Cloud Topology

Quick Guide

v8.2

Document Version: 1

Contents

Contents

Introduction

This guide is intended to help users implement ControlUp's system. Click here to skip the introductory chapters and go straight to configuration.

ControlUp is a tailor-made and comprehensive monitoring system for IT administrators and helpdesk personnel who oversee multi-user environments. In those roles, you are required to prevent and troubleshoot performance issues, application failures, and operating system errors. Typically, these tasks require repetitive and time-consuming execution on existing consoles, scripts, and various management tools.

As a system administrator your two primary goals are to:

- Quickly identify issues in a complex multi-user environment
- Resolve these issues simply and efficiently

ControlUp's solution is a comprehensive monitoring, management, and remediation system. It provides deep visibility into the real-time activity of servers, workstations, user sessions, and the applications they run, along with the tools to manage and fix any issues that arise, so you can more easily reach these goals.

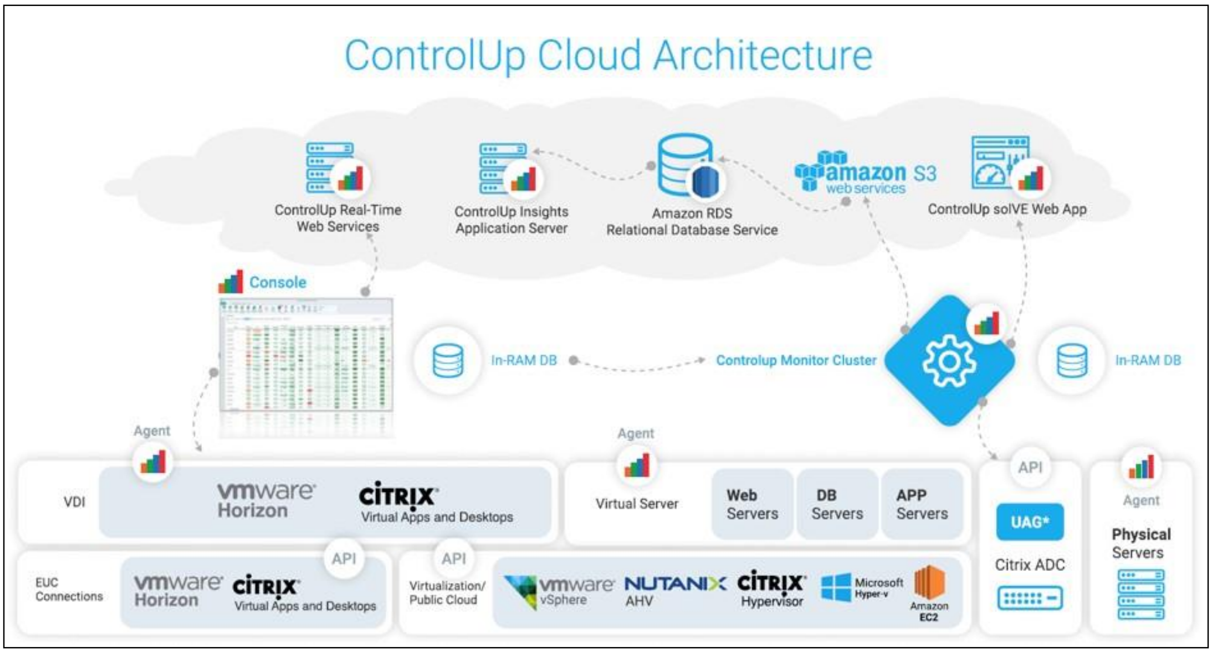
ControlUp Architecture

ControlUp supports various topologies, based on your requirements. For complete details regarding sizing guidelines, see here.

ControlUp Hybrid Cloud Topology

ControlUp Hybrid Cloud topology is enabled by default (requiring a network with internet connectivity). In this topology, ControlUp's back-end components are hosted on secure Amazon Web Services Cloud servers, while the ControlUp Console and Monitor modules run inside the enterprise network.

The following figure illustrates the ControlUp Cloud-Based topology:



Main ControlUp Modules

The ControlUp system provides the following main modules:

- **ControlUp Console** - The real-time monitoring ControlUp Console gathers and displays a wealth of current information regarding system health and performance, allowing powerful management actions to be executed to enable resolving issues and changes to system configurations. The console module is a live, spreadsheet-like grid that can be customized and configured to suit your requirements. The console grid contains metric columns, that can be sorted and double-clicked to navigate across large systems.
- **ControlUp Monitor -** The ControlUp Monitor assists with monitoring your assets 24/7 and alerting about any abnormal behavior according to a customizable set of incident triggers. It is like the ControlUp Console, but without an interactive user interface. Once installed and launched, the monitor connects to the managed assets of your organization and starts receiving system information and performance updates, just like an additional ControlUp Console user. The ControlUp Monitor is a requirement for using SOLVE.
- **ControlUp Insights** - The ControlUp Insights module is a reporting and analytics platform that accumulates activity and performance data over time and displays it over a variety of reports and dashboards. This enables the systems administrator to investigate past issues, track usage trends, analyze the system's performance, and make decisions regarding future system design and configuration.

- **ControlUp SOLVE** – The SOLVE module is a powerful and comprehensive, real-time monitoring and analysis tool that is accessible in a hosted web application. Accessing via a web interface means there's less resource consumption on the endpoints that are logging in and viewing the data, giving you and your users a leaner, more performance-driven experience. SOLVE's modern web interface also provides historical data for some available metrics.
- **Data Collectors** - The Data Collector is responsible for collecting metrics from 'external' sources such as VMware vCenter, Citrix Delivery Controllers, XenServer Poolmasters, AHV Clusters, and NetScaler appliances. Having a data collector increases the performance capabilities of both the console & monitor.
- **ControlUp Agent** - The ControlUp Agent is a lightweight component that enables rapid deployment and a minimal performance footprint on the managed computer.

ControlUp Prerequisites

The following is a set of prerequisites for the consoles, monitors, data collectors, agents, and hypervisors, to ensure the smooth installation and operation of ControlUp.

Console Prerequisites

The only software prerequisite for the console to run properly is Microsoft .NET 4.5. or later. Please ensure this prerequisite is met before running ControlUp.

Supported operating systems:

- Windows 7
- Windows 8 and 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Required open ports:

- Communication Ports used by ControlUp for Hybrid Cloud.

If you have an outbound proxy, the necessary ports and URLs are described here.

Monitor Prerequisites

Supported operation systems:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Required installed software:

- Net Framework 4.5 (.Net Framework 4.7.2 or later recommended)
- PowerShell 5.0 (for Windows PS API)

Required open ports:

- Communication Ports used by ControlUp for Hybrid Cloud.

If you have an outbound proxy, the necessary ports and URLs that are needed are described here.

Required permissions:

- The monitor's primary AD account requires the **Log on Locally** user right on the monitor service VM. The service account is defined in the monitor **Settings-> Domain Identity** tab. Therefore, you should verify the following:
  - The account has the **Allow log on locally** user right.
  - The account is not part of the **Deny log on locally** user right.

Data Collector Prerequisites

Supported operating systems:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Required installed software:

- ControlUp Agent
- Net Framework v4.5 (.Net Framework 4.7.2 or later recommended)
- When connecting a XenDesktop site (Citrix Virtual Apps and Desktops), the Citrix SDK must be deployed to the Data Collector to connect to the Citrix API.
- The SDK is available from the following here.

Required open ports:

- Depending on the type of Hypervisor/EUC site, the following ports will need to be open:
  - **Citrix XenServer** - Port 80 - open between the console/monitor/data collector and the XenServer hosts
  - **vSphere -** Port 443 - open between the console/monitor/data collector and the vCenter Appliance
  - **Nutanix** - Port 9440 - open between the console/monitor/data collector and the Nutanix AHV Prism appliance
  - **HyperV** - Port 40705 (HyperV is utilizing the same port as the ControlUp Agent)
  - **NetScalers** - 80/443

Note: A pair of data collectors can be provided for high availability purposes. In the event of a failure of the data collector, a backup data collector assumes this role until the data collector is brought back online.

Agent Prerequisites

Supported operating systems:

- Windows 7
- Windows 8 (or 8.1)
- Windows 10
- Windows Server 2008 + R2 (Full installation only. Core edition is not supported)
- Windows Server 2012 R2
- Windows Server 2016 (Core or Full Installation)
- Windows Server 2019

Required installed software:

- Microsoft .NET Framework 3.5 or Microsoft .NET Framework 4.5 (.Net Framework 4.7.2 or later recommended)

Required open ports:

- A single configurable TCP port open (40705 by default) for agent communication.

Active directory & DNS prerequisites:

- Active Directory is a prerequisite for managing machines using ControlUp.

Note: If your network includes machines that are not joined to a domain, you can connect to these machines, however, other actions are not available.

Note: ControlUp requires RPC access for the remote agent installation. If your managed machines are inaccessible using RPC, you can deploy the ControlUp agent using an MSI package. For details, see Auto Adding Machines Installed with the MSI Package .

Hypervisor Monitoring Prerequisites

The following section describes the prerequisites for monitoring Hypervisors with the ControlUp Console and Monitor.

Supported hypervisor platforms:

- vSphere 6.x environments that are managed by vCenter. (Standalone ESX/ESXi servers are not supported.)
- Nutanix AHV 5.5 & 5.6
- Citrix Hypervisor (XenServer) v6.1 (with the Performance Monitoring Enhancement Pack, CTX135033), v6.2., v7.x and v8.x
- Microsoft Hyper-V 2012 R2, Microsoft Hyper-V 2016 including standalone & clustered hosts

Specific requirements for each are listed below.

Note: For earlier versions, some performance columns not yet implemented in XenServer might be displayed as N/A.

Note: The ControlUp Agent must be installed on the Hyper-V host to monitor them as hypervisors (the console does not work on any version of Core, however, the Agent functions as long as you have .Net 3.5.1 or .Net 4.6.2 installed).

Required open ports:

ControlUp Console to vSphere, vCenter	TCP /443
ControlUp Console to Nutanix/AHV	TCP /9440
ControlUp Console to Citrix Hypervisor Controllers	TCP/80
ControlUp Console to HyperV	TCP /40705 (via the ControlUp Agent)

VMware vSphere Prerequisites

Required vCenter permissions:

- The Read-Only role is sufficient for all monitoring purposes. If you want to be able to use the built-in hypervisor-based VM power management functions, then you will need to create a custom role based on the Read-Only role, adding the following permissions:

In the Virtual Machine/Interaction category:

- Power Off
- Power On
- Reset

vSAN Prerequisites

To retrieve vSAN metrics and metadata, follow the following prerequisites.

Required installed software:

- PowerShell minimum Version 5.0 (with RemoteSigned execution policy)
- VMware PowerCLI 10.1.1.x
- .NET framework version 4.5 (.Net Framework 4.7.2 or later recommended)

Required vCenter permissions:

- vSAN Performance service should be turned on.
- The user account configured for the hypervisor connection requires **storage.View**.

Citrix Hypervisor (XenServer) Prerequisites

Required Citrix Hypervisor permissions:

- If Active Directory authentication is enabled for the Citrix Hypervisor pool, then the Read-Only role is sufficient.
- If you would like to be able to use the built-in hypervisor based VM power management functions, you will need to upgrade the user role to **VM Operators**.

Nutanix Prerequisites

Required Nutanix permissions:

- The user/service account needs to have a **Viewer** role for view-only capabilities, which is the user to be used for connecting your console to the hypervisor.
- To perform VM power management & host maintenance actions, you must configure the user/service account with the **Cluster Admin** role.

To use a dedicated user/service account already configured in your environment, you'll need to add your organizational Active Directory to Nutanix.

Configuring a ControlUp Organization

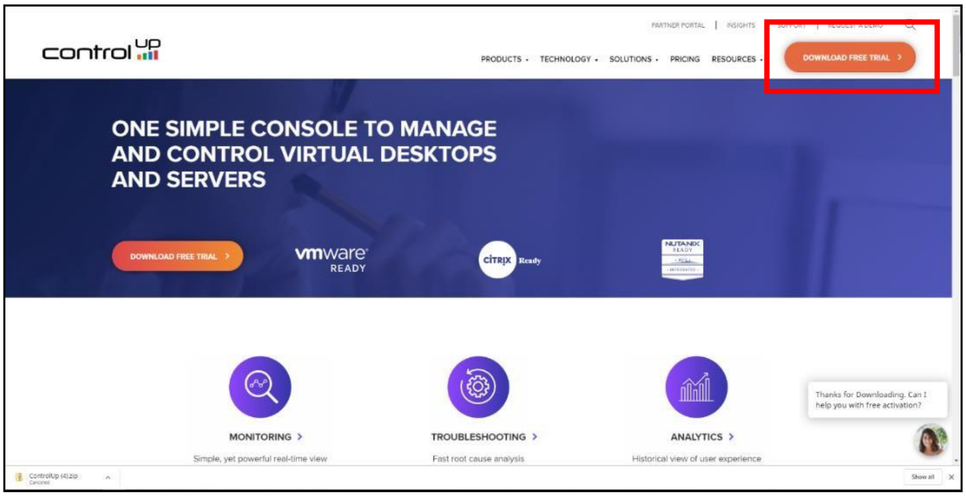
This section covers the actions required for getting ControlUp up and running in your organization and populated with hosts, machines, monitors and more. Throughout this section, if you find some terms that you are not yet familiar with, refer to the Glossary section.

Downloading the ControlUp Console

The ControlUp Console requires downloading, without any other additional installation steps.

To download the console:

Go to this link, or go to www.controlup.com and click **DOWNLOAD FREE TRIAL** and unzip the file once it has downloaded.



Launching the ControlUp Console

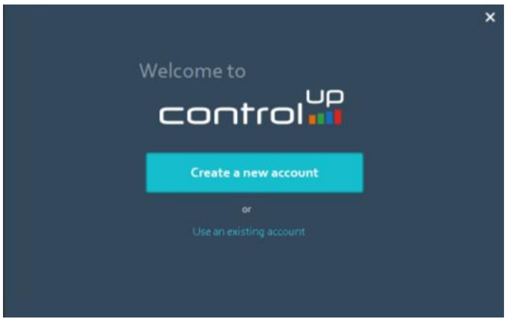
To launch the ControlUp Console, double-click the **ControlUpConsole.exe** and begin creating your User Account and Organization.

Creating a User Account

To start working with the ControlUp Console, you have to create a ControlUp user account. Follow these steps to create your ControlUp account.

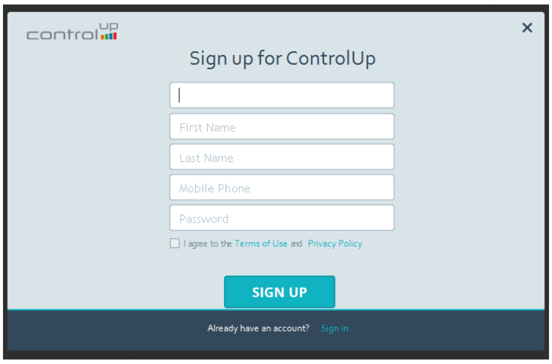
Note: ControlUp requires internet connectivity for the sign-in process.

Upon opening the ControlUp console for the first time, the following screen displays:



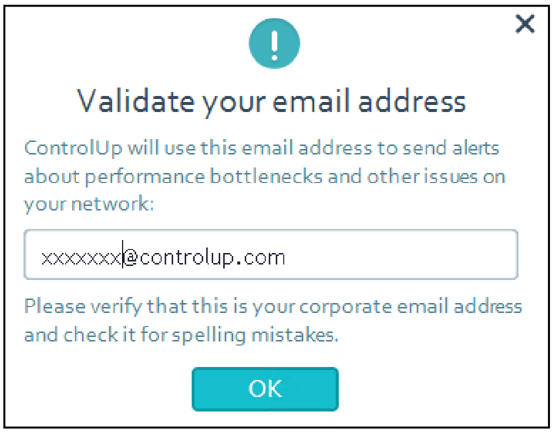
To Create the user account:

1. Click **Create a New Account** and fill out the following form:


controlUP
Sign up for ControlUp
First Name
Last Name
Mobile Phone
Password
□ I agree to the Terms of Use and Privacy Policy
SIGN UP
Already have an account? Sign in

2. Provide a valid email address, your contact details, and a password.
3. Select the check box to agree to the **Terms and Conditions.**
4. Click **Sign Up** and a confirmation message with an activation link is sent to your email.

   Once you click **OK**, the Console launches but the user still needs to be activated.



Validate your email address

ControlUp will use this email address to send alerts about performance bottlenecks and other issues on your network:

xxxxxxx@controlup.com

Please verify that this is your corporate email address and check it for spelling mistakes.

5. Click the activation link that was sent to you to activate your account.

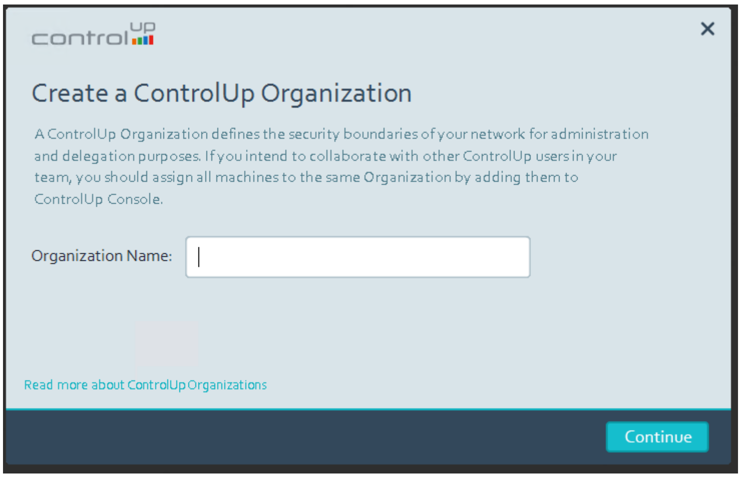
Creating a ControlUp Organization

ControlUp organizations are entities that represent groups of machines managed by the same administrative personnel. Once an organization is created, new ControlUp Users may join the same organization so they can manage and monitor the same environment.

