



BUFFERZONE

**BUFFERZONE Safe
Workspace™**

Agent v. 7.3

User Manual

BUFFERZONE™ Ltd.

www.bufferzonesecurity.com

Contents

Introducing BUFFERZONE Safe Workspace™ Pro	3
Setup and Activation.....	5
System Requirements	5
New Installation.....	5
License Extension	8
Source-Based Containment	9
Safe Browser	9
Safe Downloads	11
Safe Mail	12
Safe Removable Devices	13
Managing Containment on the Endpoint.....	15
Stopping and Removing BUFFERZONE Safe Workspace™ ..	19
Solutions & Troubleshooting	20
Agent Command Reference	20
General Troubleshooting	22
Submitting an Issue to BUFFERZONE.....	24
Application Access Syntax	24
Email Message Garbled.....	26
A Site Doesn't Load Properly	26
Agent Behavior is not According to Policy	26
Users can Upload Confidential Files to the Internet.....	27
Agent Doesn't Load	28
Agent Installation Fails.....	28
High CPU on Windows 10.....	29
General Endpoint Issues	29
Can't View Files in Contained Locations.....	30
File Viewer / Editor Crashes	30

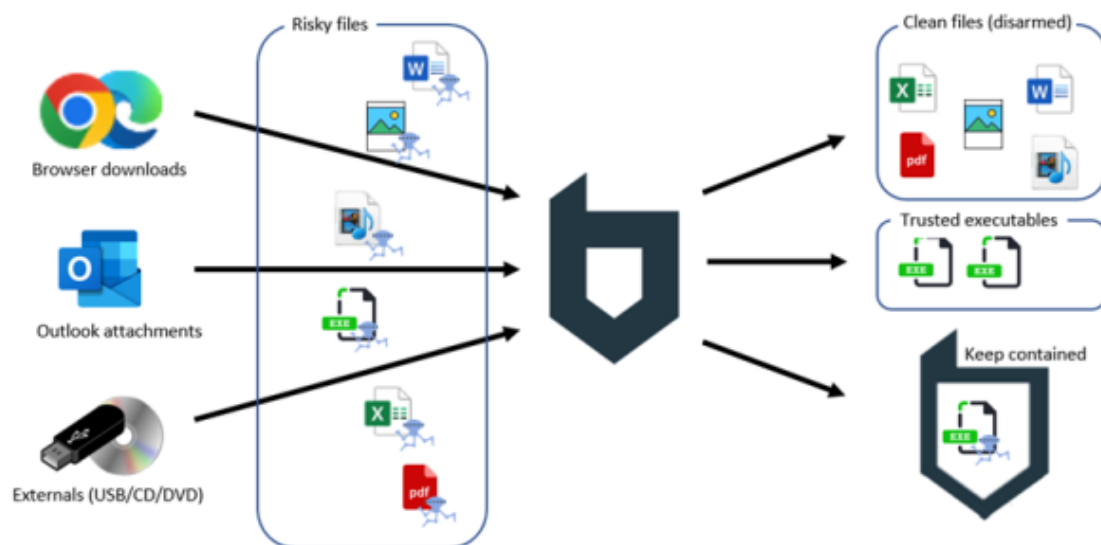
Introducing BUFFERZONE Safe Workspace™ Pro

Let's explain what Safe Workspace™ does.

Safe Workspace™ provides a safe workspace by protecting against all kinds of malware that might reach your computer, from the internet or other sources. Safe Workspace™ ensures this safe workspace by intelligently securing content from risky sources. These sources include browsers, Outlook, and removable media including USB memory and CD/DVDs.

The exact methods of securing content depend on content type and source. In general:

- **Document and media** files (Office, PDF, CSV, PNG, JPG, and JPEG, including in ZIP archives) are **disarmed** of potentially risky components (for example, Office file macros).
- Files such as **executables**, which can't be disarmed, are either:
 - From known, **trusted** publishers: **Allowed**
 - From **unknown** publishers: Kept **isolated** in a virtual container. Even if the file contains malware it can't do any damage to the rest of the endpoint; the container is periodically emptied.



Here's some more detail about how Safe Workspace™ works with each type of source:

- **Safe Browsing** (see [Safe Browser on page 9](#)): With Safe Workspace™, the actual browser process runs in an isolated virtual container, along with any possible effects, to protect against malicious sites. Downloaded files start out contained, and are then handled as above – disarmed, trusted, or kept contained as relevant.

Chrome, Edge, and Firefox are supported.

- **Safe Mail** (see [Safe Mail on page 12](#)): In Outlook, Safe Workspace™ disarms incoming message bodies by rendering inline images as HTML and blocking other inline attachments.

Upon double-clicking attachments, they are handled exactly like browser downloads (as above).

Web-based mail platforms such as Gmail and Outlook Web are secured with Safe Browsing. Safe Mail is for the Outlook desktop application, and is separately licensed.

- **Safe Removables** (see [Safe Removable Devices on page 13](#)): When a file is opened from USB memory or CD/DVD, the access is contained, and then the file is handled like browser downloads (as above).

USB flash drives and external drives are supported; access to phones as storage is blocked. Safe Removables is separately licensed.

When a file is kept contained but the user trusts it, they can manually uncontain it. When necessary, they can choose to start an unsecured browsing session, or to suspend any of the above three protections.

Some Safe Workspace™ features are independently licensed. So, if something described here doesn't match what's seen, the user should extend their license.

Setup and Activation

In most cases, customers should intuitively be guided by email messages and the product installer through setup. Just in case there are issues, this section describes the flows.

In This Section

System Requirements	5
New Installation	5
License Extension	8

System Requirements

Safe Workspace™Pro is supported on systems with the following requirements:

- **OS:** Windows 10/11 64-bit, MS-supported builds
- **Processor, RAM:** As OS requirements
- **Disk:** OS requirements + 500 MB

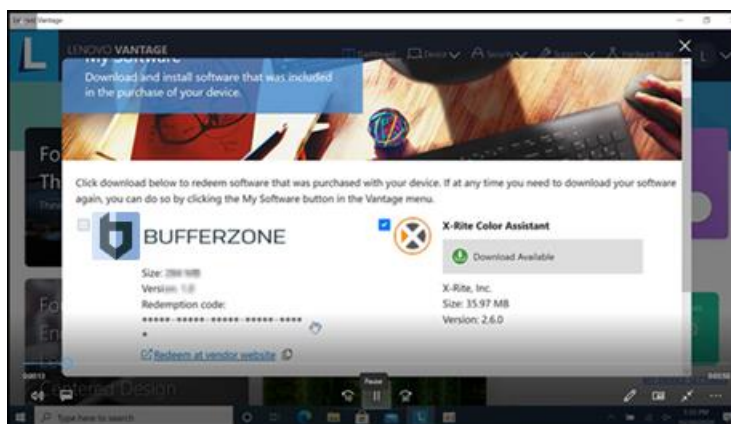
New Installation

Lenovo Vantage customers follow these steps to redeem their eligibility to install and use BUFFERZONE Safe Workspace™:

1. The customer may receive from Lenovo a redemption code for Safe Workspace™ in several ways. In all cases, the customer needs to then go to the Safe Workspace™ registration page. When possible, the customer will have a link to the registration page, and the linked URL will include the redemption code.

Specifically, depending on how the customer has obtained the redemption code, the customer does one of the following:

- In a purchased computer with Lenovo Vantage preconfigured with a BUFFERZONE Safe Workspace™ redemption code, customer goes to **Lenovo Vantage > My software**, and by the BUFFERZONE item clicks **Redeem at vendor website**:



The customer's default browser opens to the BUFFERZONE Safe Workspace™ registration page.

The URL passes the redemption code to the site.

- Upon receiving a purchase confirmation email from Lenovo, customer clicks a link in the email message.

The customer's default browser opens to the BUFFERZONE Safe Workspace™ registration page.

