How to Install Cyber Crucible

How to Install Cyber Crucible

Created by Dennis Underwood, last modified by Mark Weideman on Sep 27, 2023

Cyber Crucible installation is painless. Login to the web application at
https://dashboard.cybercrucible.com

Go to the Agents page, and click on the Download Agent button.

85131265.png?width=680
After you click the button, the following modal appears:

85229569.png?width=340
Select the group that you want the agent(s) you are installing to initially appear in.

If the group does not appear in the list, you either need to create the group, or ask the group administrator to add you to the existing group.

After installation, you can always change the group one agent is in, or multiple agents at a time. It is typically easier to configure group membership before mass deployment, than to organize the agents after they install.

Permissions Required

Administrative access to a machine is required to install and load the Cyber Crucible service and driver.

The script installation specifically downloads and the configure installer to the default C:\ location. The script must be executed as a user or role that has permission to the download and execution location.

Thus, either a user with permission to use C:\ during installation is needed, or the script (detailed below) needs adjusted to download and execute a different location.

GUI Installation

This installation method allows the user to manually configure and install an installation.

This installation method requires a user with permissions to install to the specified group, to be able to login.

It is best used for 1 or 2 installations, by a single user.

Script Installation

This is by far the most common installation method.

With this method, the Cyber Crucible web application automatically configures the installation process, and secure agent bootstrapping to the web application.

A Windows batch file is used. While there are other more complex installation methods possible, this method has the widest compatibility with Remote Management tools.

The batch file may be run as a user with the appropriate permissions (usually administrator), or copy/pasted into your preferred automatic deployment tool.

Below is a technical examination of the contents of the batch file, which may be configured to your needs.

Installation Script Detailed Examination

The group identifier selected during script creation is entered into the script, as is the oauth token required for agents to join the specific group.

47480849.png?width=680
Please note that this oAuth authentication token is not associated with the web application, nor any user. It cannot be used to make REST calls to the web application API.

In some environments, permissions may be gained automatically. This is typically in circumstances where a user is running the installation script by clicking on it, versus programmatic access. In enterprise environments or automated deployment tools, it likely is not executed.

47480857.png?width=680
At this next location in the script, the file location that the installer may be downloaded and executed from may be customized.

It is highly recommended to make this location local to the machine the tool is being installed on. Multiple machines downloading installers to the same location will cause failures and overwrites.

Please note that automatic restart via the installation script is not used by default. This is because automated reboot in this script lacks the management to schedule installs for a specific time, clean shutdown methods which check whether the user is currently logged in or running applications, or giving warning to the user of an impending reboot.

47513621.png?width=680

This next section performs the download and custom naming of the installer on the machine. Please note that the date and time is used to provide uniqueness to the installation file, in case it is downloaded multiple times with different settings or versions.

Bitsadmin is a Windows utility that attempts to download files without negatively impacting the machine if the Operating System is currently under heavy load.

47448109.png?width=680
In some environments the Bits protocol is disabled. Additionally, bits may be in a non-operational state due to a Windows error. In case the download via Bits fails, the next section uses an alternative method (.net JSC) to download the installer file. This code only executes is the previous bits downloader failed.

47415316.png?width=680
After the installer is downloaded, this final section of the script runs the installer. Please note that customization of the command line arguments should be tested, to ensure that installer.exe settings and protections align with the command line arguments provided here.

Please open a support ticket if additional settings are required, or for advanced environments such as SSL man in the middle settings.

47480877.png?width=680
Please notice that reboot is not required, and commented out from execution. Rarely, more commonly in older versions of Windows, drivers would not register & load in the operating system despite being instructed to by the installer. In those scenarios, the easiest method of ensuring the driver is loaded, is to export agents to an Excel document, and look for missing machine names from your list of assets. If all of the installations are in a new group, agent counts may also be used.

47480889.png?width=680
This section at the end of the installation script is the function used to download the installer using JSC if required. It is only executed if .net JSC is leveraged to download the installer, such as if bits fails.