To create a ControlUp Organization:

1. Choose an **Organization Name** and Click **Continue** and the ogranization creation process begins.

   ***Tip**: Choose a clear and descriptive organization name as this will allow future ControlUp Users from your company to easily recognize the organization when they sign in to ControlUp.*



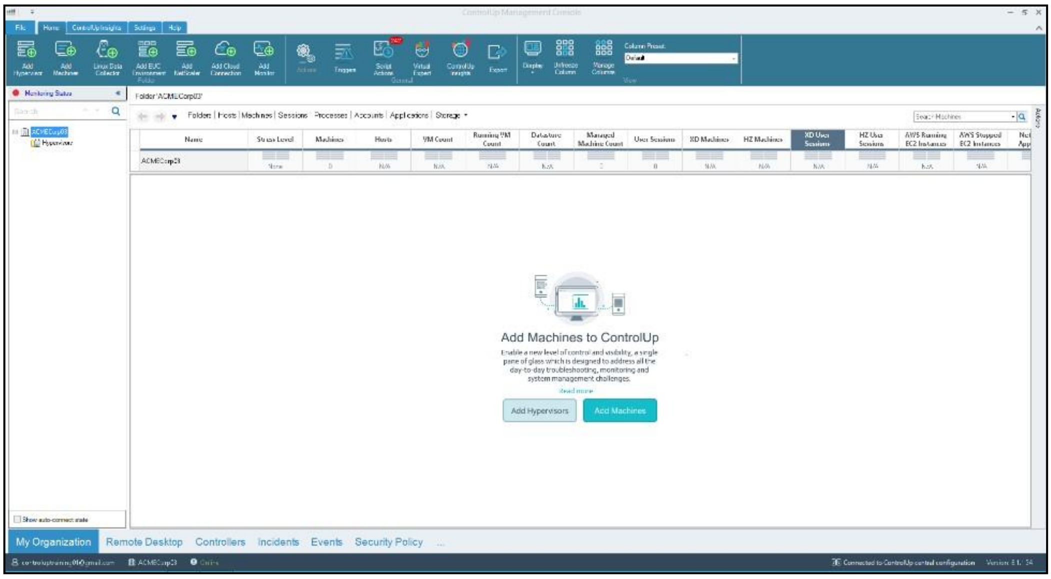
Create a ControlUp Organization

A ControlUp Organization defines the security boundaries of your network for administration and delegation purposes. If you intend to collaborate with other ControlUp users in your team, you should assign all machines to the same Organization by adding them to ControlUp Console.

Organization Name: |

Read more about ControlUp Organizations

2. Once the new organization is created, the ControlUp Console application launches, and the initial screen appears.



Add Machines to ControlUp

Enable a new level of control and visibility, a single pane of glass which is designed to address all the day-to-day troubleshooting, monitoring and system management challenges.

Adding Managed Machines

To add Machines in ControlUp, two distinct operations are required:

1. Adding the machine to the ControlUp organization.
2. Deploying the ControlUp Agent on the machine.

Each of these actions can be completed either manually or automatically as follows:

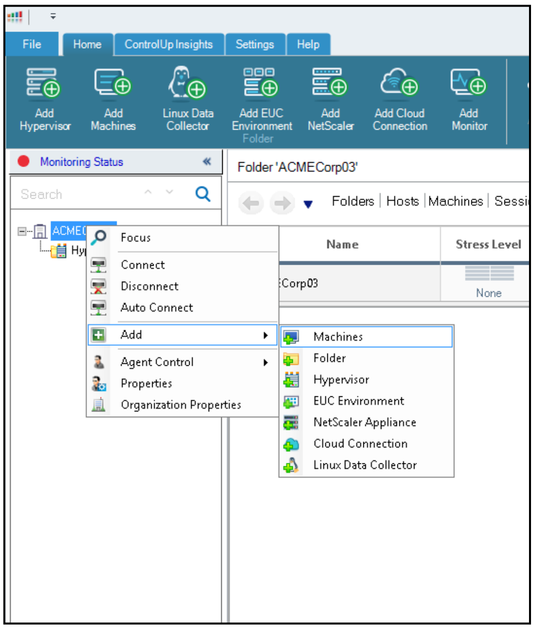
- **Manually** – Using the ControlUp Console
- **Automatically** – Using PowerShell scripts and an MSI package

This section covers the required steps for each operation.

Adding Managed Machines Manually to the Console

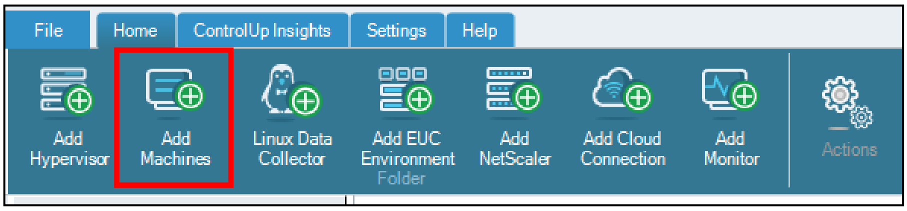
To add a managed machine manually:

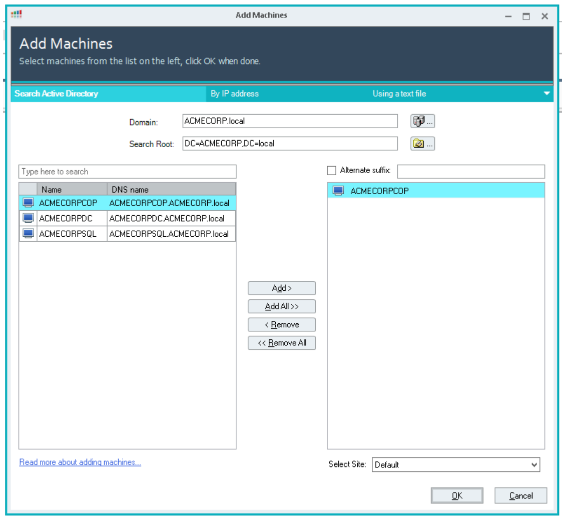
1. Open the **Add Machines** window by right-clicking the Root Folder or any other folder in the organizational Tree and select **Add** > **Machines** and the Add Machines window appears:



For more information regarding ports, see here.

2. Alternatively, you can click **Add Machine** in the Home ribbon and the Add Machines window appears:





Add Machines

Select machines from the list on the left, click OK when done.

Domain: ACMECORP.local

Search Root: DC=ACMECORP,DC=local

Type here to search

Name	DNS name
ACMECORPCOP	ACMECORPCOP.ACMECORP.local
ACMECORPDC	ACMECORPDC.ACMECORP.local
ACMECORPSQL	ACMECORPSQL.ACMECORP.local

☐ Alternate suffix:

ACMECORPCOP

Read more about adding machines...

Select Site: Default

To select a machine from your active directory:

1. Click the **Domain** selector button to choose a domain containing the names of the machines to be added.
2. Choose a root OU for the Active Directory search using the **Search Root** selector.
3. Search for the machines you want to add and select them from the Search tab.

   Tip: *Typing text inside the Search Filter box performs inline filtering of the result table, which allows for faster location of machine accounts. The text that you type in the Search Filter box can be any part of the machine name and does not require the use of wildcard characters.*
4. Select the machines and click **Add** or **Add All.**
5. Click **OK** and the Machines are added to the Organizational Tree.

By default, once a machine is added to the organizational tree, the ControlUp Agent is installed automatically on that machine. However, ControlUp also allows you to disable the automatic installation of the agent in cases where you would like to manually control and initiate the installation process.

Optional: To disable the automatic installation of the agent:

1. Go to the Settings tab and click **Agent** and the **Agent Deployments** setting screen appears.

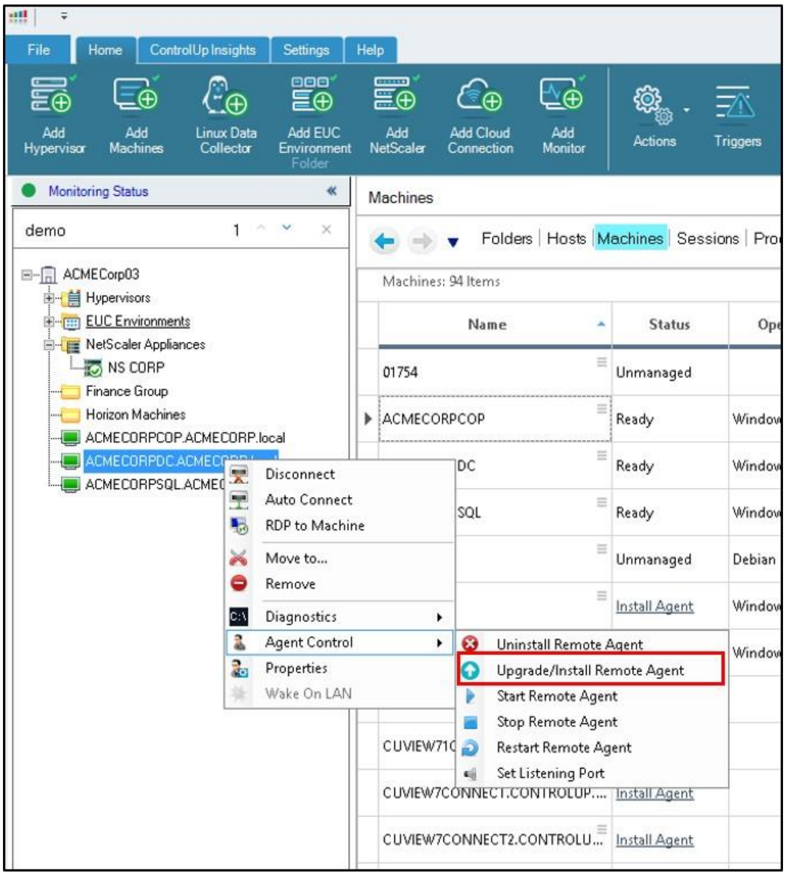
2. Uncheck the **Deploy Agents Automatically** option and the automatic installation of the agent is disabled.

Once this function is disabled, you must install the agent remotely via the ControlUp Console. To push the agents to the remote machines, the AD user you are logged in with when starting the console must have administrative permissions on the remote machine. To receive administrative permissions, contact your IT administrator.

Deploying the Agent Manually

To install the agent remotely:

In the organizational tree, right click the machine you want to install the agent on and select **Agent Control** and then **Upgrade/Install Remote Agent**.



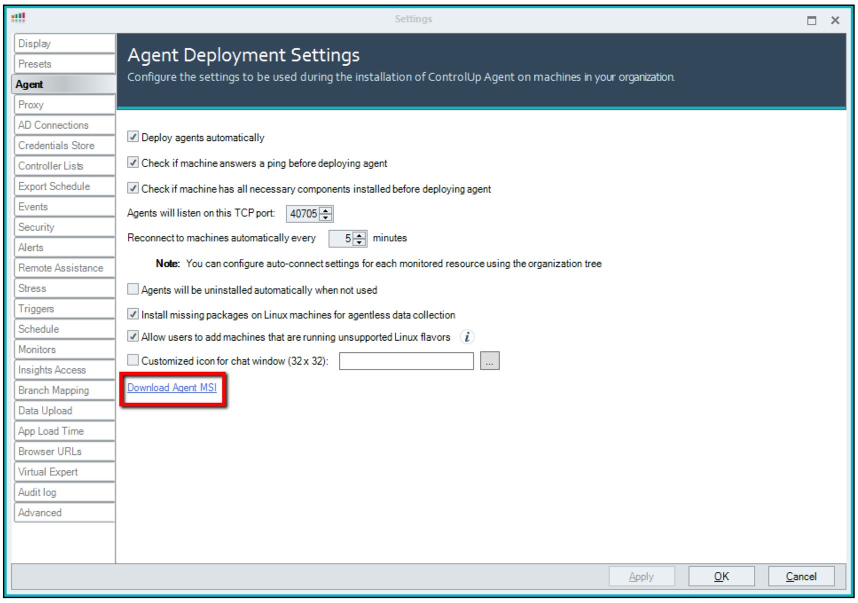
It is also possible to install the agent remotely to several machines by multi-selecting them by holding the CTRL key and right-clicking over a folder.

Deploying the Agent MSI Package on a Golden Image

ControlUp enables you to deploy the ControlUp Agent onto a golden image using the ControlUp **Agent MSI package**, as well the ability to distribute the **Agent MSI Package** in advance to machines, using SCCM or other similar systems, logon scripts, or via a group policy.

To install the MSI package:

1. Download the package from this link or from the console by selecting the **Settings** tab and then selecting **Agent** and clicking **Download Agent MSI**.



Agent Deployment Settings

Configure the settings to be used during the installation of ControlUp Agent on machines in your organization.

☑ Deploy agents automatically

☑ Check if machine answers a ping before deploying agent

☑ Check if machine has all necessary components installed before deploying agent

Agents will listen on this TCP port: 40705

Reconnect to machines automatically every 5 minutes

Note: You can configure auto-connect settings for each monitored resource using the organization tree

☐ Agents will be uninstalled automatically when not used

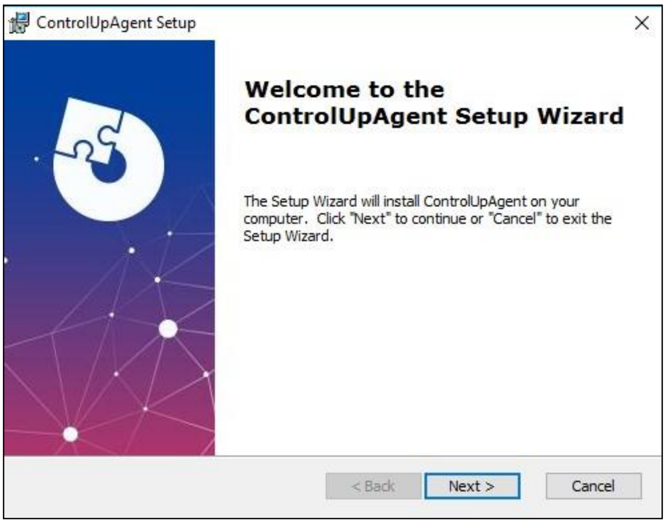
☑ Install missing packages on Linux machines for agentless data collection

☑ Allow users to add machines that are running unsupported Linux flavors

☐ Customized icon for chat window (32 x 32):

Download Agent MSI

2. Install the MSI package on the golden image using the setup wizard. No other configurations required.



Welcome to the ControlUpAgent Setup Wizard

The Setup Wizard will install ControlUpAgent on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

To add a machine to the organizational tree and start monitoring it, follow the steps in the Adding Managed Machines section or use a PowerShell script to add the machines automatically as described in the next section.

Note: When adding machines to a Horizon EUC Environment, refer to Adding EUC Environment.

Adding Machines Automatically to the Real Time Console (via PowerShell)

Using this method, prior to adding the machine to the console, you must install the **Agent MSI Package** on a golden image to start monitoring the machine. To streamline the process of adding machines with the Agent MSI package installed, a PowerShell script can be used. ControlUp includes several PowerShell cmdlets to provide automation capabilities for manipulating the organizational tree.

Secure Communications Between ControlUp Console/Monitor and ControlUp Agent

To secure the communication between the installed agent and the ControlUp environment, we recommend you do the following.

1. On any computer running the ControlUp agent, enable a Firewall inbound rule that allows access to port **40705** only to authorized computers.
2. Add these computers which ideally should use static IP addresses:
    - Computers running the ControlUp Monitor service
    - Computers running the ControlUp Console

If you do not have a firewall for your network, we recommend using the built-in Windows firewall alongside a Group Policy to apply the firewall rule to all machines running the ControlUp Agent.

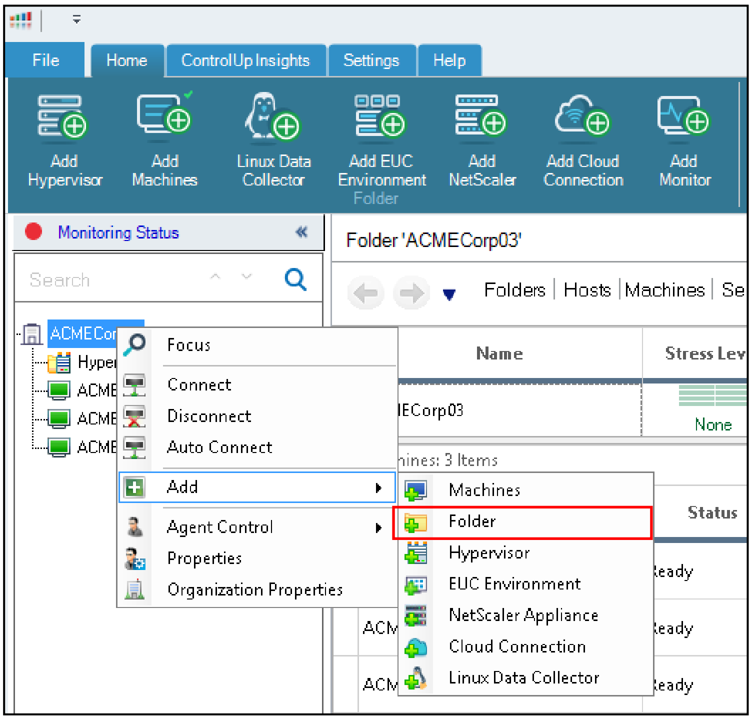
Note: This recommendation reduces the risk of a potential attacker manipulating a ControlUp Agent using malicious code in case that potential attacker has penetrated the organization network.

Creating a Folder

After adding managed machines into ControlUp, it is recommended to create a folder tree that reflects the structure of your network.

To create a folder:

1. Right-click the root folder you would like to add an additional folder under and select **Add** from the available options.
2. From the submenu click the **Folder** option and a new folder is created.



