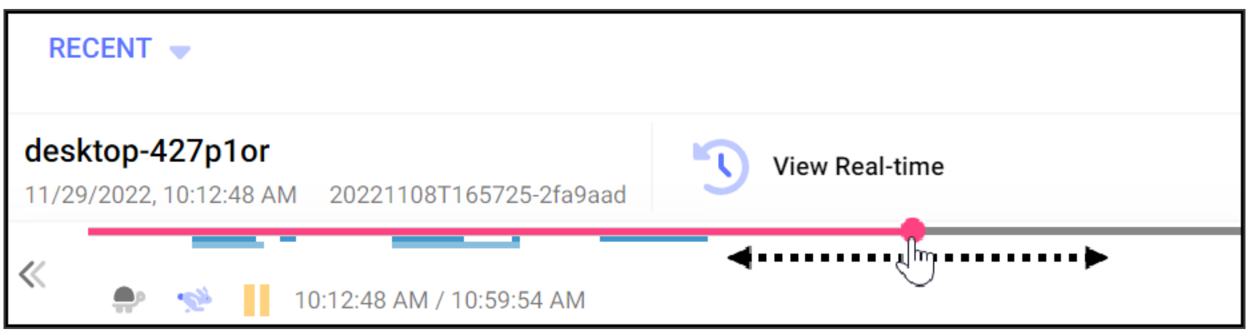


This video control bar contains the following elements:

- A progress bar
- A (**Playback: Slow**) button –Clicking this button then clicking the **Play** button causes the recording to display 10 seconds of machine history every 3 seconds.
- A (**Playback: Fast**) button –Clicking this button then clicking the **Play** button causes the recording to display 10 seconds of machine history every second.
- A (**Play**) button –Clicking this button causes the recording to begin playing at whatever playback speed you selected.
- A (**Pause**) button –Clicking this button pauses the recording. Note that the Pause button only appears after video playback has started.

As the progress bar advances, the statistics in all the fields below will continue to update.

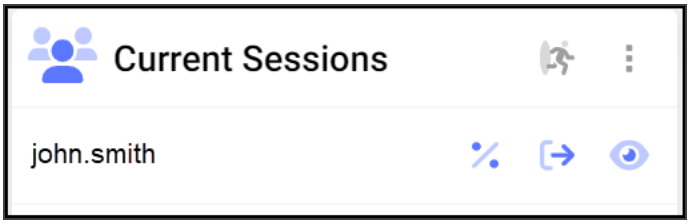
18. To jump to a particular point in time within the hour, click and hold the progress bar circle and drag it to the left or to the right.



View the Environment Variables for a Current Session

To view the environment variables for an end user's current session, complete the following steps:

1. If the end user's machine statistics are not already displayed in your CommandCTRL screen, search for their machine and then click it to make it show up in the dashboard.
2. In the **Current Session** widget in the top right of the machine's dashboard, locate the username of the person whose session variables you want to view. Note that in most cases, there will be only one name listed.



4. Click the (**Environment Variables**) icon in the line belonging to the user.

   An **Environment Variables** screen pops up, displaying a long list of statistics about the current session including, but not limited to, the following data:
   - The machine name
   - The number of processors
   - The operating system
   - The processor identifier
   - The processor level
   - The username

Kill a Process

To kill a process that is currently running on a machine, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine running the process that you want to kill.
3. In the side navigation panel, go to **Task Manager** > **Processes**.
4. On the **Processes** screen that opens, scroll through the list or use the search field to locate the process you want to kill.
5. Click the (**Kill**) icon on the right side of the process row.

Stop, Start, Restart, Disable, or Remove a Service

The tasks of stopping, starting, restarting, disabling, and removing a service are all carried out on the same screen within CommandCTRL. To perform any of these actions, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate and click the name of the machine that is running the service you want to manage.
3. In the side navigation panel, go to **Task Manager** > **Services**.
4. On the Services screen that opens, scroll through the list or use the search field to locate the service you want to manage.
5. Click one of the following icons in the service's row:

- (**Stop**)–Stops a service that is currently running.
- (**Start**)–Starts a service that is not currently running.
- (**Restart**)–Restarts a service that was previously running.
- (**Disable**)–Prevents a service from being able to continue to run on the machine.
- (**Remove**)–Removes a service from the machine.

Block or Unblock a Machine

At times, it might be necessary for a CommandCTRL user to block a machine, which stops the machine from reporting metrics and fulfilling requests. When blocking a machine, you have the option of imposing a temporary block or a permanent block. The main difference is that a permanent block also uninstalls the Agent from the end user's machine.

Temporary Block

A temporary block might be used when an IT department is performing a system upgrade or other system maintenance that would prevent machines from reporting statistics or would lead to machines reporting statistics that are not indicative of the normal state of the machine.