47480895.png?width=680

Firewalls blocking CRL/OCSP certificate authority access (DMZ Mode)

_General

Created by Dennis Underwood on Jul 28, 2025

Background

All Cyber Crucible communications from the endpoint agents to the CC infrastructure is protected by TLS. The list of domains used by CC agents, and each domain's function, is listed here:

Which domains are used by Cyber Crucible?

Access to those domains can be tested by an installer listed here:

How can I test connection to these domains?

Most of those domains listed are directly in control of by Cyber Crucible, and end in *.cybercrucible.com

A couple, notably the AWS Cognito domain required for some token and agent authorization capabilities, are not. Please note that, as of July 2025, agents no longer use Amazon Web Services (AWS) Cognito for machine-to-machine authentication.

By default, HTTPS libraries used by applications, including Cyber Crucible, verify the authenticity of TLS certificates by reaching out to the Certificate Authority (CA) servers via either CRL or OCSP.

This means that a firewall must not block the Certificate Authority domains either. These CA server domains typically service a large number of applications beyond Cyber Crucible, and can require additional justification from network security architect teams.

DMZ Mode

For environments in which the ability to adjust firewalls or other network security tools, to reduce or eliminate the number of tickets to the network security team, DMZ mode can be applied as a group setting.

DMZ mode enabled will do a few things:

- Insert the CA chains into any installer created for that group automtically.
- Automatically install the CA chain files into Cyber Crucible's folders.
- Automatically protect the CA chain files with Cyber Crucible's kernel level anti-tampering technology.
- Automatically configure the Cyber Crucible network communications to rely on the installed CA chain files for TLS certificate (HTTPS) verification.
- Automatically enable a service to ensure the CA Chains are maintained.

Enabling DMZ Mode for currently deployed agents

Turning on DMZ mode for a group with pre-deployed agents will attempt to task all existing agents to use the CA files, without user involvement.

This works as long as the agents are currently able to authenticate with CC infrastructure such as to receive this tasking. This means the agents currently do NOT need DMZ mode enabled, but will in the future. The likely scenario is either movement of the agents to a more restrictive firewall environment, or a desire to remove the existing firewall rules.

Enabling DMZ mode to CC agents which currently cannot authenticate due to CRL/OCSP errors in the CC service logs (likely found in C:\Program Files\CyberCrucible\service_log.0 or .1, etc), will not correct the matter. This can cause a chicken-or-the-egg scenario, if network security rules may not be adjusted at least temporarily, to allow the CC agents to receive the tasking to download and configure the CA chain files.

"Fire escape" method for enabling DMZ Mode for currently deployed agents

There are circumstances where Cyber Crucible agents are deployed without DMZ mode enabled, that cannot receive tasking, and which changing firewall rules to accommodate (even temporarily) to allow agents to receive DMZ tasking is difficult.

In those situations, please find the following digitally signed PowerShell script.

Three baseline requirements for this script to work:

1. This script must be run when the driver is disabled. This probably means Safe Mode, and NOT with Safe Mode Protection enabled in the CC portal. If it is enabled, please contact your Cyber Crucible support resources for assistance with a workaround.