3. Enter a descriptive name for better distinction between the folders and their purposes.

Adding a Monitor

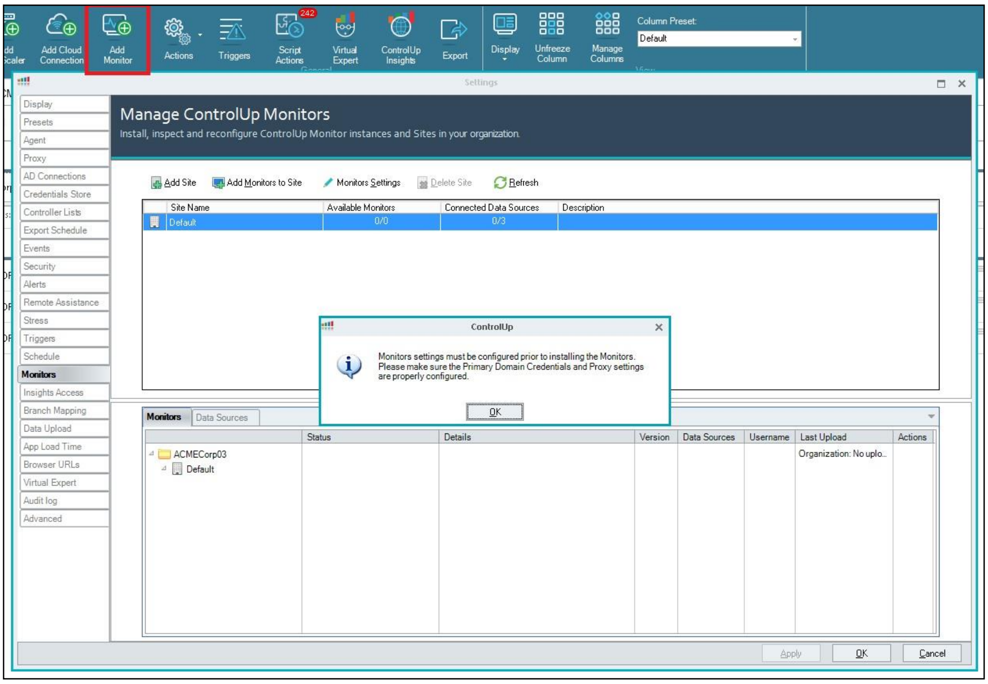
A monitor is a Windows service that allows for continuous monitoring of the system resources. It is a mandatory component for using SOLVE. For sizing recommendations for the ControlUp Monitor, see the ControlUp Monitor Guidelines section. Support for large organizations is implemented by the **Monitor Cluster** feature, which enables multiple ControlUp Monitors to work together to monitor a single organization.

Prior to installation, choose a machine or virtual machine that is correctly sized for your needs and the size of your environment. Make sure this machine can be dedicated to only running the ControlUp Monitor service and make sure that you have RPC Access to the selected machine.

It is also recommended to create a dedicated service account with local admin permissions on all managed machines.

To install a monitor:

1. Click **Add Monitor** in the Home ribbon to start the ControlUp Monitor Installation Wizard.



Manage ControlUp Monitors

Install, inspect and reconfigure ControlUp Monitor instances and Sites in your organization.

Site Name	Available Monitors	Connected Data Sources	Description
Default	0/0	0/3	

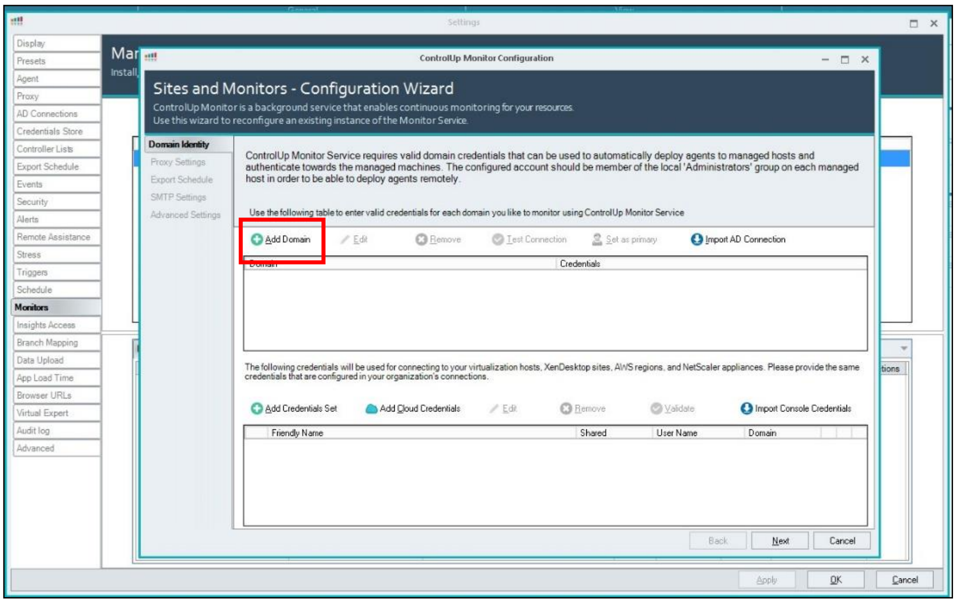
ControlUp

Monitors settings must be configured prior to installing the Monitors. Please make sure the Primary Domain Credentials and Proxy settings are properly configured.

OK

	Status	Details	Version	Data Sources	Username	Last Upload	Actions
ACMECorp03						Organization: No uplo...	
Default							

2. Click **OK** on the popup message and the **Sites and Monitors – Configuration Wizard** appears.



Sites and Monitors - Configuration Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

ControlUp Monitor Service requires valid domain credentials that can be used to automatically deploy agents to managed hosts and authenticate towards the managed machines. The configured account should be member of the local 'Administrators' group on each managed host in order to be able to deploy agents remotely.

Use the following table to enter valid credentials for each domain you like to monitor using ControlUp Monitor Service

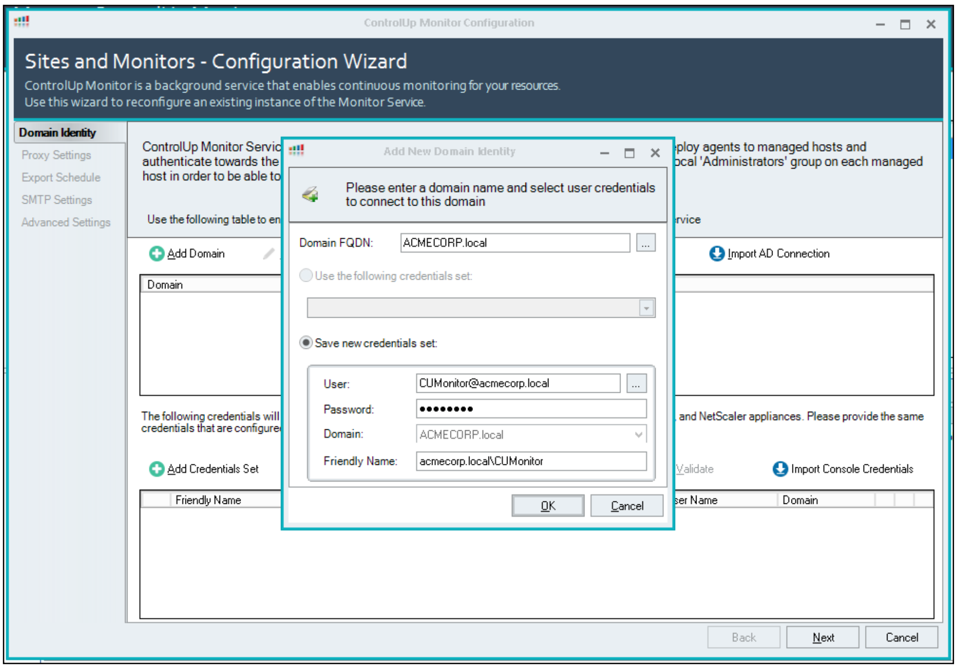
Domain	Credentials

The following credentials will be used for connecting to your virtualization hosts, XenDesktop sites, AWS regions, and NetScaler appliances. Please provide the same credentials that are configured in your organization's connections.

Friendly Name	Shared	User Name	Domain

The first configuration task for the monitor cluster is to add valid domain credetials that are used by the monitor cluster to connect to managed computers, and, optionally, deploy the ControlUp agent.

3. Click **Add Domain** and the Add New Domain Identity popup appears.



ControlUp Monitor Configuration

Sites and Monitors - Configuration Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

Add New Domain Identity

Please enter a domain name and select user credentials to connect to this domain

Domain FQDN: ACMECORP.local

○ Use the following credentials set:

● Save new credentials set:

User: CUMonitor@acmecorp.local

Password: ••••••••

Domain: ACMECORP.local

Friendly Name: acmecorp.local\CUMonitor

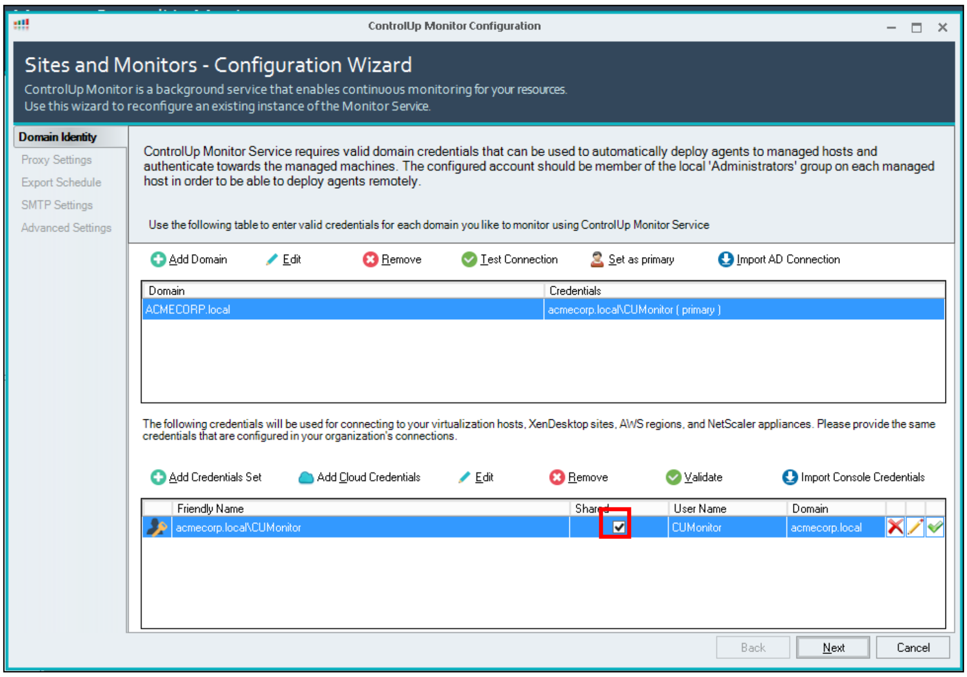
Domain Identity
Proxy Settings
Export Schedule
SMTP Settings
Advanced Settings
ControlUp Monitor Servic
authenticate towards the
host in order to be able to
ploy agents to managed hosts and
ocal 'Administrators' group on each managed
Use the following table to en
rvice
Add Domain
Import AD Connection
Domain
The following credentials will
credentials that are configure
and NetScaler appliances. Please provide the same
Add Credentials Set
Validate
Import Console Credentials
Friendly Name
ser Name
Domain
OK
Cancel
Back
Next
Cancel

Enter the Domain FQDN and valid domain credentials. It is recommended that the domain account be a member of the local administrator group to deploy agents remotely.

4. Check the **Shared** credentials for each credential set. See Configuring Shared Credentials Prerequisites for this option to work.

5. *Optional:* If you want to add additional credentials for hypervisor connections or EUC environment connections:

   - Click **Add Credentials Set** and the Add New Credentials popup appears.
   - Enter the relevant information and click **OK** and the credentials are added.



ControlUp Monitor Configuration

Sites and Monitors - Configuration Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

ControlUp Monitor Service requires valid domain credentials that can be used to automatically deploy agents to managed hosts and authenticate towards the managed machines. The configured account should be member of the local 'Administrators' group on each managed host in order to be able to deploy agents remotely.

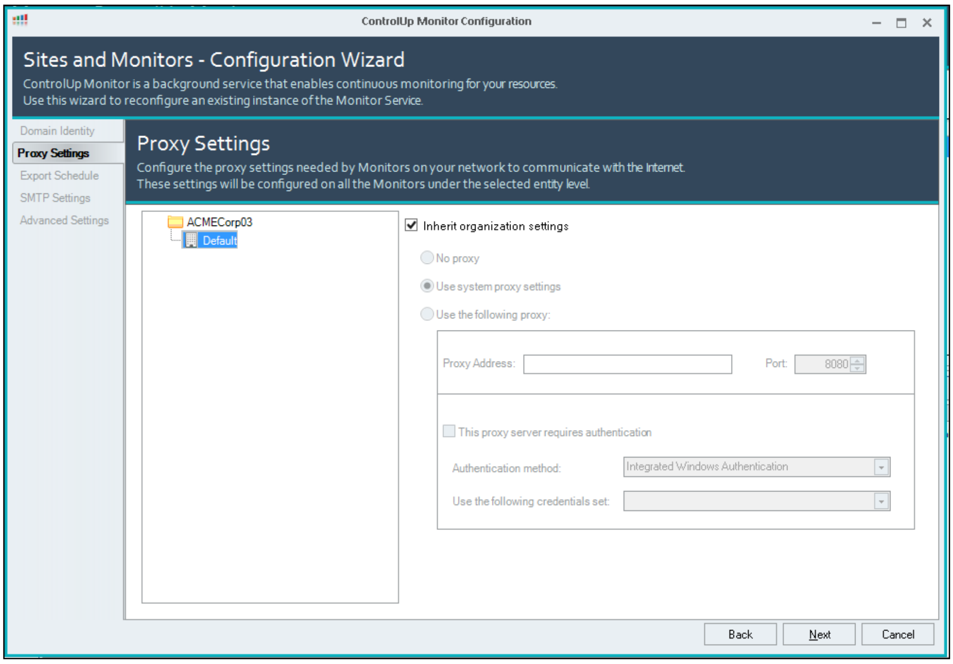
Use the following table to enter valid credentials for each domain you like to monitor using ControlUp Monitor Service

Domain	Credentials
ACMECORP.local	acmecorp.local\CUMonitor (primary)

The following credentials will be used for connecting to your virtualization hosts, XenDesktop sites, AWS regions, and NetScaler appliances. Please provide the same credentials that are configured in your organization's connections.

Friendly Name	Shared	User Name	Domain
acmecorp.local\CUMonitor	☑	CUMonitor	acmecorp.local

6. Click **Next** and the Proxy Settings tab appears.



ControlUp Monitor Configuration

Sites and Monitors - Configuration Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

Proxy Settings

Configure the proxy settings needed by Monitors on your network to communicate with the Internet.
These settings will be configured on all the Monitors under the selected entity level.

☑ Inherit organization settings

○ No proxy

● Use system proxy settings

○ Use the following proxy:

Proxy Address: Port: 8080

□ This proxy server requires authentication

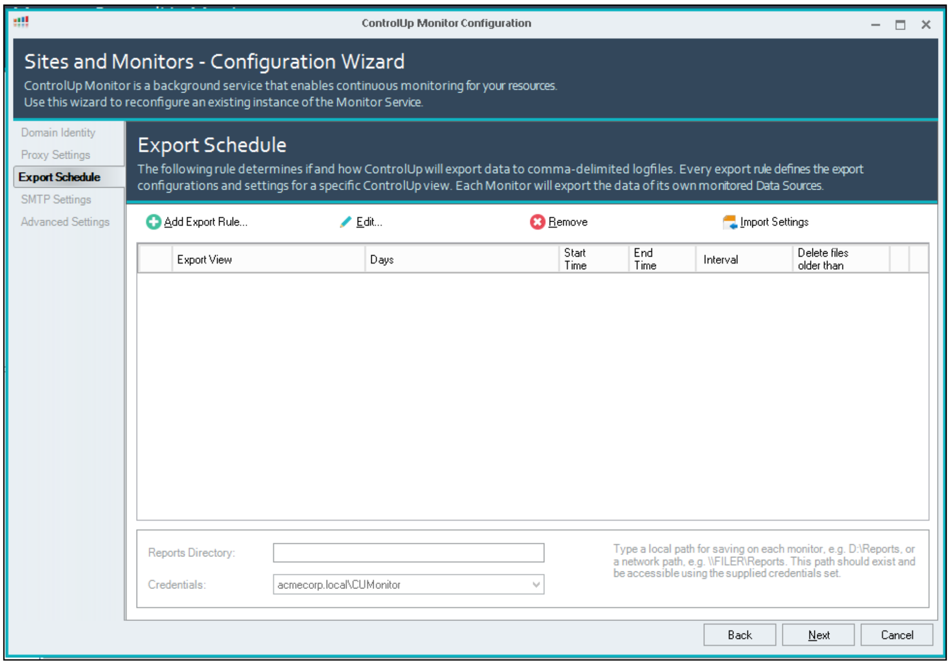
Authentication method: Integrated Windows Authentication

Use the following credentials set:

7. Configure any Proxy settings, if required, for the default site, and click **Next** and the Export Schedule tab appears.

   Note: The proxy settings option can be configured separately for each site.

8. Configure Export Schedule, if needed. Click **Next** and the SMTP setting screen appears.



ControlUp Monitor Configuration

Sites and Monitors - Configuration Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

Export Schedule

The following rule determines if and how ControlUp will export data to comma-delimited logfiles. Every export rule defines the export configurations and settings for a specific ControlUp view. Each Monitor will export the data of its own monitored Data Sources.

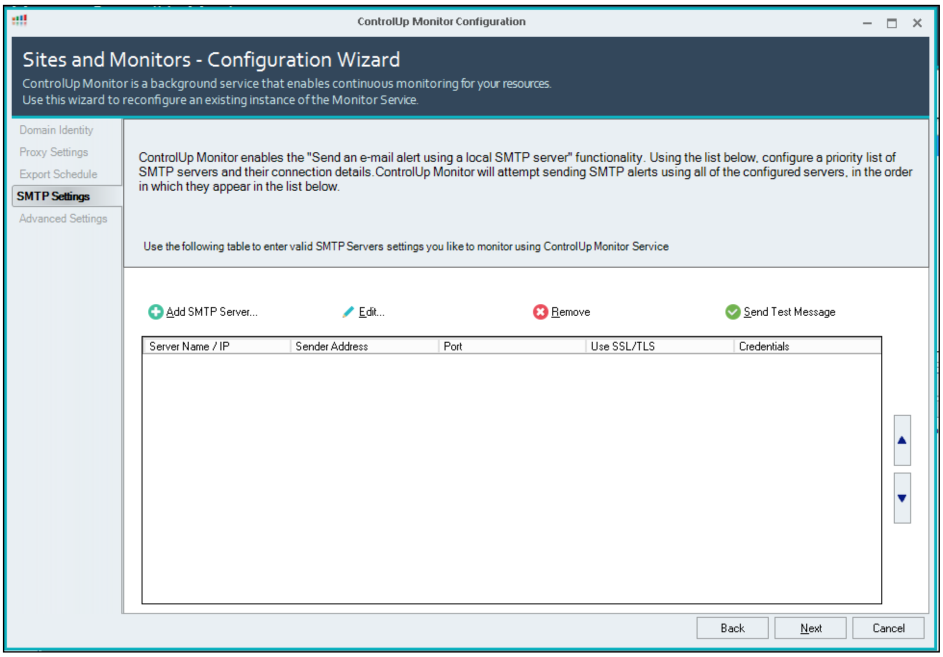
Export View	Days	Start Time	End Time	Interval	Delete files older than

Reports Directory:

Credentials: acmecorp.local\CUMonitor

Type a local path for saving on each monitor, e.g. D:\Reports, or a network path, e.g. \\FILER\Reports. This path should exist and be accessible using the supplied credentials set.