> **Note:** When setting up a time-limited block of a machine, the starting and ending points of the block are determined by **the local time of the Agent**, not the local time of the end-user. So if a CommandCTRL user is logged in to an Agent in New York City and she blocks a machine based in Honolulu until 2 p.m., the block will end at **2 p.m. New York time**, which is 8 a.m. in Honolulu.

Permanent Block and Uninstall

A permanent block might be used if the end user is somehow abusing the system or engaging in actions that could jeopardize system security. In these cases, a CommandCTRL user is able to not only block the offending machine, but uninstall the Agent on that machine remotely to prevent the machine from being able to reconnect.

Blocking a Machine

Whether you are blocking a machine temporarily or permanently, the process is the same.

1. In the side navigation panel, go to **Inventory** > **Machines**.
2. On the **Machines** screen that appears, locate the machine you want to block.
3. Select the checkbox to the left of the machine's name.
4. In the top right corner of the header, click the (**Remove License**) button.

5. On the **Unlicense Machine** screen that pops up, the **Exclude Machine ID** toggler is turned off by default. Click the toggler to turn it on if you want the machine's ID to be permanently excluded from calling back into the system and taking a license. You might need to do this if a machine has become unreachable or if it is being used in a rogue manner.
6. The **Exclude IP Address** toggler is also turned off by default. Click the toggler to turn it on if you want the machine's IP address to be permanently excluded from calling back into the system and taking a license. You might need to do this if a machine has become unreachable or if it is being used in a rogue manner.
7. Decide how long you want to block the current machine.
    - Select the **Block Machine For** radio button if you want to block the machine for a relatively short amount of time. Then enter the number of minutes you want the block to remain in effect.
    - Select the **Block Machine(s) Until** radio button if you want to block the machine for a longer period of time. Then select the end date for the block.
    - Select the **Block Indefinitely** radio button if you want to create an indefinite block of the machine. The machine will remain blocked until you manually remove the block.
8. If you want to remove the CommandCTRL Agent from the machine you are blocking, click the **Do Not Uninstall Agent** toggler to switch it to **Uninstall Agent**.

Unless you are blocking a machine indefinitely, you would most likely not want to turn this toggler on because it will force you to reinstall the Agent when the machine is unblocked.

9. Click the **Block Machines** button.
10. On the **Unlicense Machines** screen that pops up, click **Done** to complete the process of blocking the machine.

Adding a Machine to the Blocked List

This can be used in lieu of Blocking a Machine in cases where you want to manually block a machine.

1. Find the machine you want to block. Note the name of the machine, its Machine ID and IP address.
2. Click the  icon located in banner to the right of the **Search Machines** field.

   An **Add Block** dialog box appears.
3. Enter the Machine name
4. Enter the Machine ID.
5. Enter the IP address.
6. Decide how long you want to block the current machine.
    - Select the **Block Machine For** radio button if you want to block the machine for a relatively short amount of time. Then enter the number of minutes you want the block to remain in effect.

   - Select the **Block Machine(s) Until** radio button if you want to block the machine for a longer period of time. Then select the end date for the block.
   - Select the **Block Indefinitely** radio button if you want to create an indefinite block of the machine. The machine will remain blocked until you manually remove the block.
7. Click **Add Block** in the lower right corner.

   The machine appears in the blocked list.

Unblocking a Machine

Important: If you uninstalled the CommandCTRL Agent when you blocked the machine, you cannot simply unblock it because it no longer appears in the system. To view it in the system, you must install the Agent again and then unblock it using the procedure outlined below.

To unblock a machine that has the Agent installed on it, complete the following steps:

1. In the side navigation panel, go to **Inventory** > **Blocked Machines**.
2. On the **Blocked Machines** screen that appears, locate the machine you want to unblock.
3. Select the checkbox to the left of the machine's name.
4. Choose either method to unblock the machine:
   - In the top right corner of the header, click the (**Remove Block**) icon.
   - On the same line as the machine, to the far right, click the (**Remove Block**) icon.

     The machine is removed from the block machine list.

   Note: Make sure you want to remove the machine from the block list before clicking the or (**Remove Block**) icon because you will not be asked if you are sure before the machine is removed from the list.

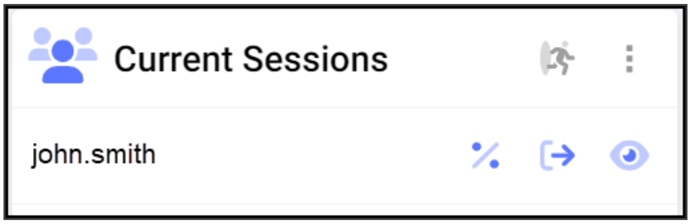
Log a User or All Users Out of a Machine

The CommandCTRL dashboard gives you the ability to log a user out of a machine quickly and easily. If the machine is running Windows 10 Enterprise multi-session or other multi-session hosting software, you have the ability to log all active users out at the same time.