2. This script must have the ability to contact "http://agent.tasking.rpp.cybercrucible.com/public/latestCARoots"
3. This script is digitally signed, so altering the script will cause it to not run by default.

```
if ((driverquery /v | Select-String "CCRRSecMon").Matches.Length -gt 0) {
    Write-Error "Cyber Crucible is running."
    Write-Error "This script only works in safe mode with Cyber Crucible configured to not run i
    exit
}

$installPath = Get-ItemPropertyValue -ErrorAction SilentlyContinue -Path "Registry::HKEY_LOCAL_M
if ([string]::IsNullOrEmpty($installPath)) {
    Write-Error "Failed to get install path.  Is Cyber Crucible installed?"
    exit
}
Write-Host "CC Install path: $installPath"

Write-Host "Fetching CA bundle..."
$json = (Invoke-WebRequest "http://agent.tasking.rpp.cybercrucible.com/public/latestCARoots").Co
if ([string]::IsNullOrEmpty($json)) {
    Write-Error "Failed to get CA roots."
    exit
}

Write-Host "Encoding CA bundle..."

$b64 = [System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($json))
if ([string]::IsNullOrEmpty($b64)) {
    Write-Error "Encoding error."
    exit
}

$standardAlphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/="
$ccAlphabet = [byte[]](0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x11,0x1
$b64 = ($b64.ToCharArray() | ForEach-Object {
    $index = $standardAlphabet.IndexOf($_)
    $ccAlphabet[$index]
})

$persist = New-Item -Force -Path $installPath -Name "persist" -ItemType "Directory"
if (-Not $persist.Exists) {
    Write-Error "Inner directory missing."
}

try {
    Set-Content -Value $b64 -Path "$installPath\persist\dmz.dat" -Encoding byte
    Write-Host "Updated CA bundle."
} catch {
    exit
}

try {
```

```
    Set-ItemProperty -Path "Registry::HKEY_LOCAL_MACHINE\SOFTWARE\CyberCrucibleAgent" -Name "dmz
    Write-Host "Enabled DMZ mode."
} catch {
    exit
}

Write-Host -ForegroundColor Green "Success!  Please disable safe mode and reboot."