9. Configure SMTP settings for Trigger Alerts if needed. Click **Next** and the Advanced Settings screen appears.



Sites and Monitors - Configuration Wizard

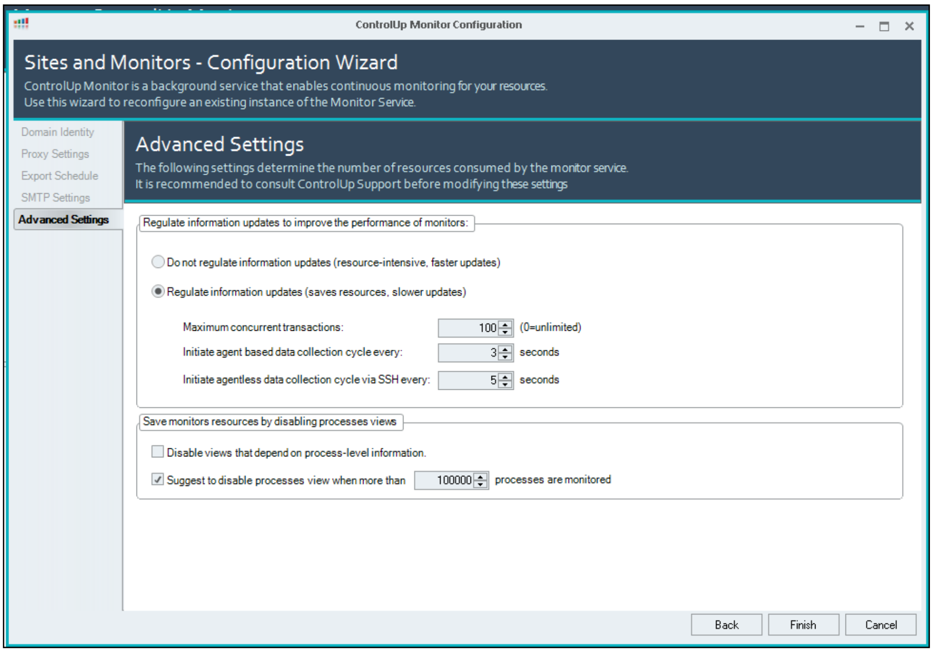
ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

ControlUp Monitor enables the "Send an e-mail alert using a local SMTP server" functionality. Using the list below, configure a priority list of SMTP servers and their connection details. ControlUp Monitor will attempt sending SMTP alerts using all of the configured servers, in the order in which they appear in the list below.

Use the following table to enter valid SMTP Servers settings you like to monitor using ControlUp Monitor Service

10. The Advanced Settings screen displays the default monitor service resource settings.

    We recommend using the default interval configuration. If you want to change it, see here.



Sites and Monitors - Configuration Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to reconfigure an existing instance of the Monitor Service.

Advanced Settings

The following settings determine the number of resources consumed by the monitor service.
It is recommended to consult ControlUp Support before modifying these settings

Regulate information updates to improve the performance of monitors:

○ Do not regulate information updates (resource-intensive, faster updates)

● Regulate information updates (saves resources, slower updates)

Maximum concurrent transactions: 100 (0=unlimited)

Initiate agent based data collection cycle every: 3 seconds

Initiate agentless data collection cycle via SSH every: 5 seconds

Save monitors resources by disabling processes views

□ Disable views that depend on process-level information.

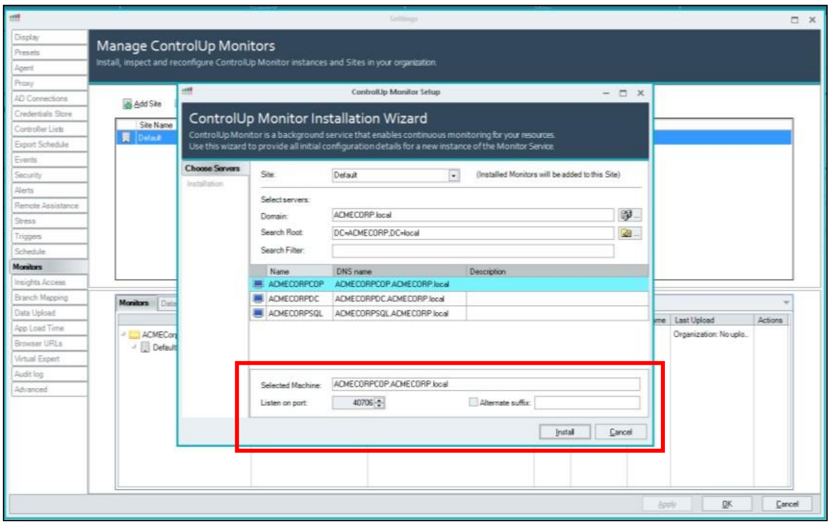
☑ Suggest to disable processes view when more than 100000 processes are monitored

Note: The Export schedule, SMTP settings, and Advanced settings are global and are not set per site.

11. Click **Finish** and the ControlUp Monitor Installation Wizard appears.

12. Select the machine you would like to install the monitor on.

    If needed, modify the port that the monitor will listen to ensure that the corresponding port is open in your firewall. By default, the port the monitor listens to is 40706 (console <> monitor).



Manage ControlUp Monitors

Install, inspect and reconfigure ControlUp Monitor instances and Sites in your organization.

ControlUp Monitor Setup

ControlUp Monitor Installation Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to provide all initial configuration details for a new instance of the Monitor Service.

Site: Default (Installed Monitors will be added to this Site)

Select servers:

Domain: ACMECORP.local

Search Root: DC=ACMECORP,DC=local

Search Filter:

Name	DNS name	Description
ACMECORPCOP	ACMECORPCOP.ACMECORP.local	
ACMECORPDC	ACMECORPDC.ACMECORP.local	
ACMECORPSQL	ACMECORPSQL.ACMECORP.local	

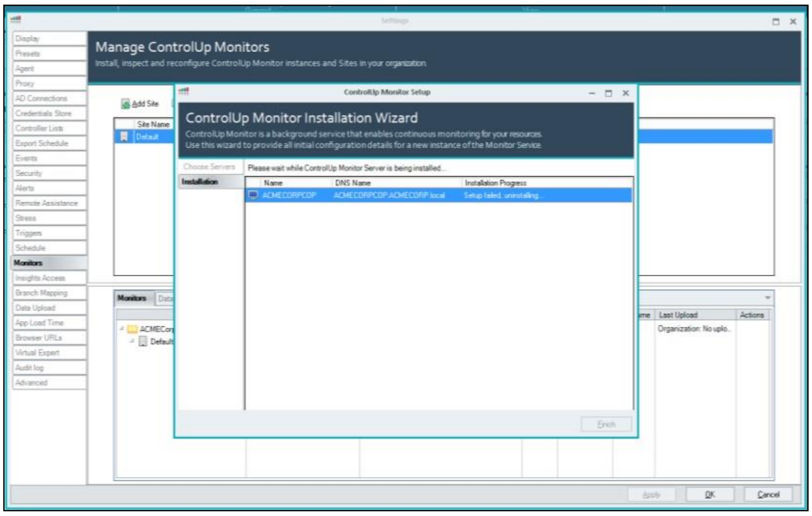
Selected Machine: ACMECORPCOP.ACMECORP.local

Listen on port: 40706

□ Alternate suffix:

13. Click **Install** and the ControlUp Monitor Installation Wizard appears. The installation may take a few seconds.

    The monitor installation wizard tests various components of the target machine before deploying the service to make sure that it will be able to run.



Manage ControlUp Monitors

Install, inspect and reconfigure ControlUp Monitor instances and Sites in your organization.

ControlUp Monitor Setup

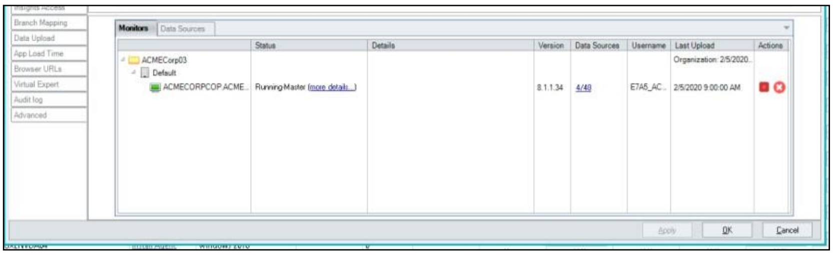
ControlUp Monitor Installation Wizard

ControlUp Monitor is a background service that enables continuous monitoring for your resources.
Use this wizard to provide all initial configuration details for a new instance of the Monitor Service.

Please wait while ControlUp Monitor Server is being installed...

Name	DNS Name	Installation Progress
ACMECORPCOP	ACMECORPCOP.ACMECORP.local	Setup failed, uninstalling...

14. Click **Finish** and then click **OK** and the added monitors appear in the Montors tab with a green icon next to it.



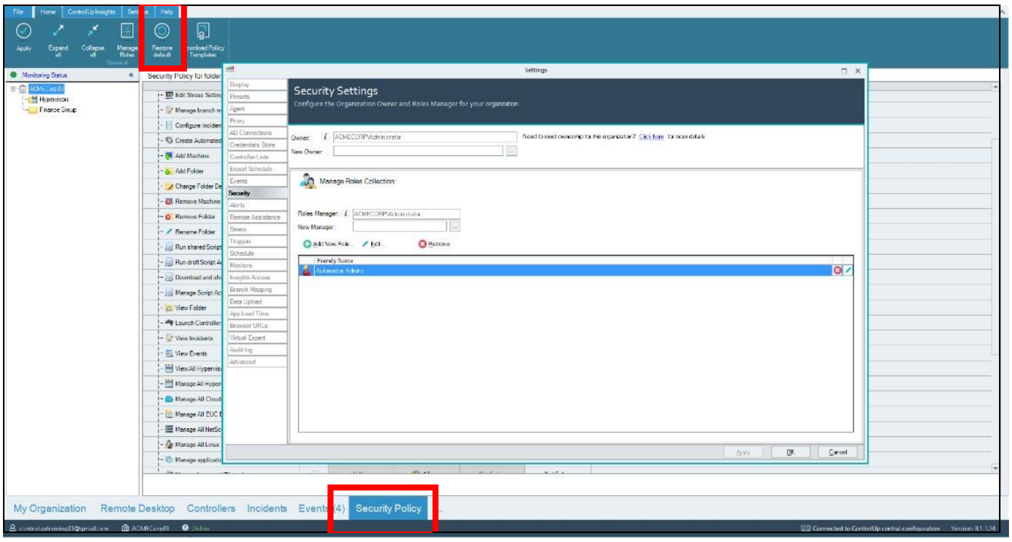
	Status	Details	Version	Data Sources	Username	Last Upload	Actions
ACMECorp03						Organization: 2/5/2020...	
Default							
ACMECORPCOP.ACME...	Running Master (more details...)		8.1.1.34	4/48	E7A5_AC...	2/5/2020 9:00:00 AM	■ ⊗

Configuring Shared Credentials Prerequisites

After installing the monitor, it is recommended to enable share credentials. This enables streamlined management of credentials and a quicker onboarding process for new ControlUp users which does not require them to know the service usernames and passwords. For the shared credentials to work, a new roles collection must be created, and the shared credentials permission must be set in the Security Policy Panel.

To create a new roles collection:

1. From the **Security Policy** pane, click **Manage Roles** and the security settings screen appears.



Security Settings

Configure the Organization Owner and Roles Manager for your organization

Owner: ACMECORP\Administrator

New Owner:

Need to reset ownership for this organization? Click here for more details

Manage Roles Collection

Roles Manager: ACMECORP\Administrator

New Manager:

Friendly Name
Automation Admins

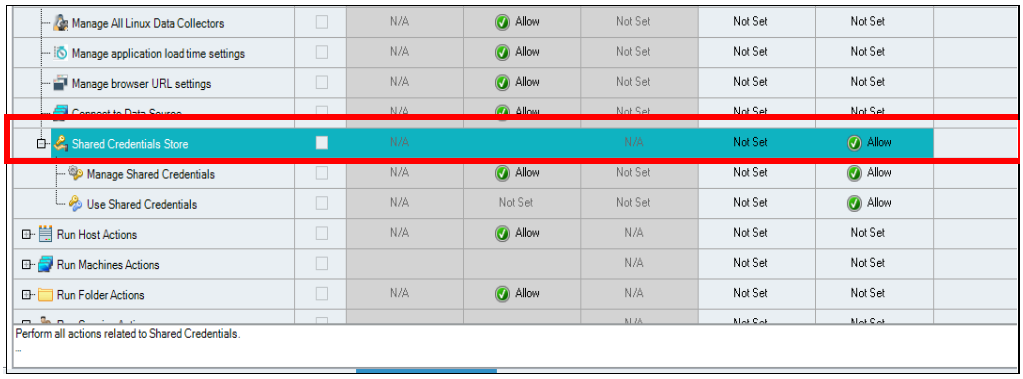
2. Click **Add New Role** and the **Add New** popup appears.
3. Fill in a role name (for example: **CU Admins**) and click **Add Users/Groups**.
4. In the **Search Filter**, type the name of the group in your active directory, where all your ControlUp Admin users reside.

   ***Tip**: Create a dedicated group in your AD for this purpose.*
5. Click **OK** and a new user role named **CU Admins** is now added to ControlUp.

Once the new roles collection has been added, you need to allow the shared credentials permission.

To allow the shared credentials permission:

1. From the security policy folder, expand the **Organization-wide Actions** section and the **Shared Credentials Store** and allow **Manage shared credentials** and **Use shared credentials** to the new role you have created.



Manage All Linux Data Collectors	□	N/A	✓ Allow	Not Set	Not Set	Not Set
Manage application load time settings	□	N/A	✓ Allow	Not Set	Not Set	Not Set
Manage browser URL settings	□	N/A	✓ Allow	Not Set	Not Set	Not Set
Connect to Data Source	□	N/A	✓ Allow	Not Set	Not Set	Not Set
Shared Credentials Store	□	N/A		N/A	Not Set	✓ Allow
Manage Shared Credentials	□	N/A	✓ Allow	Not Set	Not Set	✓ Allow
Use Shared Credentials	□	N/A	Not Set	Not Set	Not Set	✓ Allow
Run Host Actions	□	N/A	✓ Allow	N/A	Not Set	Not Set
Run Machines Actions	□			N/A	Not Set	Not Set
Run Folder Actions	□	N/A	✓ Allow	N/A	Not Set	Not Set

Perform all actions related to Shared Credentials.

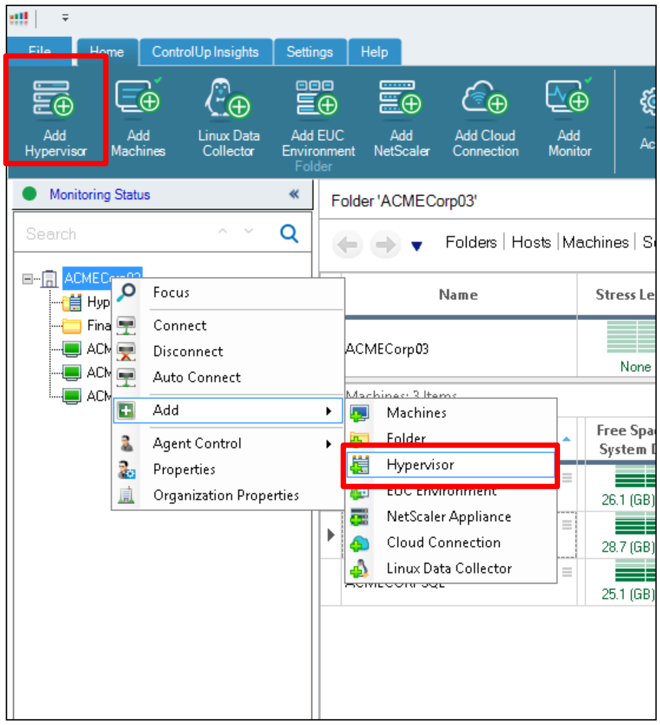
2. Click **Apply** and the credentials are saved.

Adding Hypervisors

This section describes the steps required for adding a hypervisor. Connecting to a hypervisor will populate the Hosts View, in the ControlUp Console.

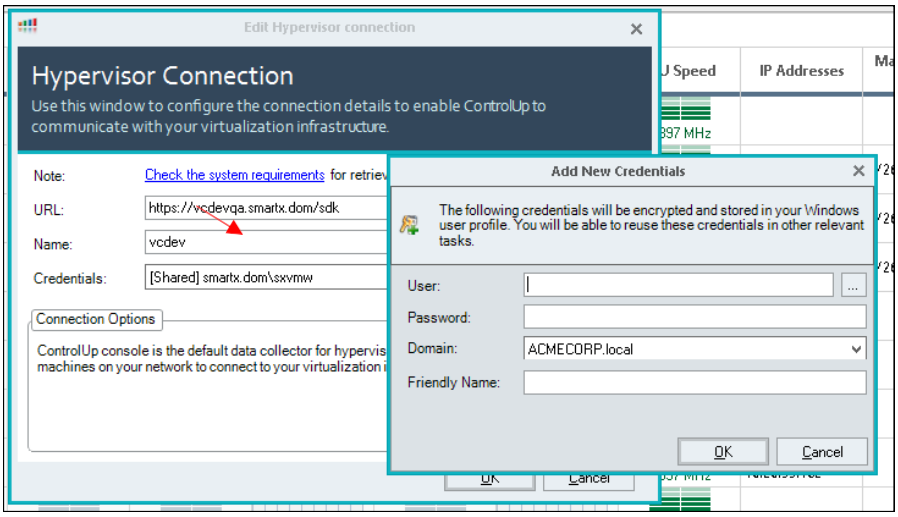
To add a hypervisor:

1. In the Home tab, click **Add Hypervisor** -OR- right-click the top folder of your Organizational tree and select **Add Hypervisor** and the Hypervisor connection screen is displayed.