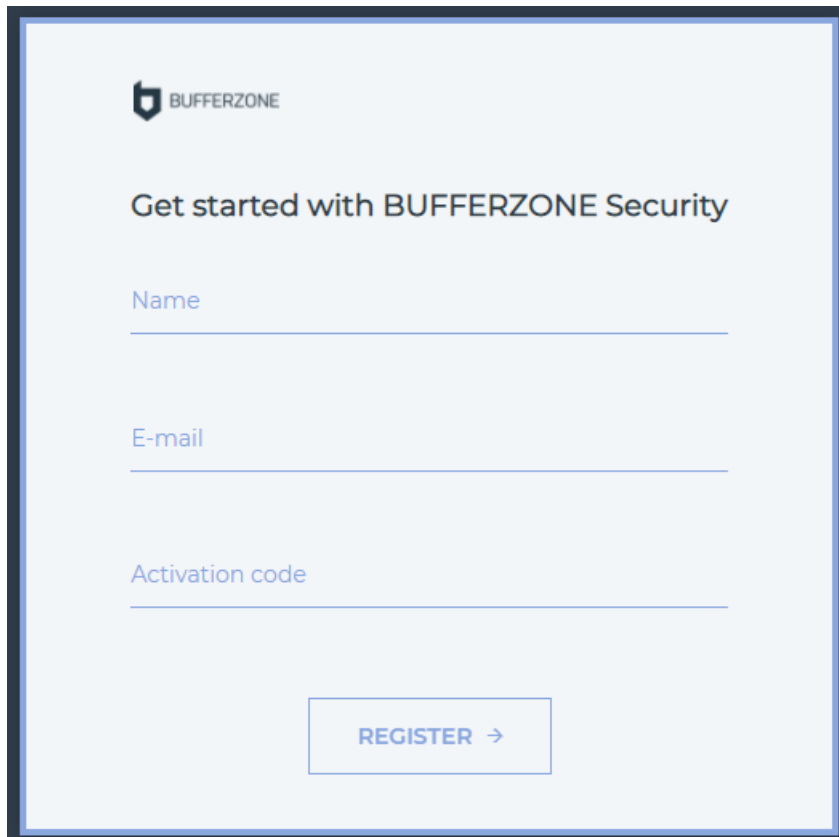
The URL passes the redemption code to the site.

- With a printed or otherwise viewed redemption code for BUFFERZONE Safe Workspace™, the customer opens their browser to the printed or viewed address of the registration page:

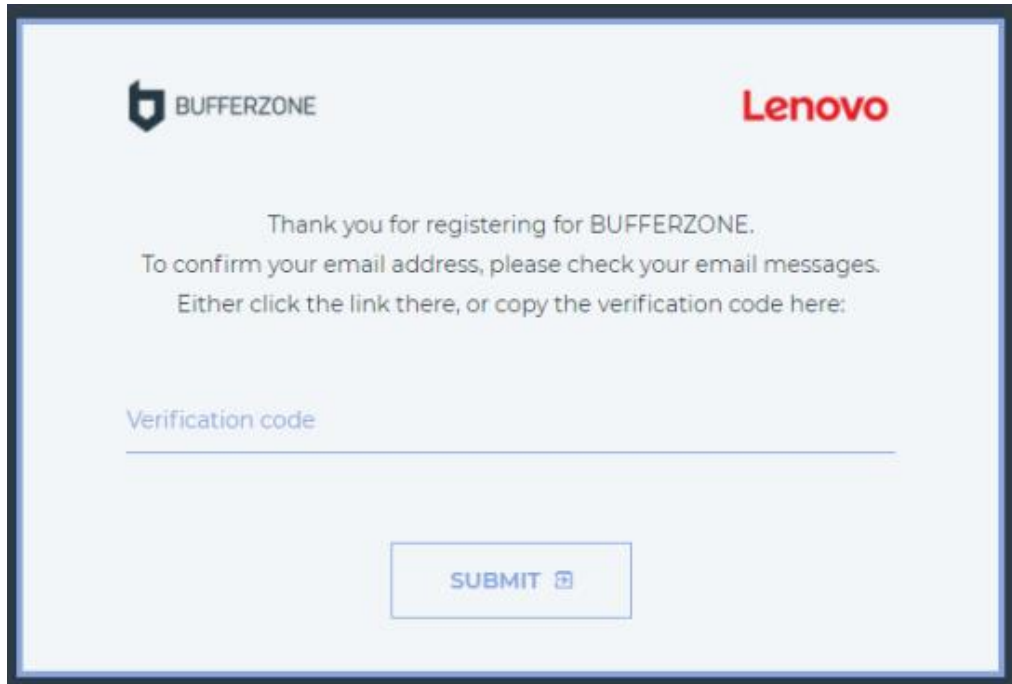
activate.bufferzonesecurity.com

A shortcut link to this address may be present on the computer desktop.

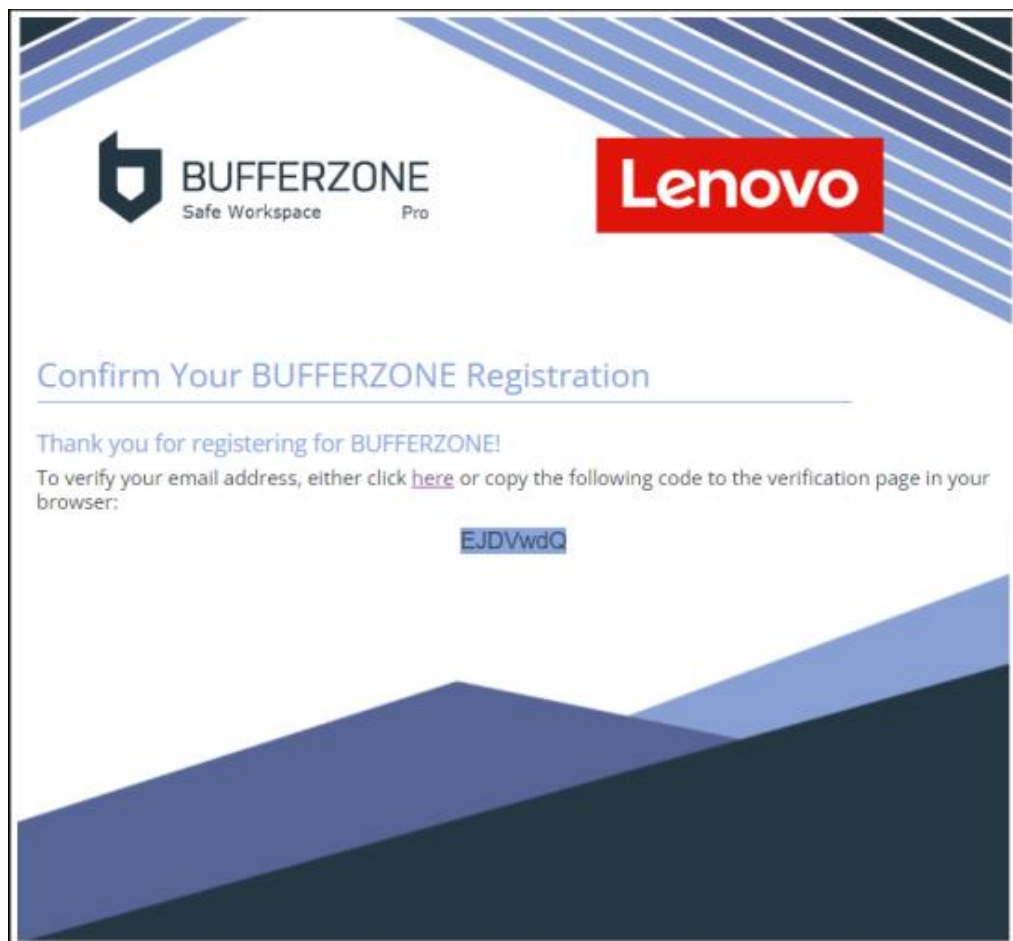
2. Customer registers, and if necessary provides their redemption code. The Redemption code field appears only if the URL did not include a redemption code:



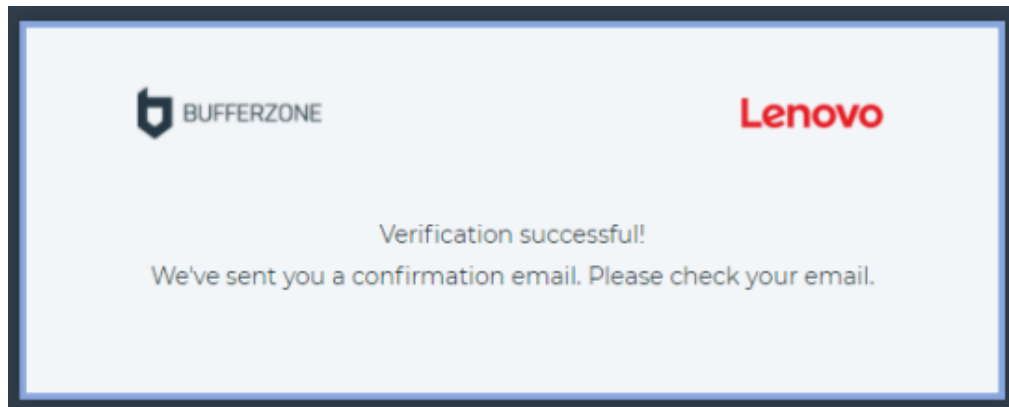
3. Upon submitting, confirmation appears with email verification field:



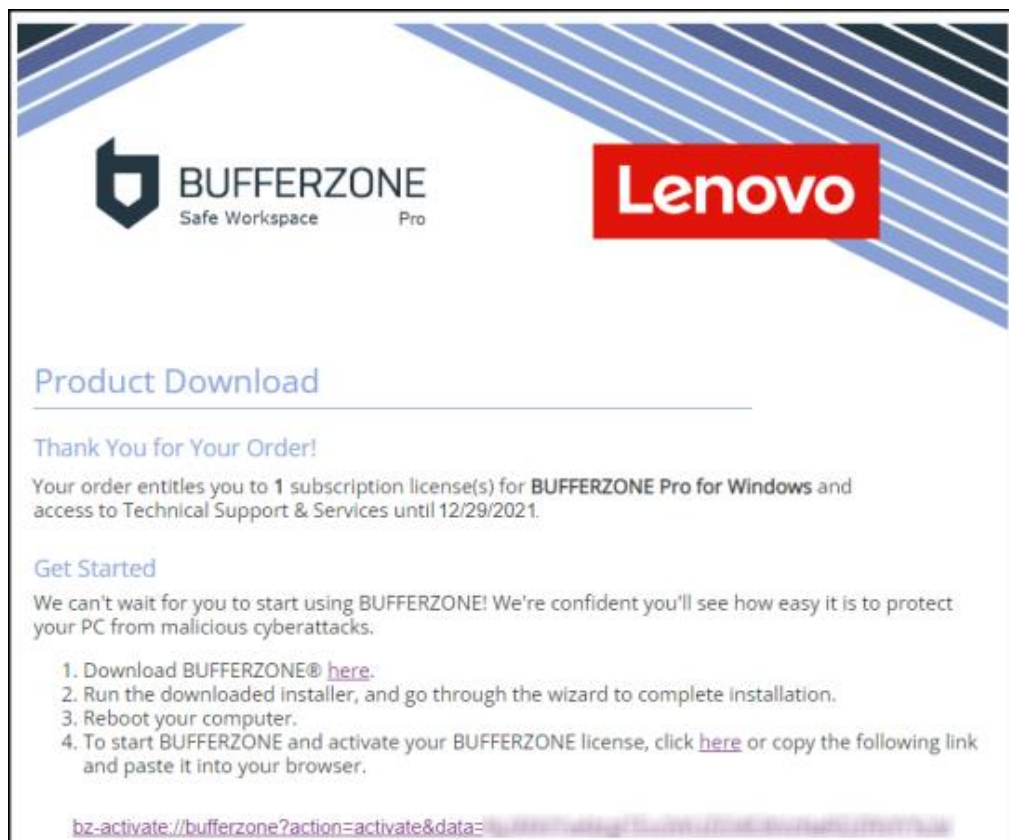
4. Customer receives verification email:



5. Upon successful verification:



6. Customer receives confirmation email:



7. The customer downloads and installs BUFFERZONE Safe Workspace™, including reboot. Clicking the link in the email message (or copying it into a browser) starts the Safe Workspace™ agent and passes the code to it. The agent then self-activates by connecting to BUFFERZONE and receiving a license.

License Extension

Customers can purchase a license extension from the Lenovo store, to enable additional features or to extend the license period.

Customers who purchase a license extension will receive a confirmation email including a link. Clicking the link (or copying it into a browser) starts the Safe Workspace™ agent and passes the extension code to it.

Source-Based Containment

BUFFERZONE contains and/or disarms content from untrusted sources. The following sections describe this behavior.

In This Section

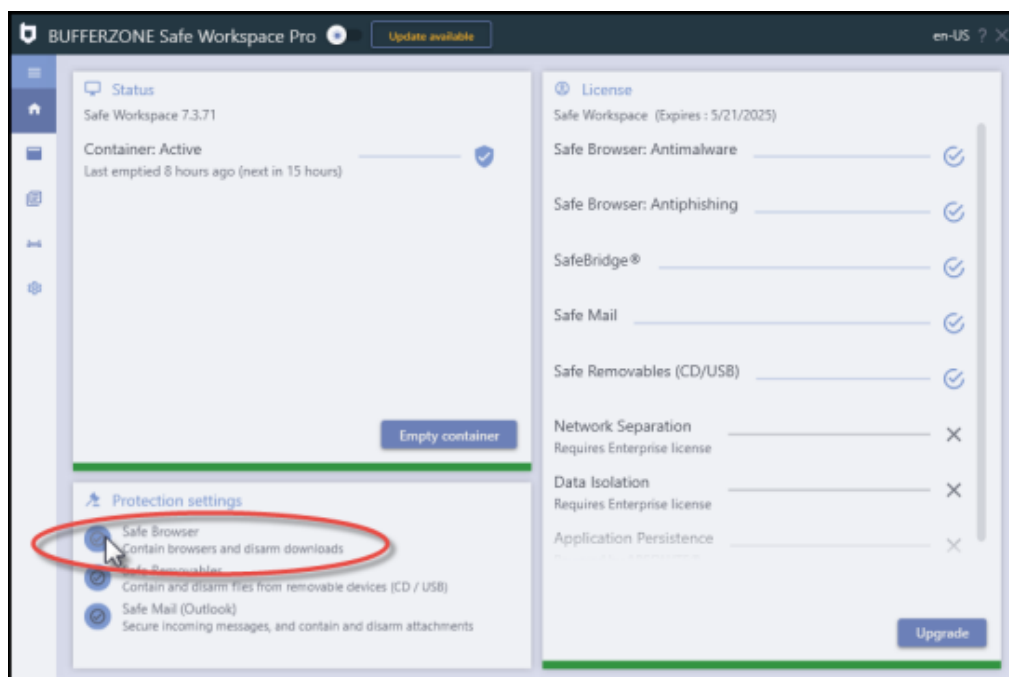
Safe Browser.....	9
Safe Downloads.....	11
Safe Mail.....	12
Safe Removable Devices.....	13

Safe Browser

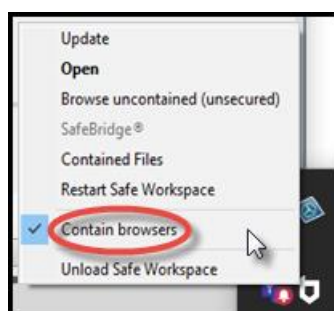
Browsing sessions may be contained, so that the browser instance process is securely contained.

You can set whether by default to **Contain browsers**, in either of the following two places:

- In the agent UI home page (to open it, double-click the BUFFERZONE tray icon):



- Right-click the BUFFERZONE tray icon:

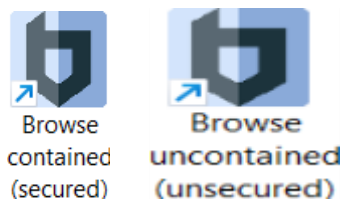


When default behavior is to contain new browser instances, browser shortcuts are marked with the BUFFERZONE icon:

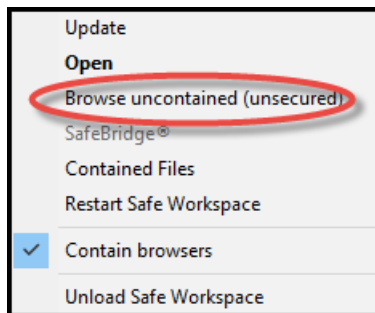


To start a browsing session with containment different than the default set above , do one of the following:

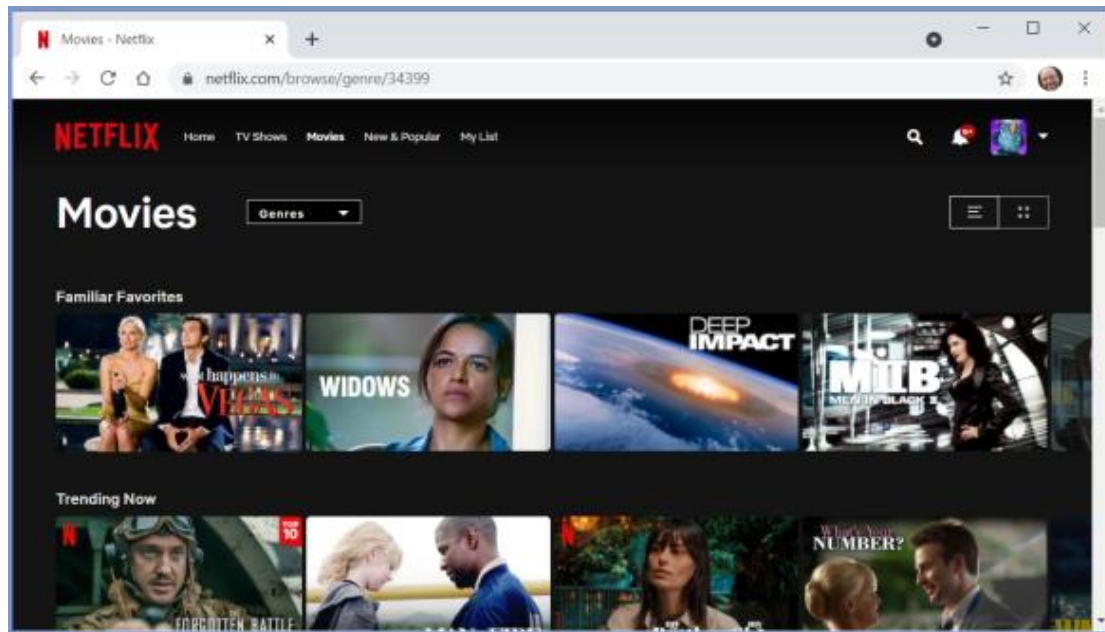
- Use the icon on the desktop:



- Right-click the BUFFERZONE tray icon and select **Browse inside / out of container:**



To make endpoint users aware of the environment they you are working in, contained browser windows are marked with a blue border:

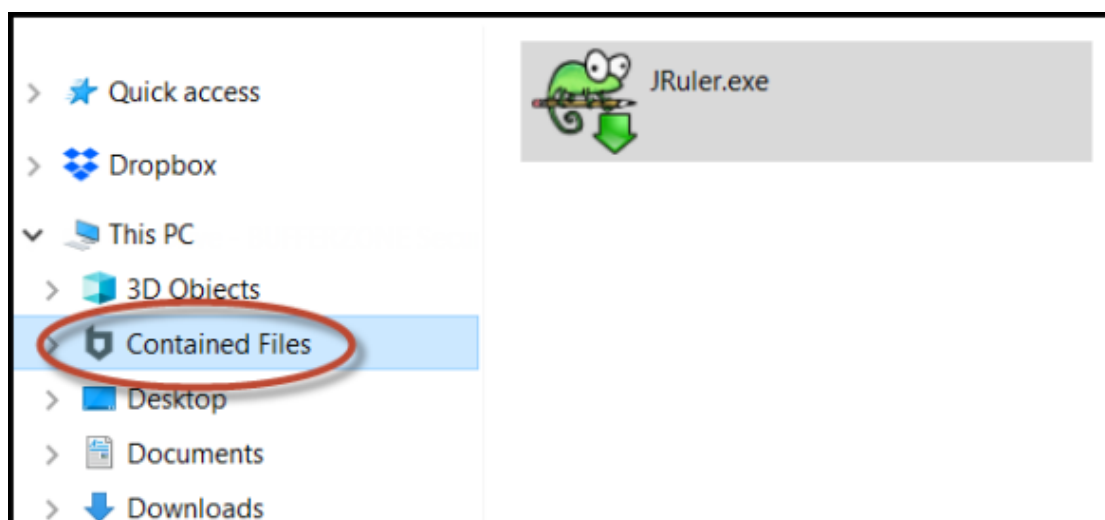


Supported browsers are vendor-supported versions of Chrome, MS Edge (Chromium-based: Edge version 79 and above), and Firefox.

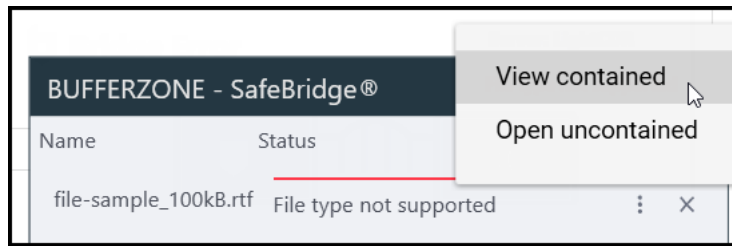
Safe Downloads

Common file types (Office, PDF, CSV, and media files, including in ZIP archives) downloaded from contained browser instances are automatically bridged: they are securely disarmed of potentially dangerous content, and then uncontained. Executables from well-known, trusted publishers such as Microsoft, Google, Adobe, Zoom, and WhatsApp are allowed out of the container.

Untrusted files that are not supported for bridging remain contained and are not downloaded to regular locations; instead, they appear only in the secure **Contained files** folder, listed in the navigation pane of Windows File Explorer:



For files that are not successfully bridged, from the SafeBridge notification you can select to:



- **View contained** (for content files, not executables): Open in the contained BUFFERZONE Viewer / Editor.
- **Open uncontained:** Insecurely remove from container and open.

From the **Contained files** folder, you can right-click and select to do the following:

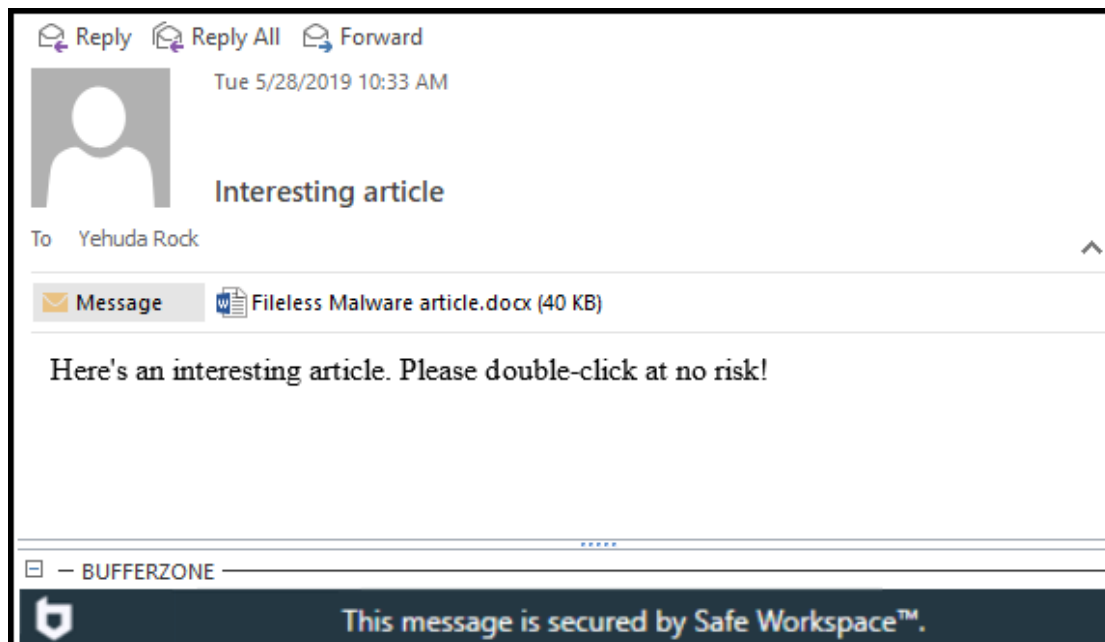
- **Uncontain without security:** If you confidently trust the file, select **Save As (non secure)**. Navigate to an uncontained location to place the file.
- **Rename or Delete.**

Safe Mail

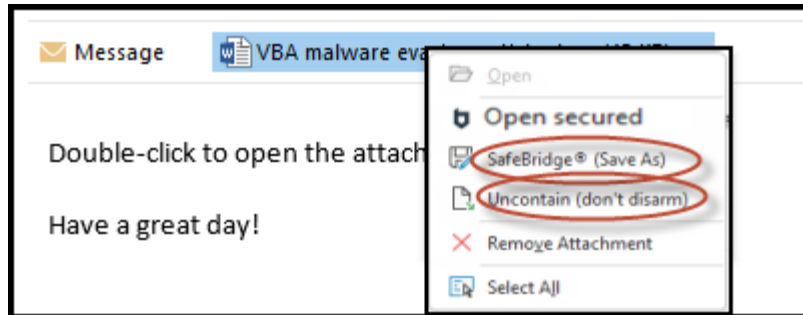
Safe Mail disarms Outlook incoming email messages and contains their attachments, protecting the endpoint and trusted organizational resources from possible malware in messages and in attachments.

Disarming of message bodies includes rendering inline images as HTML and blocking other inline attachments. Regular attachments are automatically disarmed like contained browser downloads (see [Safe Downloads on page 11](#)).