# SIG # Begin signature block
# MIISPAYJKoZIhvcNAQcCoIISLTCCEikCAQExCzAJBgUrDgMCGgUAMGkGCisGAQQB
# gjcCAQSgWzBZMDQGCisGAQQBgjcCAR4wJgIDAQAABBAfzDtgWUsITrck0sYpfvNR
# AgEAAgEAAgEAAgEAAgEAMCEwCQYFKw4DAhoFAAQUhmrUkJGB8aa0XQHFmv9zAjy6
# 2Ceggg6IMIIGsDCCBJigAwIBAgIQCK1AsmDSnEyfXs2pvZOu2TANBgkqhkiG9w0B
# AQwFADBiMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYD
# VQQLExB3d3cuZGlnaWNlcnQuY29tMSEwHwYDVQQDExhEaWdpQ2VydCBUcnVzdGVk
# IFJvb3QgRzQwHhcNMjEwNDI5MDAwMDAwWhcNMzYwNDI4MjM1OTU5WjBpMQswCQYD
# VQQGEwJVUzEXMBUGA1UEChMORGlnaUNlcnQsIEluYy4xQTA/BgNVBAMTOERpZ2lD
# ZXJ0IFRydXN0ZWQgRzQgQ29kZSBTaWduaW5nIFJTQTQwOTYgU0hBMzg0IDIwMjEg
# Q0ExMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA1bQvQtAorXi3XdU5
# WRuxiEL1M4zrPYGXcMW7xIUmMJ+kjmjYXPXrNCQH4UtP03hD9BfXHtr50tVnGlJP
# DqFX/IiZwZHMgQM+TXAkZLON4gh9NH1MgFcSa0OamfLFOx/y78tHWhOmTLMBICXz
# ENOLsvsI8IrgnQnAZaf6mIBJNYc9URnokCF4RS6hnyzhGMIazMXuk0lwQjKP+8bq
# HPNlaJGiTUyCEUhSaN4QvRRXXegYE2XFf7JPhSxIpFaENdb5LpyqABXRN/4aBpTC
# fMjqGzLmysL0p6MDDnSlrzm2q2AS4+jWufcx4dyt5Big2MEjR0ezoQ9uo6ttmAaD
# G7dqZy3SvUQakhCBj7A7CdfHmzJawv9qYFSLScGT7eG0XOBv6yb5jNWy+TgQ5urO
# kfW+0/tvk2E0XLyTRSiDNipmKF+wc86LJiUGsoPUXPYVGUztYuBeM/Lo6OwKp7AD
# K5GyNnm+960IHnWmZcy740hQ83eRGv7bUKJGyGFYmPV8AhY8gyitOYbs1LcNU9D4
# R+Z1MI3sMJN2FKZbS110YU0/EpF23r9Yy3IQKUHw1cVtJnZoEUETWJrcJisB9IlN
# Wdt4z4FKPkBHX8mBUHOFECMhWWCKZFTBzCEa6DgZfGYczXg4RTCZT/9jT0y7qg0I
# U0F8WD1Hs/q27IwyCQLMbDwMVhECAwEAAaOCAVkwggFVMBIGA1UdEwEB/wQIMAYB
# Af8CAQAwHQYDVR0OBBYEFGg34Ou2O/hfEYb7/mF7CIhl9E5CMB8GA1UdIwQYMBaA
# FOzX44LScV1kTN8uZz/nupiuHA9PMA4GA1UdDwEB/wQEAwIBhjATBgNVHSUEDDAK
# BggrBgEFBQcDAzB3BggrBgEFBQcBAQRrMGkwJAYIKwYBBQUHMAGGGGh0dHA6Ly9v
# Y3NwLmRpZ2ljZXJ0LmNvbTBBBggrBgEFBQcwAoY1aHR0cDovL2NhY2VydHMuZGln
# aWNlcnQuY29tL0RpZ2lDZXJ0VHJ1c3RlZFJvb3RHNC5jcnQwQwYDVR0fBDwwOjA4
# oDagNIYyaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VHJ1c3RlZFJv
# b3RHNC5jcmwwHAYDVR0gBBUwEzAHBgVngQwBAzAIBgZngQwBBAEwDQYJKoZIhvcN
# AQEMBQADggIBADojRD2NCHbuj7w6mdNW4AIapfhINPMstuZ0ZveUcrEAyq9sMCcT
# Ep6QRJ9L/Z6jfCbVN7w6XUhtldU/SfQnuxaBRVD9nL22heB2fjdxyyL3WqqQz/WT
# auPrINHVUHmImoqKwba9oUgYftzYgBoRGRjNYZmBVvbJ43bnxOQbX0P4PpT/djk9
# ntSZz0rdKOtfJqGVWEjVGv7XJz/9kNF2ht0csGBc8w2o7uCJob054ThO2m67Np37
# 5SFTWsPK6Wrxoj7bQ7gzyE84FJKZ9d3OVG3ZXQIUH0AzfAPilbLCIXVzUstG2MQ0
# HKKlS43Nb3Y3LIU/Gs4m6Ri+kAewQ3+ViCCCcPDMyu/9KTVcH4k4Vfc3iosJocsL
# 