2. From the drop-down list select the Hypervisor type.
3. In the **URL** field, type in the full name (FQDN), hostname or IP address of the vSphere, Citrix Hypervisor Pool Master, or Nutanix AHV Cluster that you want to connect to.
4. In the **Name** field, type the name of the folder that will contain the Hypervisor assets. There are occasions where that name populates automatically. Select the credentials from the **Credentials** drop-down list that will be used for data collection from your infrastructure. It is possible and recommended to use the credentials from the Shared Credentials Store used via the monitors' cluster.

   It is highly recommended to configure a data collector.



Edit Hypervisor connection

Hypervisor Connection

Use this window to configure the connection details to enable ControlUp to communicate with your virtualization infrastructure.

Note: Check the system requirements for retriev

URL: https://vcdevqa.smartx.dom/sdk

Name: vcdev

Credentials: [Shared] smartx.dom\sxvmw

ControlUp console is the default data collector for hypervis machines on your network to connect to your virtualization i

Add New Credentials

The following credentials will be encrypted and stored in your Windows user profile. You will be able to reuse these credentials in other relevant tasks.

User:

Password:

Domain: ACMECORP.local

Friendly Name:

5. Click **OK** and the hypervisor is added.

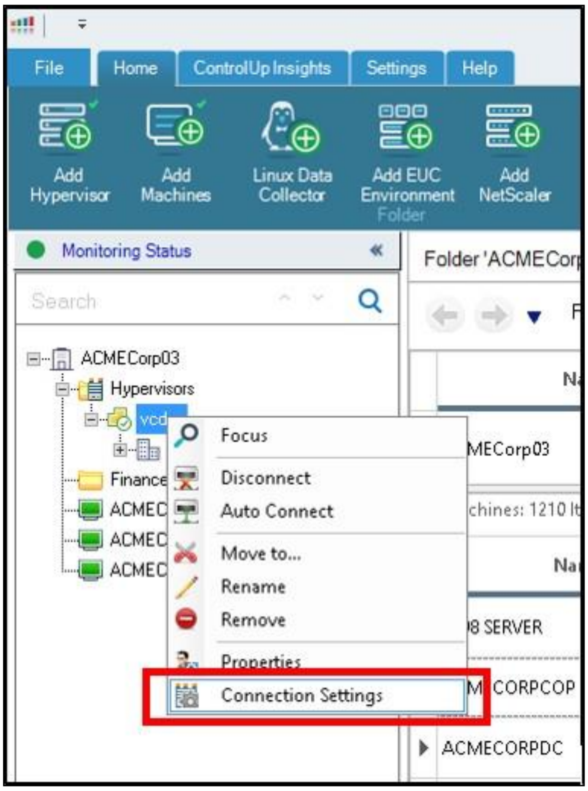
Optimizing Performance with Data Collectors

The following steps are optional but are strongly recommended to ensure optimal performance of ControlUp Connections to the console and the monitor. It is a best practice to designate one or more machines in your ControlUp organization to act as a dedicated data collector for hypervisors. The below example flow must be performed as part of the **Connect Hypervisors** described previously and **Adding EUC environments** described in the upcoming section. It is highly recommended to perform it in both cases.

To configure a dedicated data collector:

1. Add a managed machine to the console which will function as the data collector and will later be defined as the active data collector.

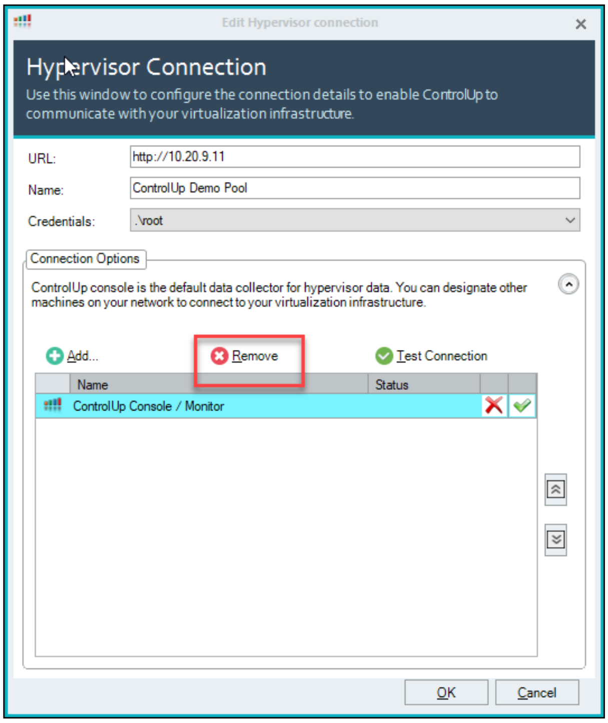
2. Right-click the **Hypervisor** or **EUC Connection** and open the **Connection Settings** dialog box.



Tip: *If the Data Collectors dropdown is hidden, expand it by pressing the down arrow.*

3. By default the ControlUp Console/Monitor acts as a data collector. As a best practice, we recommend using a dedicated data collecor.

   To do so, click **Remove** and then **OK**, and the Controlp Console/Moniotor is removed.



Edit Hypervisor connection

Hypervisor Connection

Use this window to configure the connection details to enable ControlUp to communicate with your virtualization infrastructure.

URL: http://10.20.9.11

Name: ControlUp Demo Pool

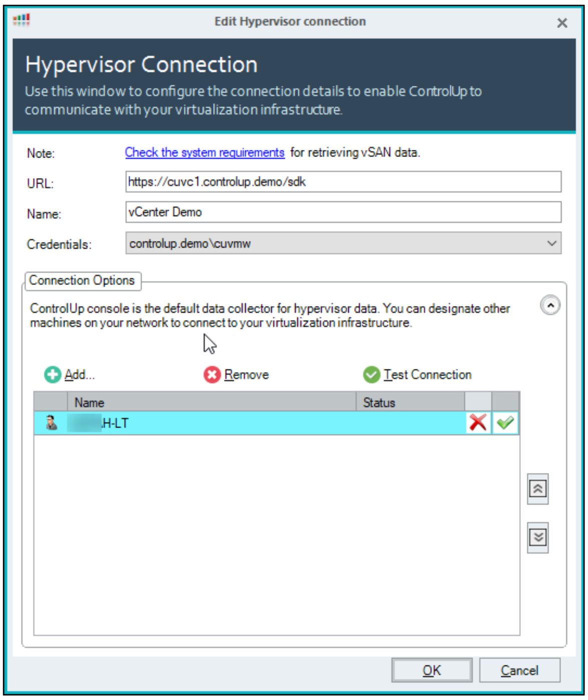
Credentials: .\root

Connection Options

ControlUp console is the default data collector for hypervisor data. You can designate other machines on your network to connect to your virtualization infrastructure.

Name	Status
ControlUp Console / Monitor	

4. Add a new data collector by opening the Data Collector tab, click **Add** and select the machine you added in step 1.



Edit Hypervisor connection

Hypervisor Connection

Use this window to configure the connection details to enable ControlUp to communicate with your virtualization infrastructure.

Note: Check the system requirements for retrieving vSAN data.

URL: https://cuvc1.controlup.demo/sdk

Name: vCenter Demo

Credentials: controlup.demo\cuvmw

Connection Options

ControlUp console is the default data collector for hypervisor data. You can designate other machines on your network to connect to your virtualization infrastructure.

	Name	Status		
	[redacted]H-LT		✗	✓

5. Click **OK** and the data collector is added.

It is also possible to set the monitor as a data collector as well, by installing the agent on the monitor machine, and following the above procedure.

Adding EUC Environment

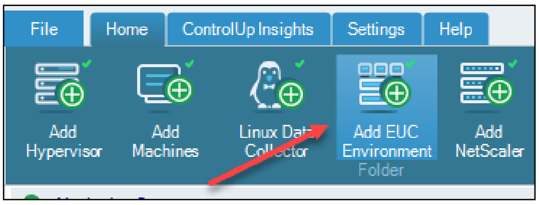
Adding a Citrix Virtual Apps and Desktops Connection

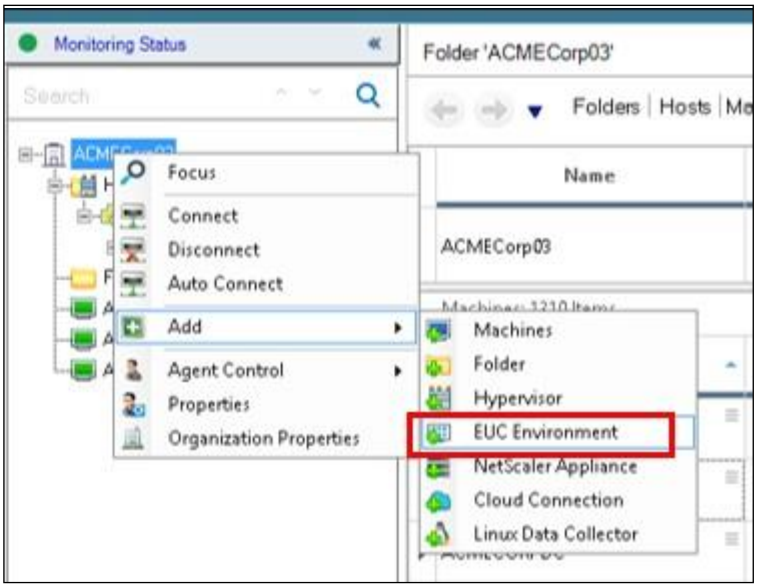
To connect ControlUp to your Citrix Virtual Apps and Desktops deployment, you will need to create an EUC Environment site connection in the ControlUp Console. The connection will define the address(es) of the broker(s) from which data will be gathered, as well as the credentials used for data collection and management actions. The following are mandatory prerequisites for adding a Citrix Virtual Apps and Desktops EUC Environment connection:

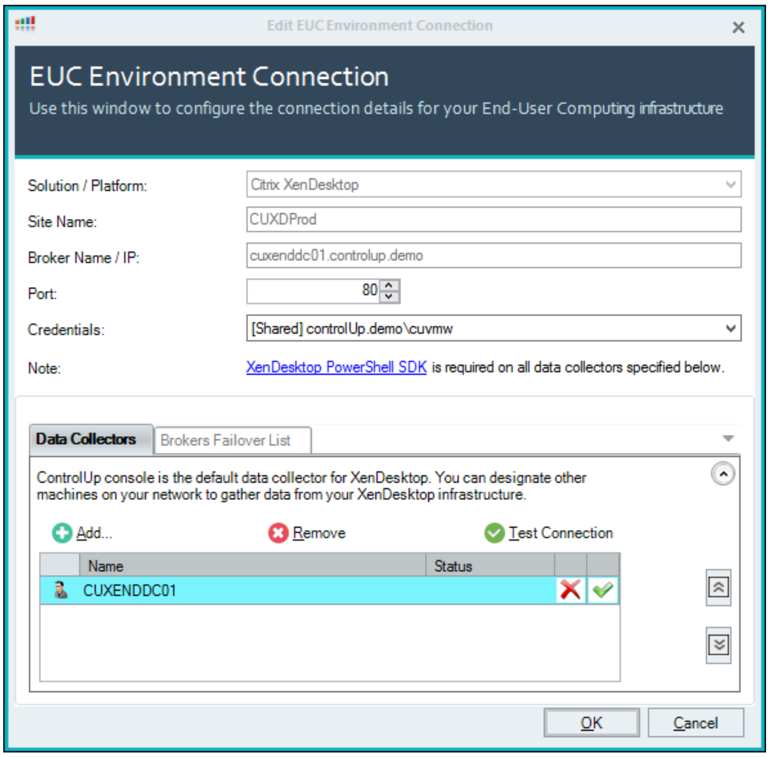
- Port TCP 80/443 opened between console <> broker or data collector <> broker
- Citrix Virtual Apps and Desktops (XenDesktop) 7.5 or later
- Citrix Virtual Apps and Desktops (XenDesktop) PowerShell SDK installed on machines configured as the Citrix Virtual Apps and Desktops data collectors (the console/monitor machines or a dedicated agent machine).

To add an EUC Environment connection:

1. Click on the **Add EUC Environment** button in the main ribbon menu -OR- right-click the root folder of your organization tree and select **Add** and then **EUC Environment** and the Add EUC Environment Connection dialog box appears.







EUC Environment Connection

Use this window to configure the connection details for your End-User Computing infrastructure

Solution / Platform: Citrix XenDesktop

Site Name: CUXDProd

Broker Name / IP: cuxenddc01.controlup.demo

Port: 80

Credentials: [Shared] controlUp.demo\cuvmw

Note: XenDesktop PowerShell SDK is required on all data collectors specified below.

ControlUp console is the default data collector for XenDesktop. You can designate other machines on your network to gather data from your XenDesktop infrastructure.

Name	Status
CUXENDDC01	✗ ✓

2. In the **Solution/Platform** drop-down, select **Citrix Virtual Apps and Desktops** and the site name will be populated automatically.
3. Fill in the Broker name/IP full name (FQDN), hostname or IP address.
4. From the **Credentials** drop-down select or add a set of credentials that will be used for data collection from your Citrix Virtual Apps and Desktops infrastructure.
   Tip: *It is highly recommended to configure a dedicated data collector.*
5. Click **OK** and the EUC Environment connection is added.

Once ControlUp establishes a connection with your Citrix Virtual Apps and Desktops site, it will automatically populate the Site Name field with the site's name and the Brokers Failover List tab with the names of all the broker servers assigned to the Citrix Virtual Apps and Desktops site.

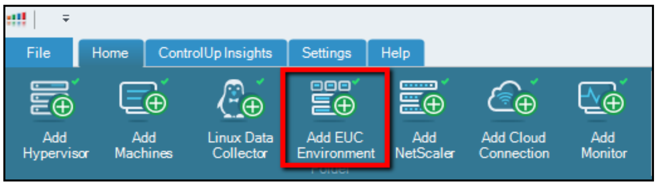
Adding a VMware Horizon Connection

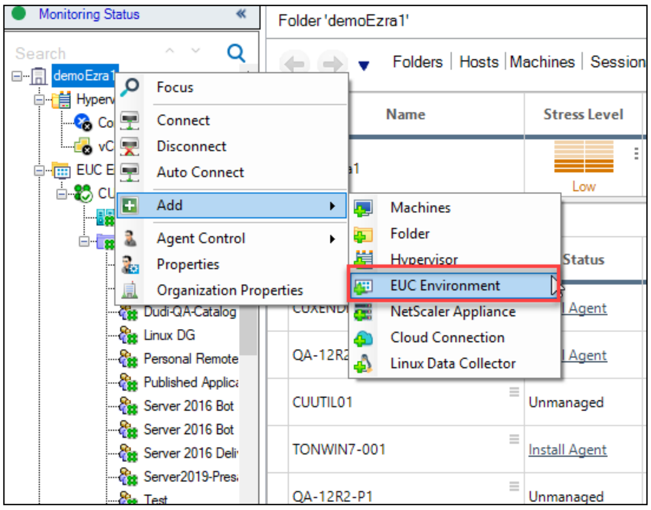
To connect ControlUp to your Horizon deployment, you must create a VMware Horizon site connection in the ControlUp Console. The connection will specify the Horizon pools(s) from which data will be gathered, as well as the credentials used for data collection and management actions. The following are mandatory prerequisites for adding a Horizon "**EUC Environment"** connection:

- Port TCP 443 opened between console <> connection server or data collector <> connection server

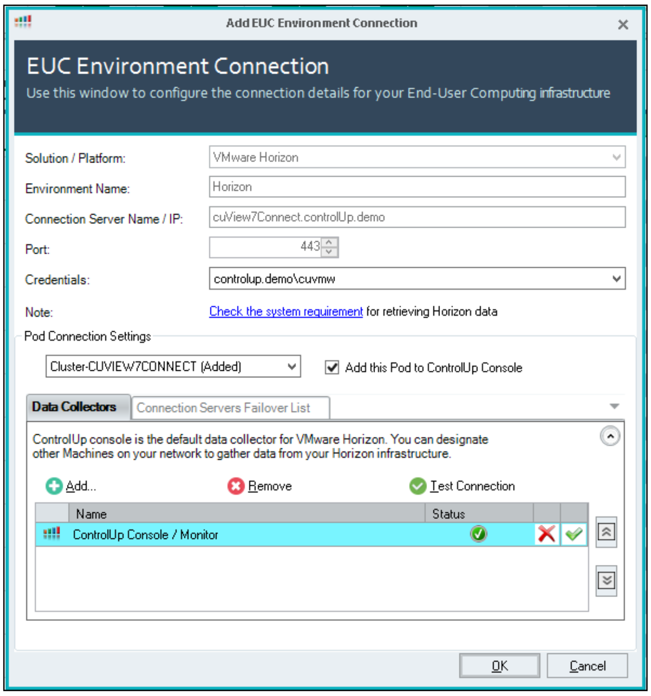
To add a Horizon site connection:

1. Click on the **Add EUC Environment** button in the main ribbon menu and select **Add** and then **EUC Environment** and the Add EUC Environment Connection dialog box appears.





2. From the **Solution/Platform** drop-down box select **VMware Horizon**.


Add EUC Environment Connection

EUC Environment Connection

Use this window to configure the connection details for your End-User Computing infrastructure

Solution / Platform: VMware Horizon

Environment Name: Horizon

Connection Server Name / IP: cuView7Connect.controlUp.demo

Port: 443

Credentials: controlup.demo\cuvmw

Note: Check the system requirement for retrieving Horizon data

Pod Connection Settings

Cluster-CUVIEW7CONNECT (Added) ☑ Add this Pod to ControlUp Console

ControlUp console is the default data collector for VMware Horizon. You can designate other Machines on your network to gather data from your Horizon infrastructure.