In Outlook, messages include an informative message:



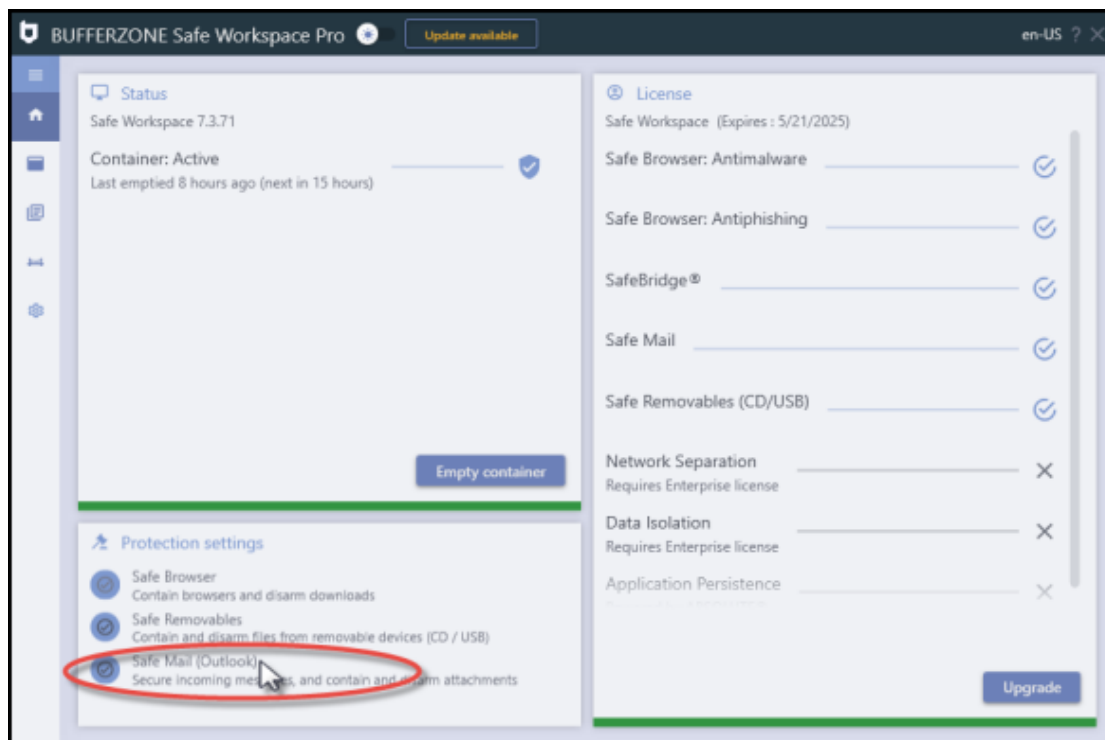
The message body is disarmed, and double-clicking an attachment disarms and opens it.



If you need to uncontain a trusted attachment that cannot be disarmed (for example, executables), you can right-click > **Uncontain (don't disarm)**.

Dragging attachments is disabled.

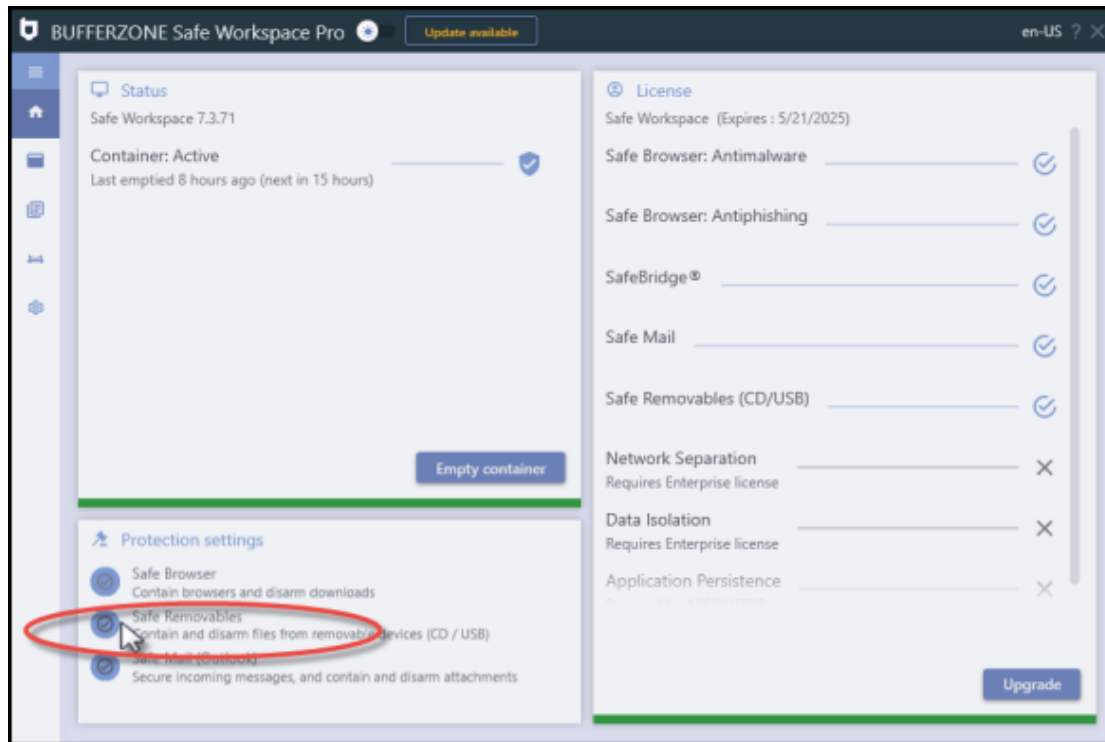
If necessary, you can disable Safe Mail in the Safe Workspace™ agent UI (double click the Safe Workspace™ tray icon):



Safe Removable Devices

External file sources such as removable media (USB drives, and CDs/DVDs) should generally not be trusted. Endpoint access to these sources is contained, preventing any malware that might be present from affecting native endpoint resources. Documents and media from them are treated like browser downloads (see [Safe Downloads on page 11](#)).

If necessary, you can disable removable device protection in the Safe Workspace™ agent UI (double click the Safe Workspace™ tray icon):

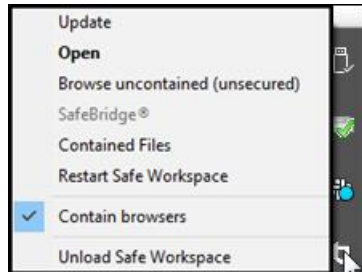


USB flash drives and external drives are supported. Phones as storage are not supported; when removable device protection is active, access to phones is blocked.

Writing to CDs/DVDs is not supported.

Managing Containment **on the Endpoint**

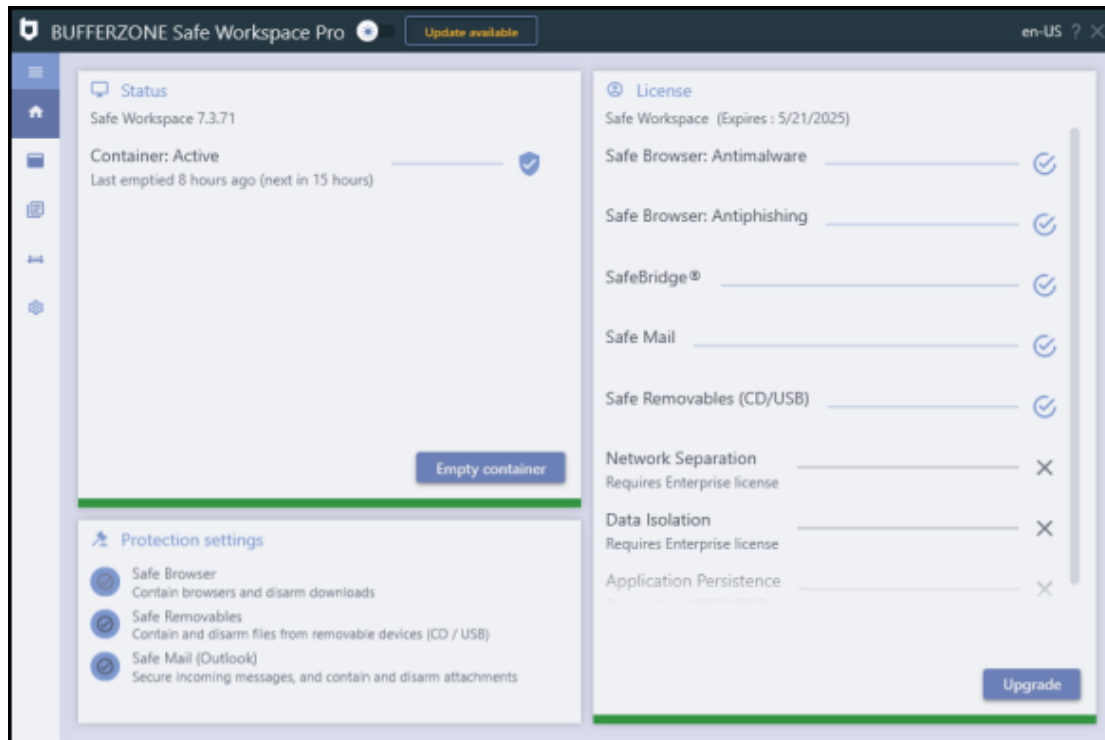
To manage Safe Workspace™ containment, right-click the Safe Workspace™ system tray icon:



Context menu options are:

- **Update:** Check for available updates to Safe Workspace.
- **Open:** As when double-clicking the icon, opens the agent UI. See below.
- **Browse contained (secured) / uncontained (unsecured):** Opens the default browser with containment different than current default.
- **Contained files:** Opens Windows File Explorer to the **Contained files** folder of contained, non-bridged files.
- **Restart Safe Workspace™:** Restarts the agent. Contained files are not removed.
- **Contain browsers:** Define default behavior for supported browsers.
- **Unload Safe Workspace™:** Stop the Safe Workspace™ agent.