6TEa/y4ZXDlx4b6cpwoG1iZnt5LmTl/eeqxJzy6kdJKt2zyknIYf48FWGysj/4+1
# 6oh7cGvmoLr9Oj9FpsToFpFSi0HASIRLlk2rREDjjfAVKM7t8RhWByovEMQMCGQ8
# M4+uKIw8y4+ICw2/O/TOHnuO77Xry7fwdxPm5yg/rBKupS8ibEH5glwVZsxsDsrF
# hsP2JjMMB0ug0wcCampAMEhLNKhRILutG4UI4lkNbcoFUCvqShyepf2gpx8GdOfy
# 1lKQ/a+FSCH5Vzu0nAPthkX0tGFuv2jiJmCG6sivqf6UHedjGzqGVnhOMIIH0DCC
# BbigAwIBAgIQBxoxP5I/FN11CdiDj62hWTANBgkqhkiG9w0BAQsFADBpMQswCQYD
# VQQGEwJVUzEXMBUGA1UEChMORGlnaUNlcnQsIEluYy4xQTA/BgNVBAMTOERpZ2lD
# ZXJ0IFRydXN0ZWQgRzQgQ29kZSBTaWduaW5nIFJTQTQwOTYgU0hBMzg0IDIwMjEg
# Q0ExMB4XDTI1MDEyMzAwMDAwMFoXDTI1MTAyOTIzNTk1OVowgdgxEzARBgsrBgEE
# AYI3PAIBAxMCVVMxGTAXBgsrBgEEAYI3PAIBAhMIRGVsYXdhcmUxHTAbBgNVBA8M
```

```
# FFByaXZhdGUgT3JnYW5pemF0aW9uMRAwDgYDVQQFEwc1NjQ4MDE4MQswCQYDVQQG
# EwJVUzEVMBMGA1UECBMMUGVubnN5bHZhbmlhMRMwEQYDVQQHEwpQaXR0c2J1cmdo
# MR0wGwYDVQQKExRDeWJlciBDcnVjaWJsZSwgSW5jLjEdMBsGA1UEAxMUQ3liZXIg
# Q3J1Y2libGUsIEluYy4wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCc
# gp0cezRZCGf8V3Uq625Qtx17DpHQGPSy0qj0J/BJ1vKuaYkvMlh7tvzyakZm4e88
# clObk/99sz2Xz6+Gs00JmY32CYPVQ9crpliTHco1/Pde65kg0otHe9IvSQJAyrbz
# J3PwnZB8tgFkWKkhaz7MSIjUmiZmrxDJ3Wzhga/87mH3RinBMY5d5C6TahBSyn5p
# RGkzDokJ6zyTeh/XiI72RDH/SHGpfCgAfIz/dHuvZddp5YJ9QLhym5c65VfNHIZr
# c8B9fvit6ADVXJbYfp1DR6C2WogfIJWXo5as+IuHm263qX96+ZoHR1jnTBegUCx6
# z9yqIA1b5bwvWCRse9pFidWFjHVaEX/+eBKDeIeoFPsps+o3E4rGnrB4sDPNd6VZ
# DqM9ddzkHNG5xWWXRIDx82GOVhyqGe8Ma26Je8ks95auuhB+Fpf7kqU80seX9Fqu
# QaWqzz4PywddTmo3eigbdYOcwvYGf5zJh7aouzlEpZBXLvvAozXlpvLFTAU/LoCH
# MkSnEHhY9wY9T40VKHxUG6YYYeydSeqdfV6fXrWfZwJbzsu1DKuUL92lNSlln+Zi
# AFP1BB0hHdE3+p1nKztvGrJPCkRmZfb0TuQcl5PMMpmkjCQhebBjXVLbzka7kALt
# QuXy9guLofly+WrlrLeAyC+mSy6KdAPlmn7jKYmGAwIDAQABo4ICAjCCAf4wHwYD
# VR0jBBgwFoAUaDfg67Y7+F8Rhvv+YXsIiGX0TkIwHQYDVR0OBBYEFMkijav6RdNE
# 3S+ZDCp309eOIGDdMD0GA1UdIAQ2MDQwMgYFZ4EMAQMwKTAnBggrBgEFBQcCARYb
# aHR0cDovL3d3dy5kaWdpY2VydC5jb20vQ1BTMA4GA1UdDwEB/wQEAwIHgDATBgNV
# HSUEDDAKBggrBgEFBQcDAzCBtQYDVR0fBIGtMIGqMFOgUaBPhk1odHRwOi8vY3Js
# My5kaWdpY2VydC5jb20vRGlnaUNlcnRUcnVzdGVkRzRDb2RlU2lnbmluZ1JTQTQw
# OTZTSEEzODQyMDIxQ0ExLmNybDBToFGgT4ZNaHR0cDovL2NybDQuZGlnaWNlcnQu
# Y29tL0RpZ2lDZXJ0VHJ1c3RlZEc0Q29kZVNpZ25pbmdSU0E0MDk2U0hBMzg0MjAy