Name	Status
ControlUp Console / Monitor	✓

3. In the **Connection Server Name/IP** enter the full name (FQDN), hostname or IP address of a Connection Server in your Horizon site, it will auto discover all the components in the Horizon Environment.

4. From the **Credentials** dropdown box select or add a set of credentials that will be used for data collection from your Horizon infrastructure.
5. Click **OK** and the Horizon site is connected.
6. Once connected you will be prompted to configure the **Pod Connection Settings.**

   If you would like to remove one of the Pod connections, select it from the dropdown and uncheck **Add this Pod to ControlUp Console.**

   Tip: *It is highly recommended to configure a dedicated data collector.*
7. Click **OK** and the VMWare Horizon connection is complete.

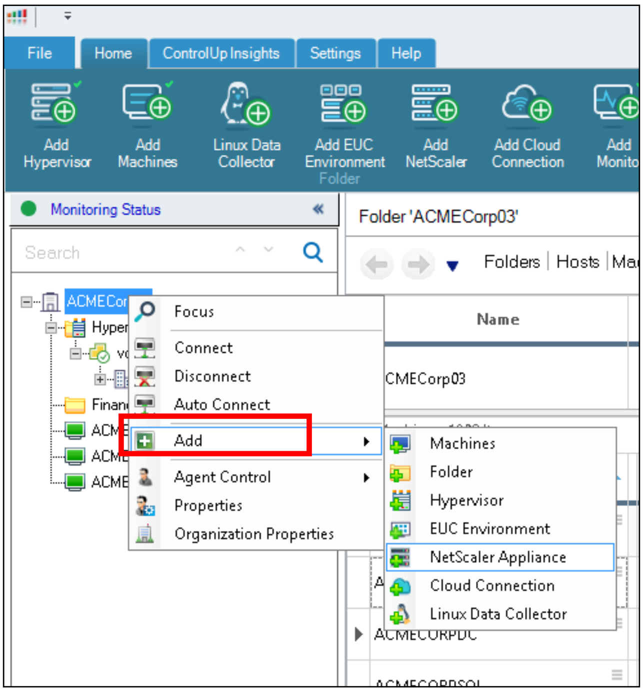
Add Horizon Environment on Azure/VMC

To collect data from Horizon Environments on Azure/VMC in ControlUp, you need to install the ControlUp Agent on the Machines. Currently we do not support retrieving data by API in these environments.

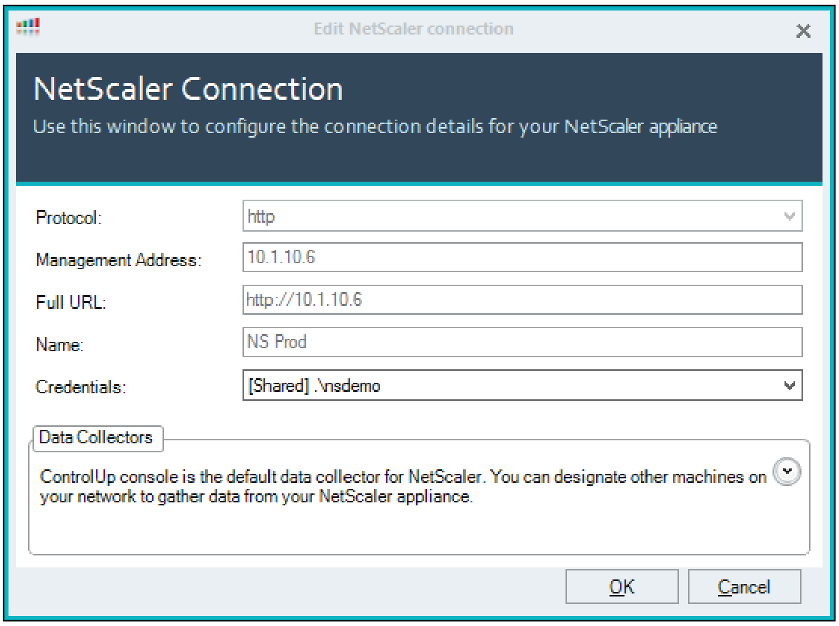
Adding NetScaler Appliance

To add a NetScaler Appliance:

1. Click **Add NetScaler** in the ribbon -OR- right-click the root folder in your organizational tree, select **Add** and then **Netscaler Appliance.**



2. From the **Protocol** drop-down list Choose the – HTTP or HTTPS.
3. Fill in the NetScaler Appliance management name or IP and fill in a name for the NetScaler Connection.



Edit NetScaler connection

NetScaler Connection

Use this window to configure the connection details for your NetScaler appliance

Protocol: http

Management Address: 10.1.10.6

Full URL: http://10.1.10.6

Name: NS Prod

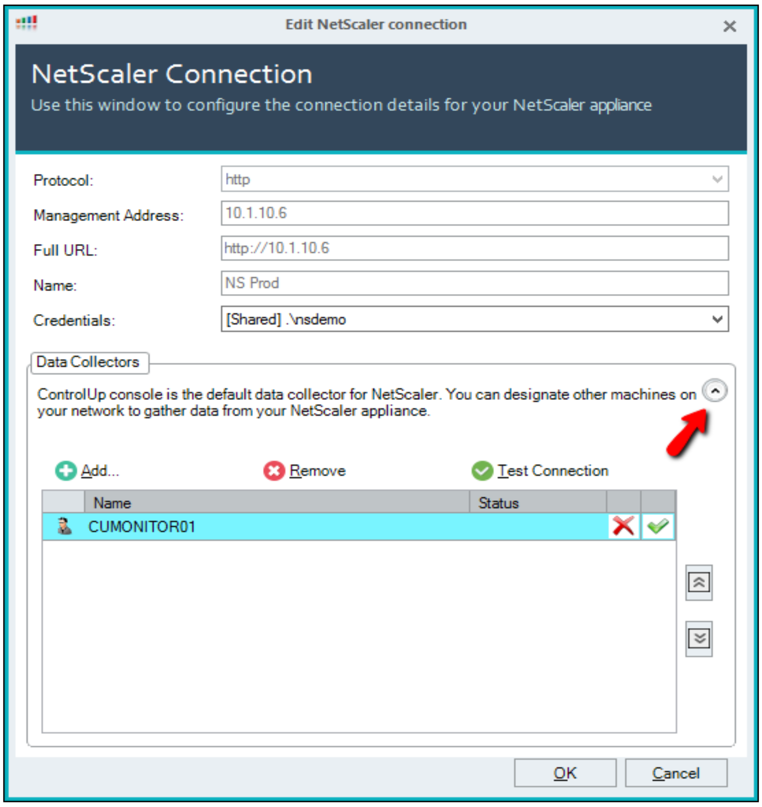
Credentials: [Shared] .\nsdemo

Data Collectors

ControlUp console is the default data collector for NetScaler. You can designate other machines on your network to gather data from your NetScaler appliance.

4. Provide credentials for the NetScaler Management (Read-Only is the minimum requirement).

   Tip: *It is highly recommended to configure a dedicated data collector.*



Edit NetScaler connection

NetScaler Connection

Use this window to configure the connection details for your NetScaler appliance

Protocol: http

Management Address: 10.1.10.6

Full URL: http://10.1.10.6

Name: NS Prod

Credentials: [Shared] .\nsdemo

Data Collectors

ControlUp console is the default data collector for NetScaler. You can designate other machines on your network to gather data from your NetScaler appliance.

Name	Status
CUMONITOR01	

5. Click **OK** and the Netscaler appliance is added.

Log into ControlUp SOLVE

Once ControlUp is installed and a user account has been created and configured, you can now access SOLVE in a hosted web application providing powerful and comprehensive, real-time monitoring and analysis.

To read more about SOLVE, see Welcome to SOLVE.

For details about logging into SOLVE, see Login Flow for SOLVE and the ControlUp Console v8.2 and Up.

To learn how to set up your SOLVE environment, see Configure SOLVE.

Log into ControlUp Insights

Once ControlUp is installed and a user account has been created and configured, you can now access Insights to view the historical reporting and check the health of your VDI environment by identifying the source of existing disruptions and getting ahead of emerging ones.

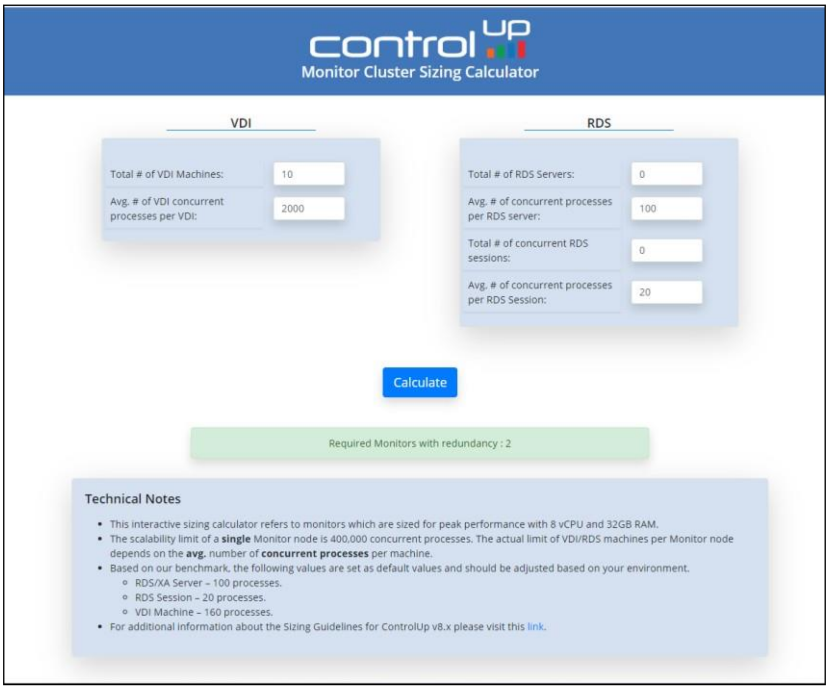
For details on logging into Insights, see Login for Insights – v8.2 and Up.

Appendix

Sizing Guidelines

The following guidelines are intended to help and guide administrators on how to optimize resource allocation for the ControlUp infrastructure.

ControlUp provides an online monitor Cluster Sizing Calculator, which provides the optimal number of monitor instances recommended for your environment. You can access the calculator here.



Monitor Cluster Sizing Calculator

VDI	
Total # of VDI Machines:	10
Avg. # of VDI concurrent processes per VDI:	2000

RDS	
Total # of RDS Servers:	0
Avg. # of concurrent processes per RDS server:	100
Total # of concurrent RDS sessions:	0
Avg. # of concurrent processes per RDS Session:	20

Required Monitors with redundancy : 2

Technical Notes

- This interactive sizing calculator refers to monitors which are sized for peak performance with 8 vCPU and 32GB RAM.
- The scalability limit of a **single** Monitor node is 400,000 concurrent processes. The actual limit of VDI/RDS machines per Monitor node depends on the **avg.** number of **concurrent processes** per machine.
- Based on our benchmark, the following values are set as default values and should be adjusted based on your environment.
  - RDS/XA Server – 100 processes.
  - RDS Session – 20 processes.
  - VDI Machine – 160 processes.
- For additional information about the Sizing Guidelines for ControlUp v8.x please visit this link.

ControlUp Console Guidelines

The charts below specify the sizing requirements for each console instance you will use depending on the number of VDIs or RDSH workloads you intend to monitor.

Note: When managing more than 2,000 concurrent user sessions, disable the flat views in the console. For further instructions, see here.

VDI-based Sizing for the ControlUp Console

Component	ControlUp Console (***)
VDI Machines(*)	0 – 3,000(**)
vCPU(**)	2
RAM	8

(*) The example above is based on an avg. of 160 concurrent processes per VDI machine with a N+1 configuration.

(**) 2.8Ghz clock speed or higher.

(***) Per console instance, based on a fully optimized console.

RDSH-based Sizing for the ControlUp Console

Component	ControlUp Console
RDSH Sessions(*)	0 – 20,000(**)
vCPU(**)	2
RAM	8

(*) The example is based on an avg. of 200 concurrent processes per an RDSH host with a N+1 configuration.

(**) 2.8Ghz clock speed or higher.

(***) Per console instance, based on a fully optimized console.

ControlUp Monitor Guidelines

In the charts below, we have specified the sizing requirements for each monitor instance you will use, depending on the number of VDIs or RDSH workloads you intend to monitor.

VDI Based Workloads for the Monitor

Component	Monitor Sizing (*)		
VDI Workloads	0 - 1,000	1,000 - 2,000	2,000 - 4,000(***)
vCPU(**)	4	8	8
RAM	16	24	32

(*) For environments with more than 2,500 VDI machines, additional monitors should be deployed. See the configuration examples below for 5,000, 20,000 and 50,000 VDI machines.

(**) 2.8Ghz clock speed or higher.

(***) The scalability limit of a single monitor node is 320,000 concurrent processes. The actual limit of VDI machines per monitor node depends on the avg. number of concurrent processes per VDI machine.

RDSH Based Workloads for the Monitor

The sizing numbers below are related to environments where the end-users are running on RDSH based servers. The main factor is the number of concurrent sessions that are managed using ControlUp.

Component	ControlUp Monitors	
RDSH Sessions	0 - 5,000	5000 – 10000 (**)
vCPU(*)	4	8
RAM	16	32

(*) 2.8Ghz clock speed or higher.
(**) Based on approx. 20 processes per RDSH session.

ControlUp Agent

The ControlUp agent is a lightweight component that was designed from the ground up to enable rapid deployment and minimal performance footprint. A machine with an agent installed is referred as a managed machine. The expected CPU usage is 0%-1% with spikes up to 2%. RAM usage should be approximately 50MB to 100MB and IOPS counters for the agent executable should normally show zero activity.

Note: The ControlUp Agent does NOT require a reboot while being installed or uninstalled and no special configuration is needed when the agent is deployed on a VDI master image.

In ControlUp, the console & monitor retrieve data from agents on servers, workstations, user sessions, etc. This action might impact your network bandwidth. This impact is extremely minimal as there is very low usage with the ControlUp Agent.

The average network traffic for a single agent communication to a monitor/console is 1KBps.

This means that a single ControlUp console will consume approximately the following bandwidth:

Number of Agents	Bandwidth
100	*100KBps*
1000	*1MBps*
10,000	*10Mbps*

For information about agent deployment and security recommendation see here.

Data Collectors

A data collector is a component in ControlUp (usually the CU Agent) that collects data from various API services and assists in reducing the load from the hypervisor or any other API connection and optimizes the performance of the console and monitor. For detailed instructions on how to set up a dedicated data collector, see here.

As a best practice, it is recommended to configure the CU Agent data collectors and run them on a dedicated virtual machine.

Note: The numbers in the sizing chart below represent the number of records that the API service is passing. The following table is a configuration example for

When linking a data source, such as VMware/Hyper-V/XenServer/Nutanix, we query hosts, machines, datastores & virtual disks.

In EUC environments like Citrix Virtual Apps and Desktops/VMware Horizon, we query topology (delivery groups/desktop pools), brokers/connection servers, machines, and sessions.

NetScaler will query appliance info and metrics, load balancers, HDX sessions, and gateways.

ControlUp Data Collector			
	0 - 2,000 (**)	2,000 - 5,000 (**)	5,000 + (**)
vCPU	2	4	4
RAM	8	8	8

(**) These numbers represent the number of records that the API service passes per query.

Sizing Examples

VDI Sizing Examples

The following is a sizing example for **5,000** VDI machines.

ControlUp Component		vCPU (per instance)	RAM (per instance)	Notes
Monitor (*)	4	8	32	N+1 configuration
Real Time Console	N/A	2	8	Per console instance
Data Collector	See Data Collectors			

*(*) The example above is based on an avg. of **160** concurrent processes per VDI machine with a N+1 configuration.*

The following is a configuration example for **20,000** VDI machines.

ControlUp Component		vCPU (per instance)	RAM (per instance)	Notes
Monitor (*)	11	8	32	N+1 configuration
Real Time Console	N/A	2	8	Per console instance
Data Collector	See Data Collectors			

*(*) The example above is based on an avg. of **160** concurrent processes per VDI machine with a N+1 configuration.*

<u>The following is a configuration example for **50,000** VDI machines.</u>

ControlUp Component		vCPU (per instance)	RAM (per instance)	Notes
Monitor (*)	26	8	32	N+1 configuration
Real Time Console	N/A	2	8	Per console instance
Data Collector	See Data Collectors			

*(*) The example above is based on an avg. of **160** concurrent processes per VDI machine with a N+1 configuration.*

RDSH Sizing Examples

It is important to remember that the scalability limit of a single monitor node is 320,000 concurrent processes, therefore, the actual limit of RDS hosts per monitor node depends on the avg. number of concurrent processes per host including the host. On average, a single monitor node will support 10,000 concurrent sessions.

The numbers below vary between organizations due to the number of sessions running on each host.

<u>The following table is a configuration example for **5,000 RDS Sessions running on 250 RDSH hosts:**</u>

ControlUp Component		vCPU (per instance)	RAM (per instance)	Notes
Monitor Nodes (*)	2	4	16	N+1 configuration
RT Console	N/A	2	8	Per console instance
Data Collector	See Data Collectors			

*(*)The example is based on an avg. of **200** concurrent processes per an RDSH host with a N+1 configuration.*

<u>The following table is a configuration example for **20,000 RDS Sessions running on 1,000 RDSHs.**</u>

ControlUp Component		vCPU (per instance)	RAM (per instance)	Notes
Monitor Nodes (*)	3	8	32	N+1 configuration
RT Console	N/A	2	8	Per console instance
Data Collector	See Data Collectors			

*(*)The example is based on an avg. of **200** concurrent processes per an RDSH host with a N+1 configuration.*

The following table is a configuration example for **50,000 RDS Sessions Running on 2,500 RDSHs.**

ControlUp Component		vCPU (per instance)	RAM (per instance)	Notes
Monitor Nodes (*)	5	8	32	N+1 configuration
RT Console	N/A	2	8	Per console instance
Data Collector	See Data Collectors			

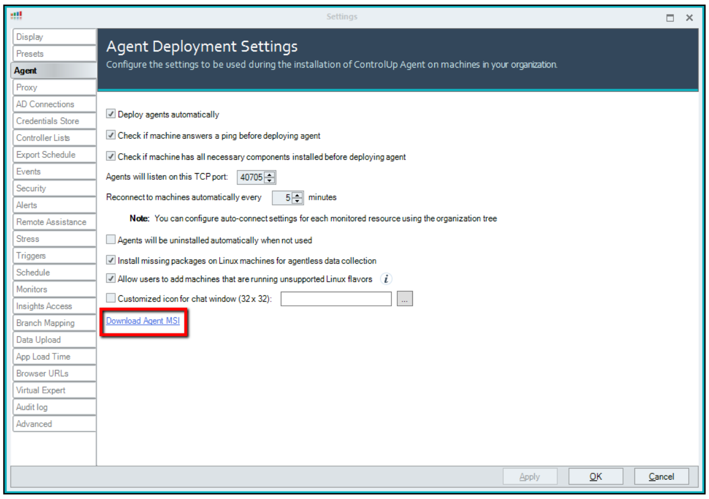
*(*)The example is based on an avg. of **200** concurrent processes per an RDSH host with a N+1 configuration.*

Adding a ControlUp Agent in Horizon Environment

In Horizon environments, it is highly recommended to deploy the ControlUp Agent via a golden image. ControlUp allows you to do that using the ControlUp Agent MSI package**.**

To install the MSI package:

1. Download the package from this link -OR- via the console by selecting **Settings** and then **Agent** and click on the Download Agent MSI URL.