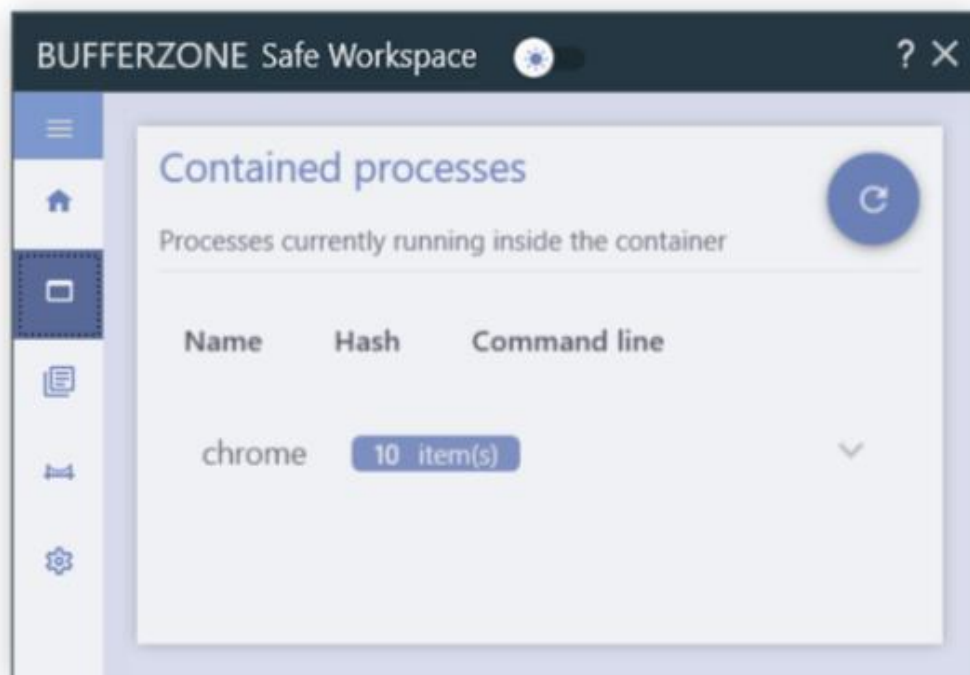
You can double-click the tray icon to view agent status, manage default containment behavior, and empty container:



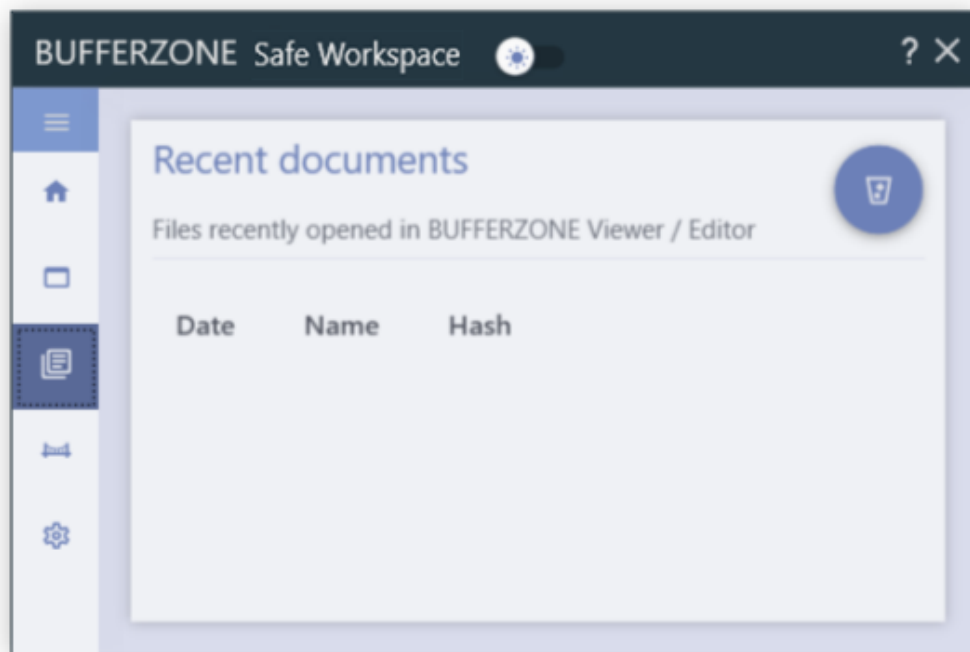
To delete all contained files including documents and media, go to the **Advanced** tab (as below) and **Reset container**.

From the left-hand menu you can go to lists of contained processes, recently-opened (in Viewer/Editor) documents, recently bridged files, and troubleshooting tools. The pages (in addition to home page) are:

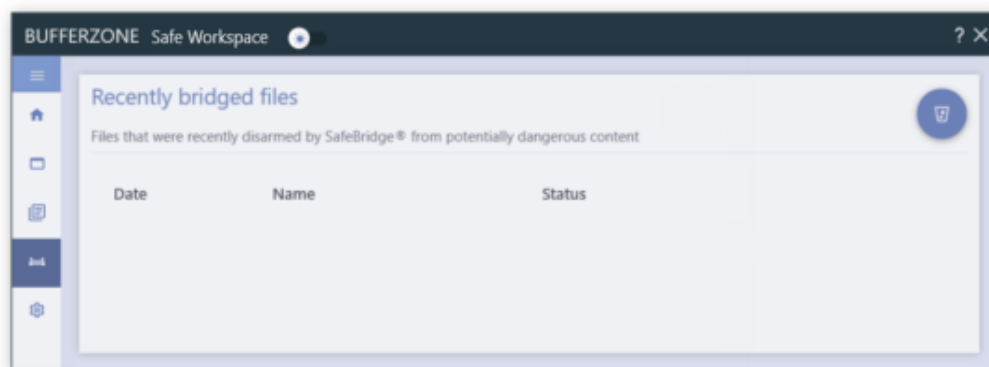
- Contained processes:
Lists processes currently running inside the container.



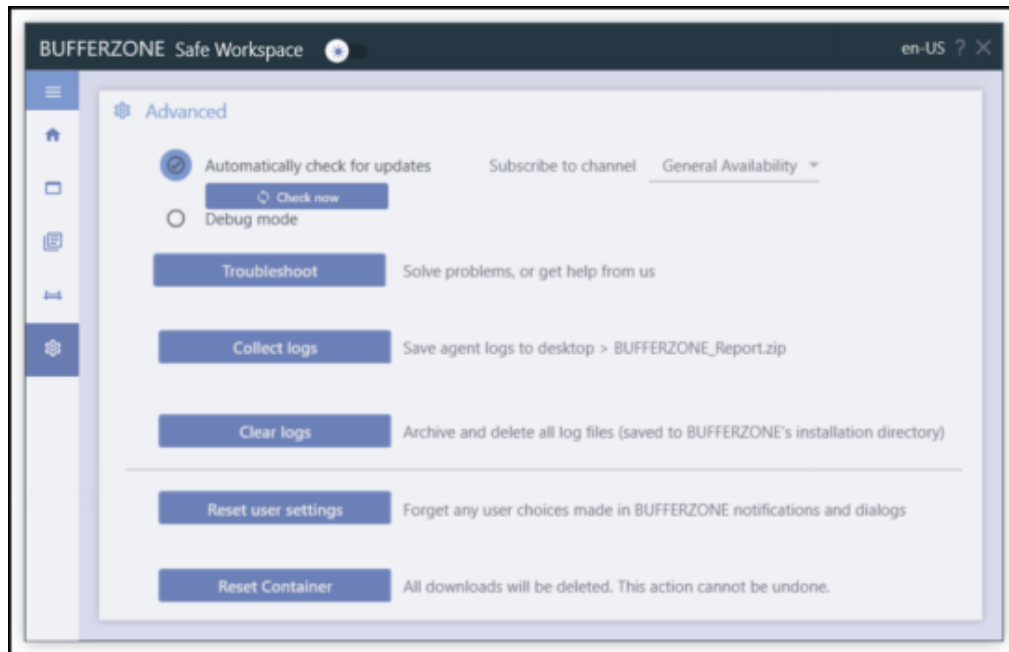
- **Recent documents:**
Lists files recently opened in the BUFFERZONE Viewer / Editor. For example, downloads unsupported for automatic disarming that you viewed contained (see [Safe Downloads on page 11](#)).



- **Recently bridged files:**
Lists files that were recently disarmed and uncontained.