# MUNBMS5jcmwwgZQGCCsGAQUFBwEBBIGHMIGEMCQGCCsGAQUFBzABhhhodHRwOi8v
# b2NzcC5kaWdpY2VydC5jb20wXAYIKwYBBQUHMAKGUGh0dHA6Ly9jYWNlcnRzLmRp
# Z2ljZXJ0LmNvbS9EaWdpQ2VydFRydXN0ZWRHNENvZGVTaWduaW5nUlNBNDA5NlNI
# QTM4NDIwMjFDQTEuY3J0MAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggIBAI02
# vz6Zr2BevD2bIH1qp/HoayEZmaDxFZbaJAOJGp2aa1o+I8jDFogpMw/sXg3tvU8i
# l32/zDZjVj3g2AIfGnyVaFaVyQTUXMk+F/ODbsK9WogqV11ZopNO5aO1dvYKd5A8
# +fHOgNDswEvUH6dqMrJuH11PU1hXDC2843Qb49SmBqKrY01ZvHMWL4IR6NDCPsa8
# FyVapgwrYdvdYw5tA9r9eVkXzMXfSwT9yMUegZAW/Z6HSE2LPPyXWSUHPT0b8D8e
# pWjmM8ruv4G3TbXZrgYIFBkVPQp9hd1MyUoYYPMTMUir3Zn/Ca7ak2rkE5Hch0+Q
# +a0Ly4vS469ezh/PikriNwTy9zhSsCAnF/T5In6X8lPCoN4m4Ex0lWEqtp5K+bD2
# Oogz2OBfHXTuIhujI0XMZqNWzyfE1iZ4S48G9Y8BBqk9KCY3P379CMBRlsrshOVE
# OT98+zV3YEvDeAJrEDzvKzCBbeER086sGsPX6hRRtJ1x+XCbV+/2YJWW/y0/EsQ4
# tKVWYW5DKQLZsJ66Co8qGKRy9RkHEps2BMrSaAopCbDkNnbVNiOPNZgMw6lXYbt2
# yLGOhA/XNV6hBjSrkuO1hyXWu1Q0Let96IaGwYEIpMR/sHAUki+JjIh/ObdnjboZ
# DlvFCdMHpB7KvGVrcz0e600ACDVubDjn2jbE5T5aMYIDHjCCAxoCAQEwfTBpMQsw
# CQYDVQQGEwJVUzEXMBUGA1UEChMORGlnaUNlcnQsIEluYy4xQTA/BgNVBAMTOERp
# Z2lDZXJ0IFRydXN0ZWQgRzQgQ29kZSBTaWduaW5nIFJTQTQwOTYgU0hBMzg0IDIw
# MjEgQ0ExAhAHGjE/kj8U3XUJ2IOPraFZMAkGBSsOAwIaBQCgeDAYBgorBgEEAYI3
# AgEMMQowCKACgAChAoAAMBkGCSqGSIb3DQEJAzEMBgorBgEEAYI3AgEEMBwGCisG
# AQQBgjcCAQsxDjAMBgorBgEEAYI3AgEVMCMGCSqGSIb3DQEJBDEWBBToaMqnekbD
# 9TNL+/F9FUVmT/wKpzANBgkqhkiG9w0BAQEFAASCAgCWUhYp7TV+jnFD0x3Ep+vL
# /tn8ZW5LpurXf3/IzAA1GhiRy5Kv0D/3fgvV7JvO/ASMwbmOGqhnfkzj5A7G41JA
# sZc18Bd+cz1bvuKd5ykUwhkQQOt3Ha2yBsazwMGarZmPK6SE/NRp0pt2ZyPjr1A6
# kJROiXOrUDAuFAGLZNAhnkhjtBu/x7Uq+8QOaYCXlulNcO1pkmHiELtMapq0Zx5k
# pj+FYJT6tERBpp+79eE37eMpXU3paYJzHziq5vXS6aoaEQrxcvdMTXzzOZS5w+AR
# YAooJCSHahONsyeDdaQC0djLi2mFOmt1eIlJATk6DyjC4N2Lu2ezXte3JH1Jqt1V
# dDNcWmmzNKHAeSdX7OZjKSc44n9sMWA7wvLBxIYjqym3Qs5+VoMs91ODi31WDMtF
# 8OjS9zYxAmnJrMdV6stZQ4XLCN4/KQTCe7ioK7/PcTGNcBMNl5QIRsMWJ8dpqo0V
# S7TNN+19Ou9QkDeTQOc2C2ZVIMf43DNtkBFl2fvL+pZtH3IzMk+Ddpv1izJ4DV1y
# p7qsxRlK9y4Idt+OKIorQLtMiGGDreeKZkNLKVz5is8YrjJ6kMwr1djhNeG+ylK2
# FTZJhuybB22z7fRoC7Z1JBwBoGhiwvjFSI+MJh9cbJN2X5lTXazxvkK7QJSkcqwh
```

```
# 23476c/iOV1mHRRSCpvDKA==
# SIG # End signature block
```