Agent Deployment Settings

Configure the settings to be used during the installation of ControlUp Agent on machines in your organization.

☑ Deploy agents automatically

☑ Check if machine answers a ping before deploying agent

☑ Check if machine has all necessary components installed before deploying agent

Agents will listen on this TCP port: 40705

Reconnect to machines automatically every 5 minutes

Note: You can configure auto-connect settings for each monitored resource using the organization tree

□ Agents will be uninstalled automatically when not used

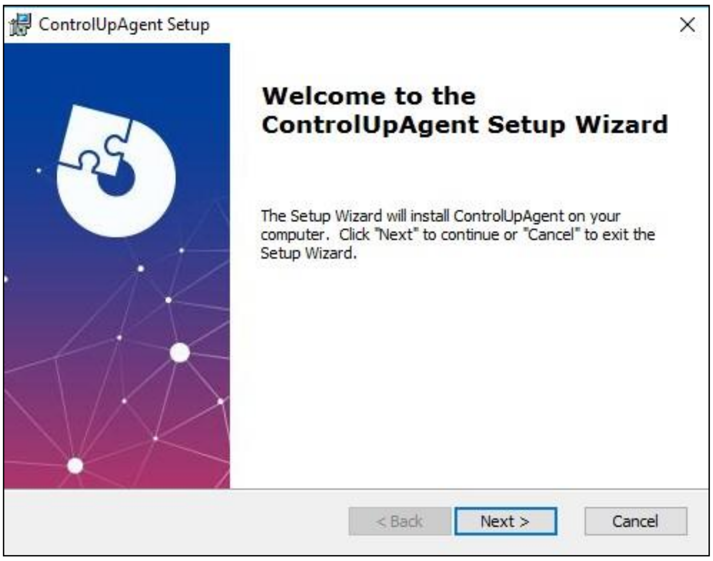
☑ Install missing packages on Linux machines for agentless data collection

☑ Allow users to add machines that are running unsupported Linux flavors

□ Customized icon for chat window (32 x 32):

Download Agent MSI

2. Install the MSI package on the golden image using the setup wizard. (No other configurations required.)



ControlUpAgent Setup

Welcome to the ControlUpAgent Setup Wizard

The Setup Wizard will install ControlUpAgent on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

To add a machine to the organizational tree and start monitoring it, follow the steps in the Adding Managed Machines section or use a PowerShell script to add the machines automatically as described in the next section.

Auto Adding Machines Installed with the MSI Package

To support the dynamic nature of Horizon environments, where desktop pools are constantly updated, ControlUp has created sync scripts that make the machine adding process easy and automated.

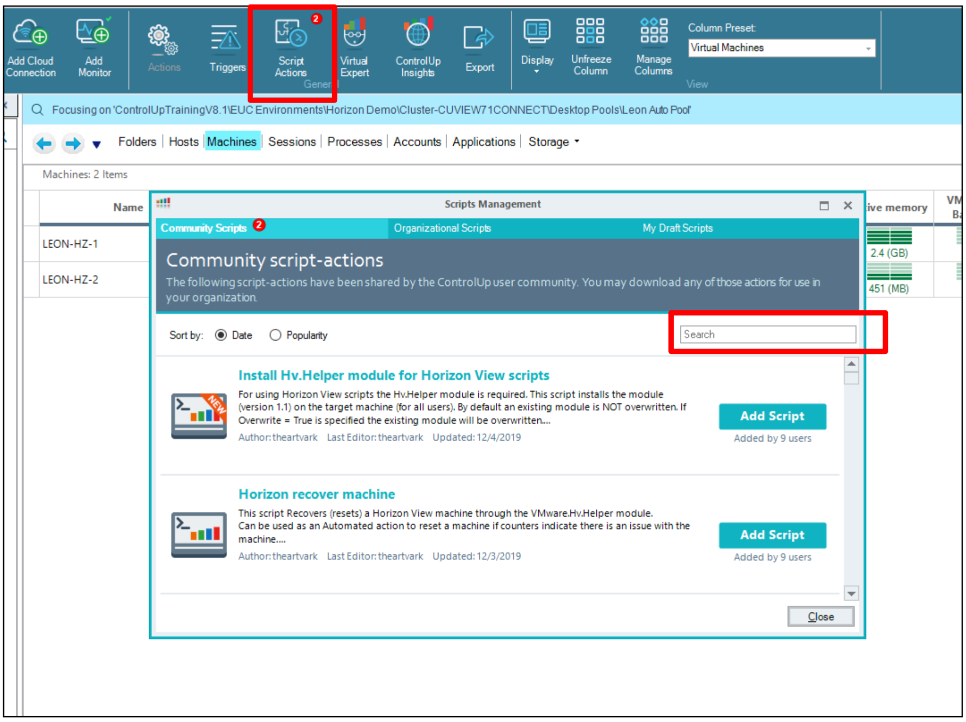
To accomplish this, the machine running the monitor service will need to go through a short preparation process in order to run several PowerShell scripts.

Installed software prerequisites:

- PowerShell 5.0
- PowerShellCLi 11.0 or later (To install the PowerShellCLi, type **Install-Module VMware.PowerCLI** in the PowerShell command line.)
- The controlup.cli PowerShell module (To install the controlup.cli, type **install -module controlup.cli** in the PowerShell command line.)

To prepare the monitor for running the Horizon Sync Script:

1. Open ControlUp Console and click **Script Actions** and the Scripts Management screen appears.



Focusing on 'ControlUpTrainingV8.1\EUC Environments\Horizon Demo\Cluster-CUVIEW71CONNECT\Desktop Pools\Leon Auto Pool'

Machines: 2 Items

Community script-actions

The following script-actions have been shared by the ControlUp user community. You may download any of those actions for use in your organization.

Sort by: ● Date ○ Popularity

Install Hv.Helper module for Horizon View scripts

For using Horizon View scripts the Hv.Helper module is required. This script installs the module (version 1.1) on the target machine (for all users). By default an existing module is NOT overwritten. If Overwrite = True is specified the existing module will be overwritten....

Author: theartvark   Last Editor: theartvark   Updated: 12/4/2019

Added by 9 users

Horizon recover machine

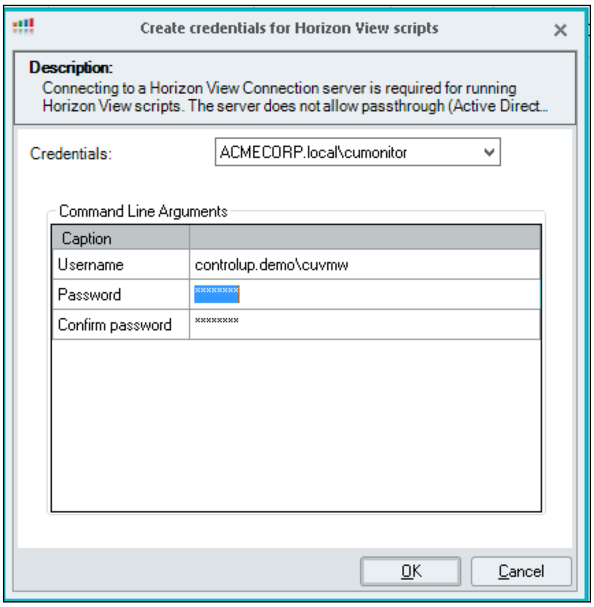
This script Recovers (resets) a Horizon View machine through the VMware.Hv.Helper module. Can be used as an Automated action to reset a machine if counters indicate there is an issue with the machine....

Author: theartvark   Last Editor: theartvark   Updated: 12/3/2019

Added by 9 users

2. From the Scripts Management screen, search for the “Create credentials for Horizon View scripts” and then click **Add Script** and the Add a Shared Script Action popup appears.
3. Click the **Accept the terms** checkbox and click **OK** and the script are added, and you are returned to the Scripts Management screen.
4. From the Scripts Management screen, search for the “Install Hv.Helper module for Horizon View scripts” and then click **Add Script** and the Add a Shared Script Action popup appears.
5. Click the **Accept the terms** checkbox and click **OK** and the script are added, and you are returned to the Scripts Management screen.
6. Click **Close** and the ControlUp Console grid appears.
7. From the ControlUp Console grid, locate the monitor server you would like to prepare and Right-click over it and the Management Actions menu appears.

8. Hover over **Script Actions** and select **Create credentials for Horizon View scripts** and the Create credentials for Horizon View popup appears.



Create credentials for Horizon View scripts

Description:
Connecting to a Horizon View Connection server is required for running Horizon View scripts. The server does not allow passthrough (Active Direct...

Credentials: ACMECORP.local\cumonitor

Command Line Arguments

Caption	
Username	controlup.demo\cuvmw
Password	********
Confirm password	********

9. From the Credentials dropdown select the user to be used to run the monitor account. That is the account you used while setting up the monitor primary domain identity.
10. In the Command Line Arguments text box enter the credentials you used to connect to the Horizon Connection Server while adding the EUC environment to the console.
11. Click **OK** and the Action Results Screen appears.
12. In the Errors tab in the Action Results Screen appears, check that the action is complete with no errors. If the action is successful a credentials XML file will be created under **C:\ProgramData\ControlUp\ScriptSupport**
13. Close the screen Action Results Screen and you are returned to the ControlUp Console grid.
14. Run the second script by hovering over Script Actions and Select **Install Hv.Helper module for Horizon View scripts** and the Action Results screen appears. Make sure the action is complete with no errors and the scripts are applied.

Secure Communications Between ControlUp Console/Monitor and ControlUp Agent

To secure the communication between the installed agent and the ControlUp environment, we recommend you do the following.

1. On any computer running the ControlUp agent, enable a Firewall inbound rule that allows access to port **40705** only to authorized computers.

2. Add these computers which ideally should use static IP addresses:
    - Computers running the ControlUp Monitor service
    - Computers running the ControlUp Console

If you don't own a firewall for your network, we recommend using the built-in Windows firewall alongside a Group Policy to apply the firewall rule to all machines running the ControlUp Agent.

Note: This recommendation reduces the risk of a potential attacker manipulating a ControlUp Agent using malicious code in case that potential attacker has penetrated the organization network.

Creating a Scheduled Task to Run the Script

Once the monitor machine is prepared, a Windows Task Scheduler task must be created in order to regularly run a sync script.

The following procedures must be performed prior to creating the Task Scheduler:

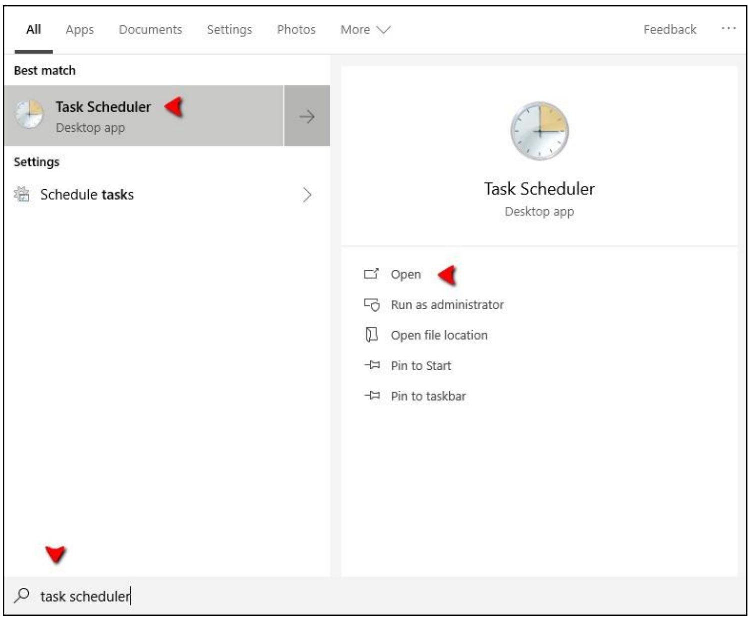
1. Download the PS script linked here.
2. Create a new folder for example, Horizon_Sync_Script, and place the file in this folder.
3. If you would like to exclude pools from being added to the console, create an “exceptions.txt” file with the names of the pools you would like to exclude, and place it in the folder.
4. Create a Task Scheduler that will run this script daily.

Creating a Task Scheduler for Automatically Adding Horizon Machines via a Script

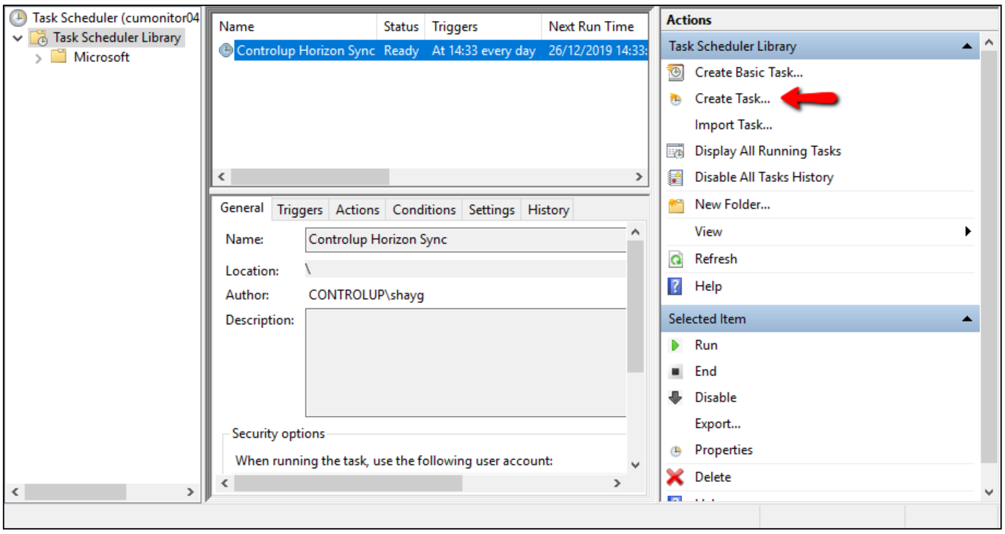
The Task Scheduler for automatically adding Horizon machines via a script, must be created on the ControlUp Monitor server machine.

To Create the Task Scheduler:

1. Open the Task Scheduler.

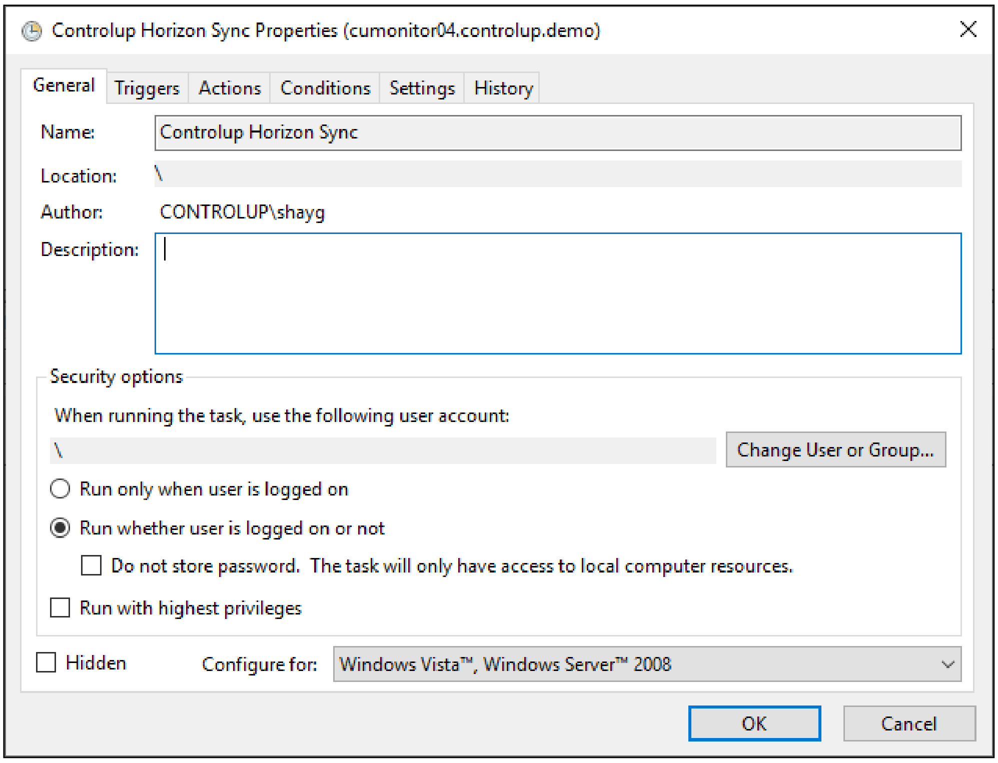


2. In the Task Scheduler window, go to the **Actions** panel and click **Create Task** and the Create Task window is displayed.



3. In the **General** tab, name the newly created task “ControlUp Horizon Sync”.
4. In the Security options, Click **Change Users or Group** and select the service account used for running the monitor.