To log a user or all users out of a machine, complete the following steps:

1. If the end user's machine dashboard is not already displayed in CommandCTRL, search for their machine and then click its name to open the dashboard.

2. In the **Current Session** widget in the top right of the dashboard, locate the name of the person who you want to log out.



4. Click the (**Logout**) button beside the person's name. To log everyone out, click the (**Logout All**) button beside the **Current Sessions** header.

Review the Types of Remote Sessions

CommandCTRL users can access an end user's machine remotely using two different methods.

Remote Assist

If a CommandCTRL user is unable to resolve an end user's issues using the functionality built into the CommandCTRL user interface, he or she can initiate a remote session with the end user and access the end user's machine directly.

The Remote Assist option automates the Microsoft Remote Assistance feature built into Windows, and adds new features and a more robust workflow to it. Remote Assist works on all versions of Windows. However, the following requirements must be met in order for it to work correctly:

- The feature must be installed on server OS's being used as desktops. With Windows 10, there is no need to do anything in particular to get it to work correctly. For versions other than Windows 10, the following script should be run in the PowerShell in the base image or on a computer at startup:

  ```
  powershell.exe -executionpolicy bypass Install-WindowsFeature -Name Remote-Assistance
  ```

- The CommandCTRL user and end user machine must be on a routable network.

The CommandCTRL application manages the opening and closing of the firewall ports on the end user's machine automatically.

Go to the Create a Remote Assist Session topic.

Quick Assist

If a CommandCTRL user is unable to resolve an end user's issues using the functionality built into the CommandCTRL user interface, he or she can initiate a remote session with the end user and access the end user's machine directly.

The Quick Assist option works on all Windows 10 versions and Windows 10 Enterprise for Remote Sessions (Win 10 ERS). Quick Assist differs from Remote Assist in the following ways:

- Quick Assist does not require the CommandCTRL user and end user to be on the same routable network.
- With Quick Assist, the CommandCTRL user does not need to install or enable any scripts.
- Quick Assist does not need access to the end user's firewall ports. All connections are made outbound to the cloud.
- Unlike Remote Assist, when using Quick Assist, the CommandCTRL user needs to have a valid Microsoft account. An Office 365 account is sufficient.

With Quick Assist, the CommandCTRL user does not need to install or enable any scripts.

Quick Assist does not need access to the end user's firewall ports. All connections are made outbound to the cloud.

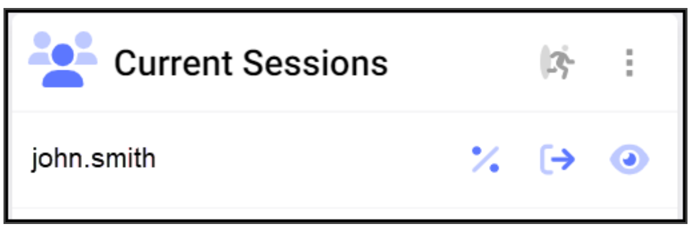
Unlike Remote Assist, when using Quick Assist, the CommandCTRL user needs to have a valid Microsoft account. An Office 365 account is sufficient.

Go to the Create a Quick Assist Session topic.

Create a Remote Assist Session

To initiate a remote assistance session using the Remote Assist option, complete the following steps:

1. If the end user's machine dashboard is not already displayed in CommandCTRL, search for their machine and then click its name to open the dashboard.
2. In the **Current Session** widget in the top right of the dashboard, locate the name of the person who is requesting help.



> **Note:** If the machine is running Windows 10 Enterprise multi-session or other multi-session hosting software, it is possible that multiple user's names will appear in the **Current Sessions** field.

5. Click the (**Remote**) icon in the line belonging to the user.
6. In the drop-down list that appears, select the **Remote Assist** option.
7. After a short delay, the assistant connects to the remote machine and a Connected popup screen appears on your computer. At the same time, a **Windows Remote Assistance** popup window appears on the end user's screen. Although this popup window displays a password for con-

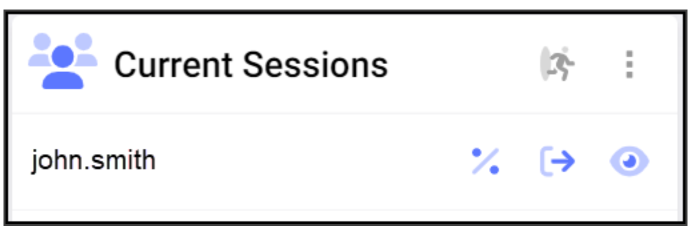
necting the two machines, the same password is visible on your screen, so the end user does not need to provide it to you.