Hosts File IP Addresses

Notice

> These IP addresses are up to date as of **August, 2025**. But are liable to change. It is important that these IPs are used only for testing communication errors, and that DNS resolution failures are actually resolved. These IPs are liable to change in the future, particularly due to load balancing.
>
> Note that deprecated domain names/services, such as Amazon Cognito are not provided.

Domain ?? IP Addresses: Hosts File Format

For an up to date list of required domains, please see

https://support.jira.cybercrucible.com/servicedesk/customer/portal/1/article/34603009

The following IPs are required by the **Cyber Crucible Agent** for endpoints' connectivity.

```
151.181.219.152 agent.oauth.rpp.cybercrucible.com
151.181.219.153 agent.tasking.rpp.cybercrucible.com
34.210.57.13    installerfiles.rpp.cybercrucible.com
```

How do I locate installation logs?

Created by Kyle Nehman on Aug 04, 2025

Headless CLI installers output their status and logs both to `stdout` and to a log file, located in the local directory of the installer exe. By default, when using a pre-packaged script, such as the ps1 or bat scripts downloaded from https://dashboard.cybercrucible.com, the log file will be located in the root of the C: drive.

Installation log files are named `cc_installer.log`

GUI installers do not produce the same log files, as they are not headless, and all logs are displayed in the scrollable text section of the GUI window.

Forcibly Push Installer to AD Domain

Created by Kyle Nehman, last modified on Aug 07, 2025

In some fragile environments, particularly if recovering from a recent attack or outage, normal RMM and/or SCCM deployments might not be an option. Here you will find a script that can serve as a template for how you might be able to forcibly push a CC installation across an active directory environment.

Note: This script will likely need to be tailored for your use case, and does require domain credentials to run. It is expected that this script would be run directly on a (primary) domain controller.

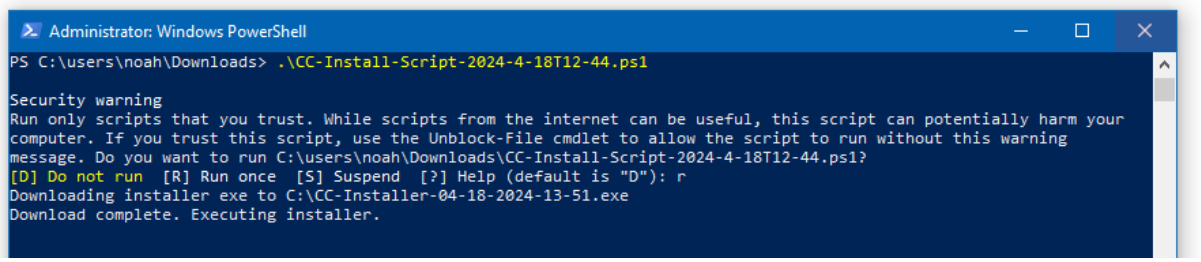
Steps to run

1. Update the `$install_targets` variable with a list of machine names (NETBIOS or similar host names)
2. Download a 'normal' installer ps1 script from the Cyber Crucible dashboard
3. Update variables in the push_installer_ad.ps1 script to be the same as your group specific variables from the dashboard script
    1. `${GroupId}`
    2. `${ClientAuth}`
    3. any `--rest-pub-key` variables
4. Download a native CLI executable from the Cyber Crucible dashboard
    1. Place the CLI on a network share, or somewhere accessible to all machines to be installed
        1. This prevents each machine from having to waste time and bandwidth re-downloading the same exe
        2. The same exe may be executed for different OSs, as the installer will pull down the relevant service/driver/installation files for the detected OS and role of the machine.
    2. Set `${OutputFilePath` to the path of the CLI on a network share
5. Possibly remove ICMP online check (if not needed / invalid for your environment)
6. Run script with `-credential`
    1. e.g. `./push_installer_ad.ps1 -credential ad1\kyle`