5. Select **Run whether a user is logged on or not**, and add a description if desired.



Controlup Horizon Sync Properties (cumonitor04.controlup.demo)

Name: Controlup Horizon Sync

Location: \

Author: CONTROLUP\shayg

Description:

Security options

When running the task, use the following user account:

\

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

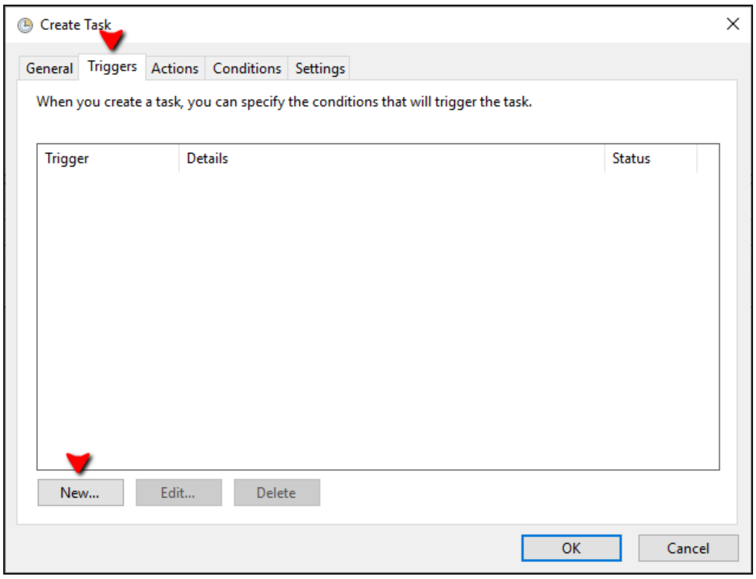
□ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

Set the triggers:

6. To add a new trigger, select the **Triggers** tab and click **New**.



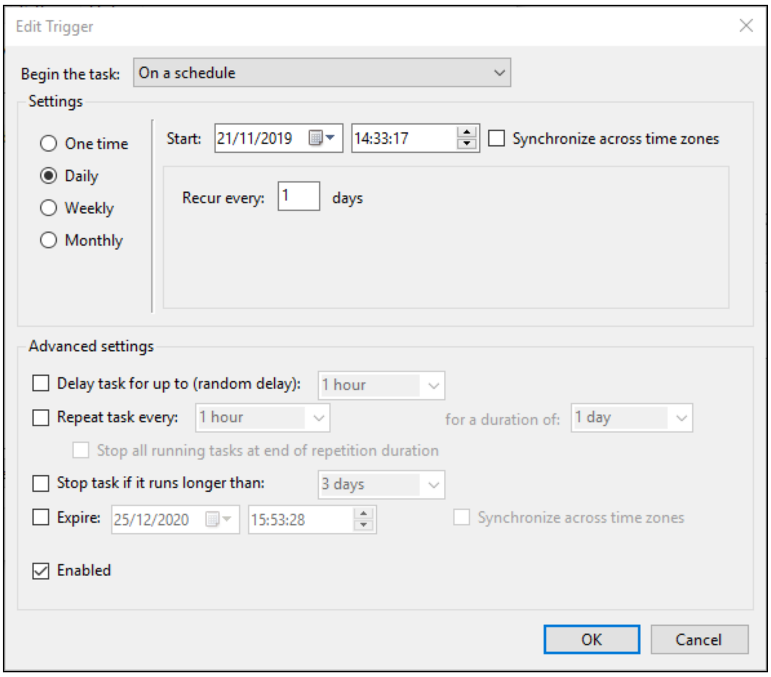
Create Task

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status

7. Click **Begin** in the task drop-down box and select **On a schedule** and select **Daily** and set a daily time to start the task in Task Scheduler in the '**Recur every'** text box to 1 days. Click **OK** and the trigger is set.

Note: The time you set will also be the time the task runs daily.



Edit Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 21/11/2019 14:33:17 □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

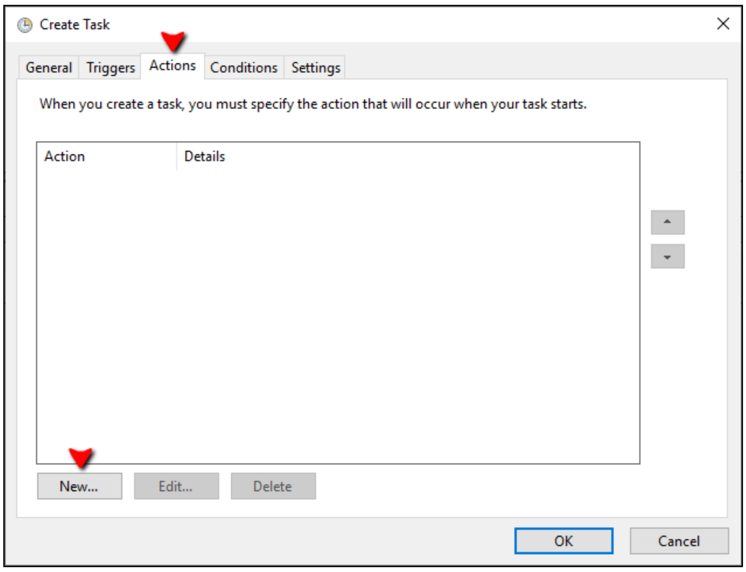
□ Stop task if it runs longer than: 3 days

□ Expire: 25/12/2020 15:53:28 □ Synchronize across time zones

☑ Enabled

Set a task action:

8. Select the **Actions** tab, and click **New** and the Set Actions popup appears.



Create Task

When you create a task, you must specify the action that will occur when your task starts.

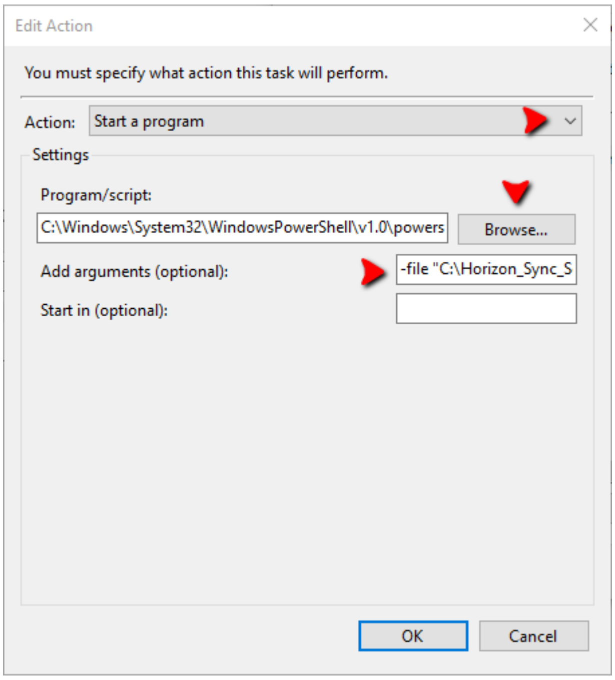
Action	Details

9. In the Set Actions popup, select **Start a program** from the dropdown menu.

10. Click **Browse...** and choose **powershell.exe** (located in: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe).

Add the following arguments to the template below:

-file "[FILE NAME AND PATH]" -hvconnectionserverfqdn "[CONNECTION SERVER FQD]" -targetfolderpath "[ORG TREE FOLDER PATH]" -pooldivider "[ORG TREE DESKTOP POOLS FOLDER NAME]" -rdsdivider "[RDS FARMES FOLDER NAME]" -exceptionfile "[EXEPTION FILE NAME AND PATH]"



Edit Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: C:\Windows\System32\WindowsPowerShell\v1.0\powers

Add arguments (optional): -file "C:\Horizon_Sync_S

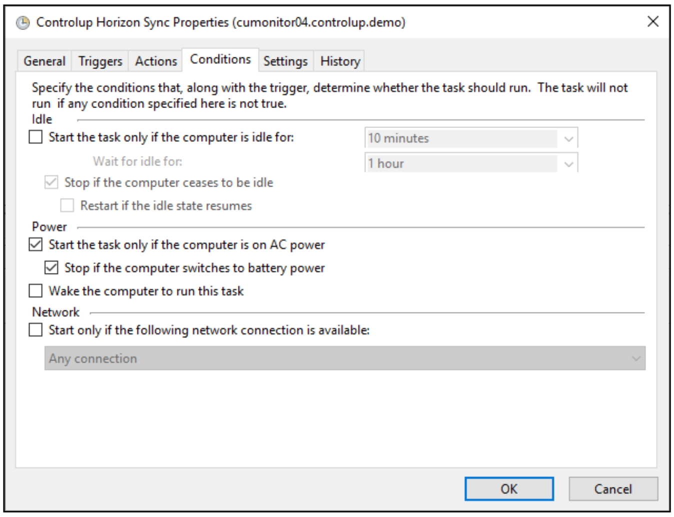
Start in (optional):

You will need to modify the arguments depending on your desired outcome.

11. Click **OK** and the actions are set.

Conditions setting:

12. Leave the task conditions with the default values and click **OK**.



Controlup Horizon Sync Properties (cumonitor04.controlup.demo)

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

☑ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

□ Wake the computer to run this task

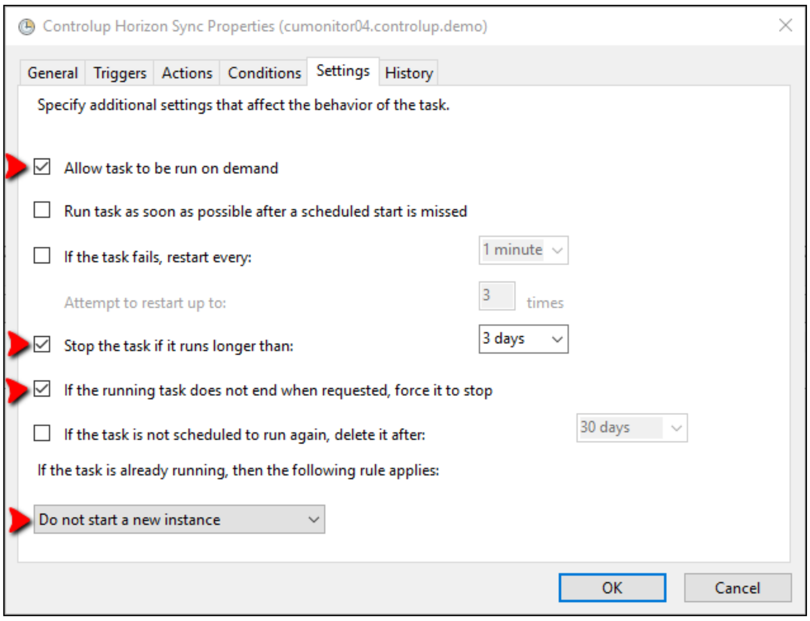
Network

□ Start only if the following network connection is available:

Any connection

Settings Tab:

13. In the Settings tab, make sure that the following are checked:


Controlup Horizon Sync Properties (cumonitor04.controlup.demo)
General
Triggers
Actions
Conditions
Settings
History
OK
Cancel

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

14. Click **OK** and the settings are set.

Argument Description:

The following is a description of the argument variables used in the script, that will allow you to control the outcome according to your needs.

The Argument:

-file "C:\Horizon_Sync_Script\Sync_ControlUP_With_ Horizon_View_v2.ps1" -hvconnectionserverfqdn "horizon.controlup.demo" -targetfolderpath "controlup demo\il datacenter\virtual desktops\horizon demo" -pooldivider "Desktop Pools" -rdsdivider "RDS Farms" -exceptionfile "C:\Horizon_Sync_Script\exceptions.txt"

The Description:

- **file** - (Mandatory) - "C:\Horizon_Sync_Script\Sync_ControlUP_With_ Horizon_View_v2.ps1"
- The location of the Sync PS Script can be changed to any desired location.
- **hvconnectionserverfqdn** - (Mandatory) - "horizon.controlup.demo" - The FQDN of a Connection Server.
- **targetfolderpath** - (Mandatory) - "controlup demo\il datacenter\virtual desktops\horizon demo" - The path of the folder where all objects will be placed in the ControlUp organizational tree.
- **pooldivider** - (Mandatory) - "Desktop Pools" - The Name of the folder where the Desktop Pools will be placed in the ControlUp organizational tree.

- **rdsdivider** - (Mandatory) - "RDS Farms" – The name of the folder where RDS Farms will be placed in the ControlUp organizational tree.
- **exceptionfile** - (Not mandatory) - "C:\Horizon_Sync_Script\exceptions.txt" – The location of a text file with the list of DNS names for machines you DO NOT want to be added to the ControlUp organizational tree.

Glossary

Activity files – A set of files generated by the ControlUp Console and Monitor, which contain historical data about your system's activity. These files are then uploaded to the cloud by the monitor and indexed to be presented in the Insights module.

Automated actions – A feature in ControlUp that utilizes the creation of an Incident Trigger **(**see below) that invokes a PowerShell, VBA or BAT script based on a predefined condition. The idea is that along with the email alert that is sent when an incident is triggered, a script will also be invoked and resolve the issue immediately. For information on how to add a script to ControlUp, please refer to Auto Adding Machines Installed with the MSI Package .

ControlUp Console – The main executable of ControlUp, available for download as a single file named ControlupConsole.exe. There are no install/uninstall routine for this component, just a portable executable file.

ControlUp User – Typically a systems administrator, technical specialist, or support technician working with ControlUp Console. Every ControlUp user is required to create an online login account that is used for user identification and licensing.

Column Preset – A predefined set of metric columns that is aimed at providing information about specific problems or platforms.

ControlUp Agent – A lightweight executable named cuAgent.exe that runs as a system service on every Managed Machine. This component provides performance information and handles the execution of management actions.

ControlUp Organization – A logical grouping of managed machines handled by the same team. A ControlUp User selects an organization during login and is authorized to manage only the machines that belong to the selected organization. ControlUp organizations allow an unlimited number of ControlUp Consoles to connect to every managed machine, as long as these consoles have different ControlUp User accounts logged on. All managed machines are configured only permit connections from ControlUp Users that are members of the same organization.

ControlUp Monitor – A background service that operates similar to the ControlUp Console but without the graphical user interface. ControlUp Monitor connects to all the machines in your organization and performs continuous monitoring and reporting of incidents as well as automatically exporting data tables for historical reporting. If you require 24/7 monitoring and alerting about incidents in your environment, it is recommended that you install at least one instance of ControlUp Monitor, or, alternatively, a monitor cluster for environments with a large amount of assets. (For full instructions on how to install a ControlUp monitor, see here. For sizing recommendations for a ControlUp Monitor, see here.

ControlUp Insights – A reporting and analytics platform that displays historical reports using data gathered by ControlUp. In order to start using ControlUp Insights, one instance or more of ControlUp Monitor must be installed in an organization

Data Collectors – A data collector is a component in ControlUp (usually the CU Agent) that assists in reducing the hypervisor or any API connection and optimizes the performance of the console and monitor. Click here for detailed instructions on how to set up a data collector.

Incident – In ControlUp, an incident is an occurrence on one of your managed machines that fall under the scope of one of the configured incident triggers. For example, you might configure a "Process Ended" incident trigger with a filter of "Process name=svchost.exe". In such a case, every subsequent crash, error, and process exit with this name will generate an incident. Incidents are recorded in the ControlUp Cloud Services database and are available for display in the Incidents Pane of ControlUp.

Incident Trigger – A definition of an occurrence that should be recorded as an incident. Triggers of two types are supported in ControlUp: community triggers, which are created by ControlUp based on vendor recommendations and industry best practices, and user-defined triggers, which can be configured according to your needs. Each trigger includes a set of conditions: trigger type (Stress Level, Process Started, etc.), filter (specific conditions like machine name or operating system), scope (folders and schedule – when and where the trigger applies). In addition, every trigger may include a set of follow-up actions, for example, an email alert. (For full instructions on Trigger Settings go to page 26.)

Script Action (or SA) – A PowerShell, VBScript or batch script that was imported to ControlUp as a management action. Script-based actions (SBAs) can be assigned to any of ControlUp's managed resources (folders, machines, sessions, etc.). SBAs can be downloaded from the community repository or created manually and shared within your ControlUp system.

Hypervisor connection – The connection parameters needed for a console or data collection agent to connect with a supported hypervisor management platform (vCenter or XenServer pool master). Once the connection to the hypervisor management platform is established, host and VM information is automatically retrieved and populates the ControlUp database. (If the connection is to vCenter, datacenter and cluster information is also gathered, for better organization of virtualization resources.)

Hypervisor –Connection points to the virtualization world, namely vCenter, Xen pool master, Hyper V, and Nutanix AHV environments. Strictly speaking, the vCenter server is not a hypervisor, but for the purposes of consistency in ControlUp, it is referred to as one.

Hypervisor folder – Similar to a regular folder, but intended it organizes hypervisor connections.

Host – A machine running VMware ESX/ESXi, Citrix XenServer, Hyper V, and Nutanix AHV that ControlUp accesses via the Hypervisor connection. The virtualization hosts machines that run multiple virtual machines on them.

Managed Machine – A Windows machine that a ControlUp user wishes to manage and/or monitor using the ControlUp system. It needs to belong to an Active Directory domain and have Net Framework 3.5 or 4.5 installed. When contacted for the first time by a ControlUp Console, every Managed machine is assigned to a ControlUp organization. For further details, see Adding Managed Machines.

ControlUp Monitor - The ControlUp Monitor module, assists with the 24/7 monitoring of your assets and alerts about any abnormal behavior according to a customizable set of incident triggers. It is like the ControlUp Console, only without an interactive user interface. Once installed and launched, the monitor connects to the managed assets of your ControlUp organization and starts receiving system information and performance updates, just like an additional ControlUp Console user.

Monitor Cluster – Several monitors working together in the same site, while providing redundancy and failover capabilities

Stress Level – A metric in ControlUp which presents the health condition of a recourse by calculating the load of several metrics that have crossed their defined threshold. Once a predefined load number is reached, the stress level metric will indicate if the condition of the resource is Low, Medium, High, or Critical.

VM – Virtual machines that run as guests on the ESXi, Xen server, Hyper V, or Nutanix AHV hosts. If the guest VM is running a supported version of Windows, then the ControlUp Agent can be installed on it and become a machine fully managed by ControlUp. There are some performance statistics that can be gathered about all VMs, managed or not, because ControlUp queries the hypervisor about all of them. However, full data retrieval is only possible if there is a ControlUp agent installed on the guest OS.

Virtual Expert – A machine learning algorithm in ControlUp that assists in providing information when thresholds are crossed.