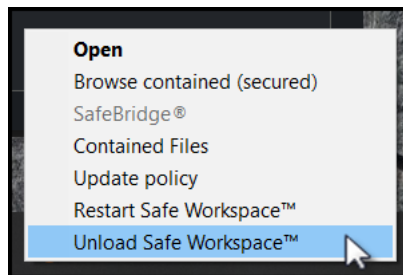


- **Advanced:**
Displays setting for product updates, and troubleshooting tools.



Stopping and Removing BUFFERZONE Safe Workspace™

Safe Workspace™ runs automatically upon startup. To stop Safe Workspace™, right-click the Safe Workspace™ tray icon and click **Unload Safe Workspace™**:



To subsequently restart Safe Workspace™, from the Windows programs menu select **Safe Workspace**.

To remove Safe Workspace™ from your computer, use Windows **Add or Remove programs**.

Solutions & Troubleshooting

The following pages provide solutions for some common scenarios.

In This Section

Agent Command Reference	20
General Troubleshooting.....	22
Submitting an Issue to BUFFERZONE	24
Application Access Syntax	24
Email Message Garbled	26
A Site Doesn't Load Properly	26
Agent Behavior is not According to Policy	26
Users can Upload Confidential Files to the Internet	27
Agent Doesn't Load	28
Agent Installation Fails	28
High CPU on Windows 10.....	29
General Endpoint Issues.....	29
Can't View Files in Contained Locations.....	30
File Viewer / Editor Crashes	30

Agent Command Reference

For various troubleshooting and automation purposes, you can locally run endpoint agent commands. You can combine these commands in custom scripts.

The agent executable is **ClientGUI.exe** , located in the BUFFERZONE installation directory (usually **C:\Program Files (x86)\BUFFERZONE**). To run a command, execute the executable with any of the following arguments, case-sensitive:

In This Section

/BZSTART	21
/BZSTOPUP <user> <password>	21
/BZTPSTOP <user> <password>	21
/BZDISABLE [<time>]	21
/BZRESUME	22
/BZEMPTY [ALL REG FILES PROC]	22
/PERFLOG:<ON OFF>	22
/NOMINALVIEW	22
/EXECBZ "<command>" [<args>"]	22
/BZEXPORT <filePath>.zip	22
/BZIMPORT [<filePath>]	22
/REFRESHALL	22

/BZSTART

Starts the agent. Requires administrative privileges.

For example:

```
"C:\Program Files (x86)\BUFFERZONE\ClientGUI.exe" /BZSTART
```

/BZSTOPUP <user> <password>

Stops the agent, and disables tamper protection (of agent and file container) even when policy is set to protect when agent is paused. If agent administrators are configured, requires credentials, unless policy allows stop by LocalSystem and command is being run as such. When credentials are not required, substitute each of <user> and <password> with a period.

For example:

```
"C:\Program Files (x86)\BUFFERZONE\ClientGUI.exe" /BZSTOPUP ..
```

/BZTPSTOP <user> <password>

Disables tamper protection. If agent administrators are configured, requires credentials.

/BZDISABLE [<time>]

Stops already-contained processes, and temporarily pauses containment for <time> minutes. If <time> is omitted, a default of 15 minutes is used; if more than 60 is specified, 60 is used.

For example:

```
"C:\Program Files (x86)\BUFFERZONE\ClientGUI.exe" /BZDISABLE  
10
```

/BZRESUME

Resumes containment after /BZDISABLE .

/BZEMPTY [ALL|REG|FILES|PROC]

Empties the container. With no arguments - prompts whether to delete each of contained registry settings, files, and processes. ALL deletes all three of these; or you can specify one or two of them, comma-separated with no space between them.

For example:

```
"C:\Program Files (x86)\BUFFERZONE\ClientGUI.exe" /BZEMPTY  
FILES, PROC
```

/PERFLOG:<ON|OFF>

Enables or disables performance logs. Requires administrative privileges and subsequent reboot.

For example:

```
"C:\Program Files (x86)\BUFFERZONE\ClientGUI.exe" /PERFLOG:ON
```

/NOMINALVIEW

For troubleshooting purposes, opens a window displaying agent driver configuration.

/EXECBZ "<command>" ["<args>"]

Runs <command> with <args> inside container.

/BZEXPORT <filePath>.zip

Creates snapshot of container (for example, before emptying the container) at <filePath>.zip . The snapshot can be re-imported as below.

For example:

```
"C:\Program Files (x86)\BUFFERZONE\ClientGUI.exe" /BZEXPORT  
C:\temp\snapshot.zip
```

/BZIMPORT [<filePath>]

Imports snapshot created with /BZEXPORT as above. If <filePath> is omitted, prompts for file.

/REFRESHALL

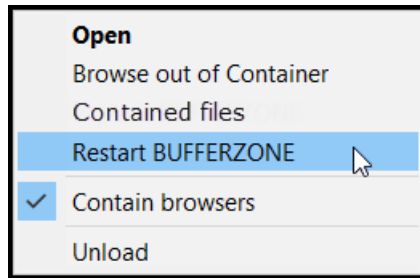
Refreshes policy, like Update Policy button in BUFFERZONE endpoint interface. If managed by BZMS, polls BZMS for new policy; otherwise, just checks registry.

General Troubleshooting

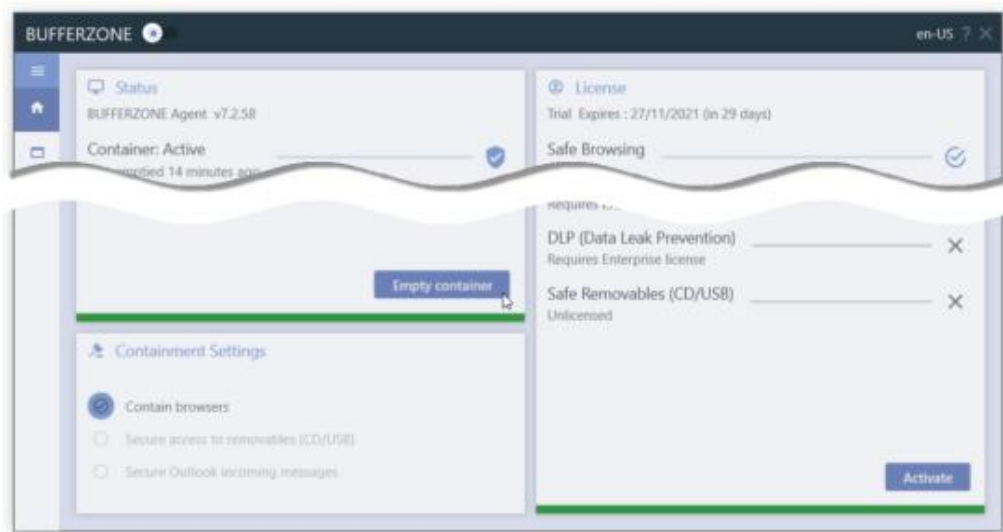
For many Safe Workspace™ agent issues, one of the following steps may solve the problem.

After each step, check if the problem is resolved.

1. **Restart the agent:** Right-click the Safe Workspace™ tray icon and select **Restart**:



2. **Empty container:** Double-click the Safe Workspace™ tray icon to open the agent UI, and click **Empty container**:



Contained documents and other common file types will not be deleted.

3. **Reset container:** Double-click the Safe Workspace™ tray icon to open the agent UI. Go to the **Advanced** page, and click **Reset container**:




All contained files will be deleted.

4. Restart your computer.

If you haven't been able to resolve the issue on your own, report it to us (see [Submitting an Issue to BUFFERZONE on](#) page 24).

Submitting an Issue to BUFFERZONE

If you need to report a problem to BUFFERZONE support, on the relevant endpoint open the Safe Workspace™ user interface and go to:  (Advanced) > **Report an Issue**.

The report automatically includes agent logs for analysis.

Application Access Syntax

When defining processes that are allowed to access contained files (exclusions to Virtual Repository Protection, in policy **Administration > Virtual Repository Protection > Allow access to contained data**) or access-contained external devices and locations (**Externals > Permitted uncontained applications**), you can use either of the following two syntaxes: **Basic syntax** or **Advanced syntax**.

Both syntaxes enable specifying the process name or path and name, and, optionally, the process signer. Advanced syntax additionally enables specifying command-line components. Basic syntax supports wildcards, while Advanced syntax supports Regular Expression (but not for signer name). For process path, environment variables are supported.

Each of these two syntaxes are independent. You cannot combine them.

In This Section

Basic syntax	24
Advanced syntax.....	25
Environment variables.....	25

Basic syntax

<process>[[<signer>]]

where

<process> (required): The process name, optionally including the path; wildcards and environment variables are supported (see **Environment variables** below).

[<signer>] (optional): Bracketed exact title of trusted certificate that signed the process, case-sensitive.