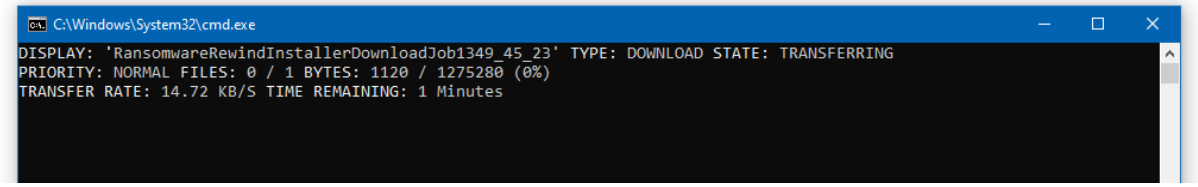
Install Script Overview

Created by Noah Greenberg, last modified by Kyle Nehman on Nov 19, 2024

1. The latest installer is downloaded from `https://installerfiles.rpp.cybercrucible.com/installers/64/installer-cli.exe`
    1. PowerShell (PS1) install scripts will use a WebClient instance.



    2. Batch (BAT) install scripts will use BitsAdmin, or JScript if BitsAdmin fails.



2. Installer is executed and passed the group ID and client authentication provided in your script.
    1. Optionally append `--reuse-agent-by-machine-name` to the execution of the exe, in order to have the installer reuse the agent object & license of a previously installed agent with the the same netbios name.
3. Installer checks for required installation conditions
    1. Running with Administrator privileges.
    2. The machine is running a supported version of Windows.
    3. There is not another installer already running.
    4. The agent is not already installed.
4. Installer checks that the machine can communicate with the required servers.
    1. Amazon oAuth 2.0 at `ransomwarerewind-agents.auth.us-west-2.amazoncognito.com`
    2. Cyber Crucible backend at `agent.tasking.rpp.cybercrucible.com`
5. Agent files are downloaded from `installerfiles.rpp.cybercrucible.com` over HTTPS.
6. The agent is installed and started.

Install with SCCM

Created by Kyle Nehman on Aug 07, 2025

Installing Cyber Crucible with SCCM is no different than any other software package. The key points for deployment via SCCM are:

1. Deploy with the pre-made PS1 script, downloaded from https://dashboard.cybercrucible.com
2. Look for the **Cyber Crucible Agent** service running, or existing on disk, as a detection method. The default location for the agent service is **C:\Program Files\CyberCrucible\service.exe**
    1. Optionally, you can also look for the **HKLM\Software\CyberCrucibleAgent** registry key’s existence, but note that after an uninstall, this key may still be present.

Default Configuration Steps

1. Create an Application, **not** a package
2. Manually specify the configuration

image-20250807-175116.png

3. Configure the application name, vendor name, description, etc.
4. Configure the Deployment Type, and specify **Script Installer**

image-20250807-175303.pngimage-20250807-175332.png

5. Specify script location, likely a network share e.g. **\\cc-dc01\share**
6. Specify installation program to execute the provided ps1 e.g. `Powershell.exe -file “CC-Install-Script-2025-8-7T13-55.ps1`
    1. Note the date timestamp in the script name, and change it to yours
    2. It is not recommended to override powershell policies, but depending on your configuration you may need to specify `-executionpolicy Bypass` or similar
7. Add a Detection Method by clicking “Add Clause”
    1. See recommended detection methods at the top of this page
8. Specify UX deployment settings
    1. Since the Cyber Crucible deployment does not require a reboot, the installation and logon requirements are up to your organizational discretion

image-20250807-175906.png

9. Select Next / Finish until you can close the wizard.