8. Click the (**Download**) icon on the popup screen and then save the **Windows Remote Assistance Invitation** file to somewhere on your computer.
9. Click the **copy** link in the bottom right corner of the password field.
10. Click **Close**.
11. Click the invitation file you downloaded in Step 6, then enter the password you copied in Step 7 and click the **OK** button.
12. At this point, the end user is prompted to allow you to connect to their computer. As soon as they click **Yes**, you are connected to their machine and can see everything they are doing.
13. If you want to request control of the end user's machine, rather than just view it passively, click the **Request control** button at the top of the Windows Remote Assistance window.
14. The end user is then prompted to grant you control of their machine. As soon as they click **Yes**, you are able to see their desktop and can take control of their machine and help solve whatever issue they are dealing with.

Create a Quick Assist Session

To initiate a remote assistance session using the Quick Assist option, complete the following steps:

1. If the end user's machine dashboard is not already displayed in CommandCTRL, search for their machine and then click its name to open the dashboard.
2. In the **Current Session** widget in the top right of the dashboard, locate the name of the person who is requesting help.



> **Note:** If the machine is running Windows 10 Enterprise multi-session or other multi-session hosting software, it is possible that multiple user's names will appear in the **Current Sessions** field.

5. Click the (**Remote**) icon in the line belonging to the user.
6. In the drop-down list that appears, select the **Quick Assist** option.
7. After a short delay, the assistant connects to the remote machine and a **Quick Assist** popup screen appears on your machine.
8. Click the **Assist another person** button at the bottom of the popup screen.
9. Copy the six-digit security code that appears.

10. Provide the security code and the following instructions to the end user via email or chat. To send the instructions, click the image below to highlight it, then right-click and copy the image. Open an email or chat session and paste the image into it.

    a. Click the (**Windows**) icon to open the Start menu.

    b. In the list of applications that appears, scroll down to **Windows Accessories > Quick Assist**. Or simply type **Quick Assist** in the search bar.

    c. Click the **Quick Assist** application to launch it.

       The Quick Assist application opens.

    d. In the **Code from assistant** field, enter the code provided by the CommandCTRL user.

    e. Click the **Share screen** button.

       Your screen will be in waiting mode until the CommandCTRL user connects and then selects a control option. As soon as they make a selection, your screen will display a **Share your screen** field.

    f. Because the CommandCTRL user will be able to see and/or control everything on your computer, you should shut down any non-essential applications and remove any private data you do not want them to see. After doing that, click the **Allow** button.

       Note: To pause the sharing of your screen at any time, click the **Pause** button in the Quick Assist field at the top of your screen. You can also end the session at any time by clicking the **X** in the field and then clicking the **Close** button on the confirmation screen that pops up.

12. As soon as the end user clicks the **Share screen** button in Step 8e above, a sharing option field appears on your machine. Choose from one of the two options, then click **Continue**.
    - **Take full control**—Take full control of the remote computer.
    - **View screen** —View the remote screen without having full control.

    After the end user clicks **Allow** in Step 8f above, you are able to see their desktop and can either view or take control of their machine and help solve whatever issue they are dealing with.

Glossary

Agent

A small application installed on an end user's machine that enables a CommandCTRL user to view the machine's CPU and network statistics and render assistance remotely if necessary.

Block (a machine)

To stop a machine from reporting its statistics to the CommandCTRL Agent and to prevent it from fulfilling any requests from the Agent.

Quick Assist

One of the two ways in which a CommandCTRL user can provide remote assistance to an end user. Quick Assist is cloud-based and does not require the CommandCTRL user and end user to be on the same routable network, nor does it require any software or scripts to be downloaded or enabled.

Remote Assist

One of the two ways in which a CommandCTRL user can provide remote assistance to an end user. Remote Assist is an extension of the Microsoft Remote Assistance feature that is built in to the Windows OS. Although more robust than Quick Assist, Remote Assist has more requirements for usage: the CommandCTRL user and end user must be on the same routable network and Windows versions other than Windows 10 require the installation of a script in the base image or on a computer at startup.

Tag

A user-provided identifier for a script or trigger, used to categorize the script/trigger and make it easier to locate when conducting searches in the system. An example of a script tag could be **Windows**, which would help users find all Windows-related (and Windows-tagged) scripts in the system.

Tenant

Similar to the concept of an account. It is used to identify all users within that account instance. The users that are part of a tenant could be from the same organization or invited from outside organizations.

Tenant Owner

The person who initially creates a tenant and who invites others to join it.