For example:

Entry	Matches
explorer.exe	Any process named explorer.exe
C:\windows\explorer.exe	C:\windows\explorer.exe
explorer.exe[Microsoft Windows]	Any process named explorer.exe that was signed by a trusted certificate titled Microsoft Windows
%WIN%\explorer.exe[Microsoft Windows]	C:\windows\explorer.exe , if signed by a trusted certificate titled Microsoft Windows

Advanced syntax

|<process>| [<command-line>] [<signer>]

where

<process> (required): The process name, optionally including the path; Regular Expression and environment variables are supported (see **Environment variables** below).

<command-line> (optional): The command line that ran the process; Regular Expression supported. Use `.*<term>.*` to match any command line that includes <term>.

<signer> (optional): Exact title of trusted certificate that signed the process, case-sensitive.

Note: The pipe symbol (|) is used only for signifying Advanced syntax and for delimiting its parts. It cannot be used as part of Regular Expression.

For example:

Entry	Matches
explorer.exe	Any process named explorer.exe
notepad\..*\.test1.txt.*	Any process named beginning with notepad. , with test1.txt in the command line. For example: notepad.exe test1.txt notepad.test.exe test2.txttest1.txt
%WIN%\explorer.exe .c:\virtual.* Microsoft Windows	C:\windows\explorer.exe c:\virtual , if signed by a trusted certificate titled Microsoft Windows
%WINSYS%\notepad\..* Microsoft Corporation	Any process beginning C:\windows\system32\notepad. , if signed by a trusted certificate titled Microsoft Windows
.*test.*	Any process with test in the command line

Environment variables

For process path, in both syntaxes, in addition to standard environment variables, the following are supported:

Variable	Resolves to (in usual configuration)
%WIN%	C:\windows
%WINSYS%	C:\windows\system32
%DOCUMENTS-ALLUSERS%	C:\users\all users\documents
%PROFILESBASE%	C:\users
%COMMON-APPDATA%	C:\programdata

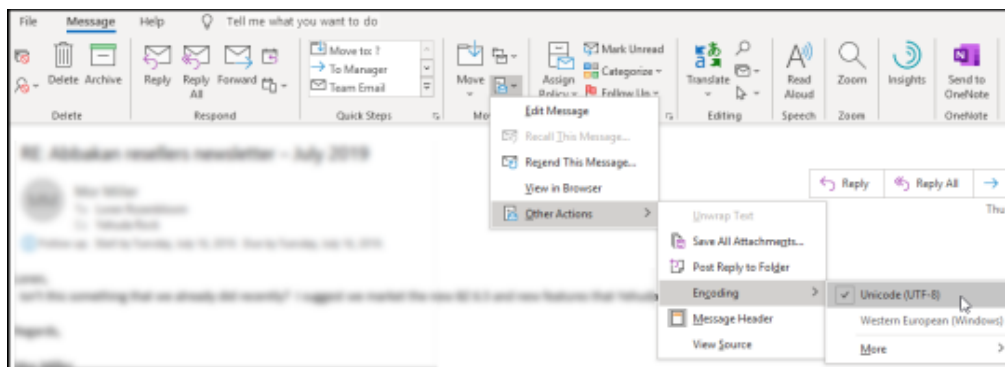
Note: Environment variables are resolved by a service process, so using user-specific variables such as %USERPROFILE% is not recommended.

Email Message Garbled

If, with Safe Mail, an email message appears with garbled characters, it is possible that the encoding is set incorrectly.

To resolve this:

1. In Outlook, double-click the message to open it in its own window.
2. In the **Message** ribbon > **Move** area, go to **More Move Actions** > **Other Actions** > **Encoding**, and select **Unicode (UTF-8)**:



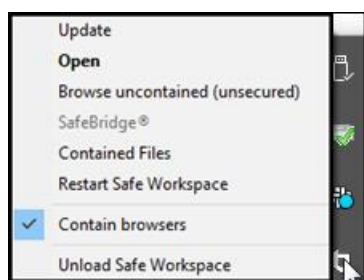
A Site Doesn't Load Properly

If in a contained (bordered) browser, a site page is not loading properly (for example, its images don't appear), first try refreshing it, or closing and re-opening the tab.

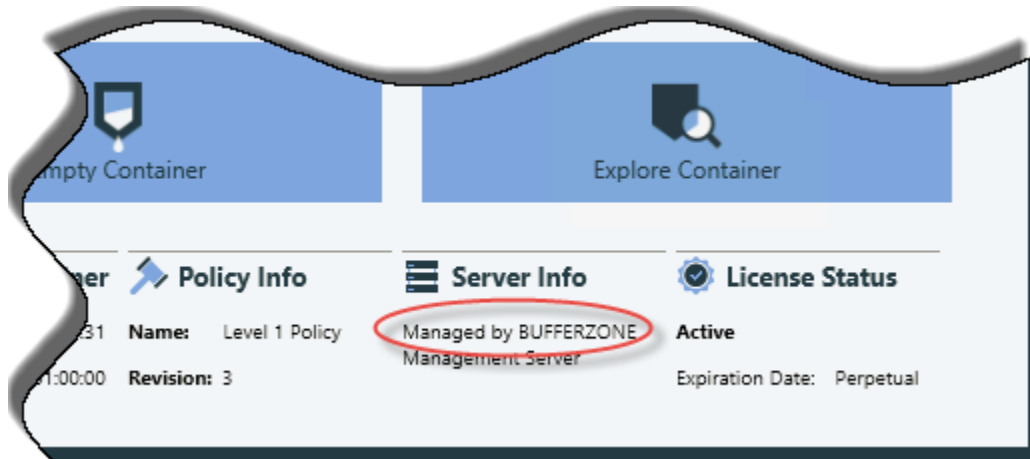
If that doesn't work, go to the Safe Workspace™ UI and **Empty Container**.

Agent Behavior is not According to Policy

If endpoint Safe Workspace™ agent behavior does not seem to be in accordance with organizational configured policy, to check that the agent has received some policy, open the Safe Workspace™ interface (right-click the BUFFERZONE icon and select **Open**):



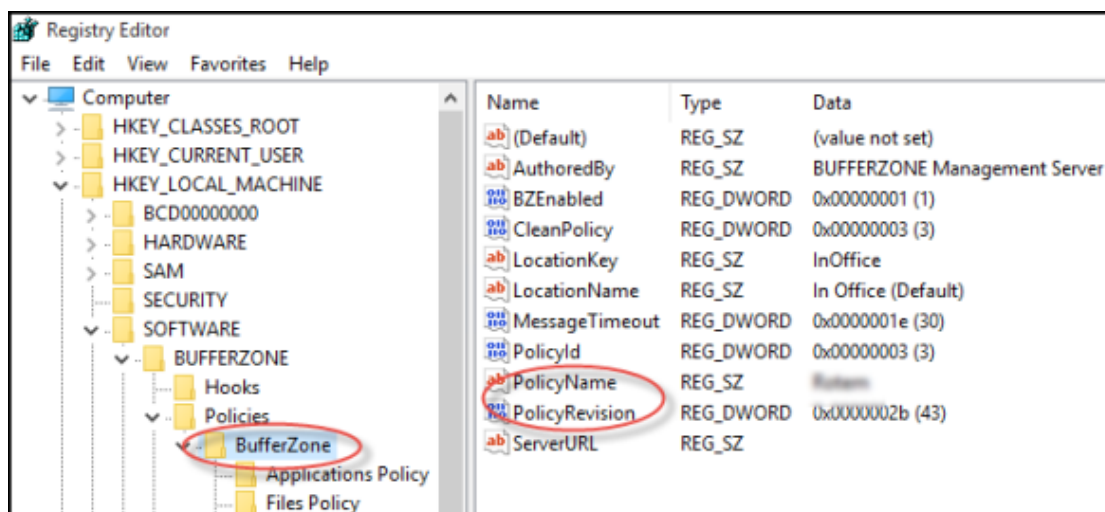
Check if the agent is **Managed**:



If the agent is managed, to check if its policy is the current one, in the computer registry go to:

HKEY_LOCAL_MACHINE\SOFTWARE\BUFFERZONE\Policies\BufferZone

and check the **PolicyName** and **PolicyRevision**:



If the agent hasn't received the current policy, check distribution configuration and group assignment.

Users can Upload Confidential Files to the Internet

The Safe Workspace™ container protects endpoints and organizations from external threats by keeping files downloaded from the internet from reaching organizational resources, but does not, by default, prevent organizational informational resources from reaching the internet.

However, that's just the default; the good news is that BUFFERZONE can do much more.

In addition to its function of protecting endpoints and organizational resources from potential external threats, Safe Workspace™ also provides various features that can contribute to an organization's data-loss prevention (DLP) strategy by blocking information from exiting the organization by various paths. These features include:

- **Hidden Files:** Set endpoint file locations that may contain sensitive data (not system files), to be hidden from contained applications. Optionally, also hide all network locations.
- **Upload Blocker:** When Upload Blocker is enabled in DLP mode, users can upload to contained browsers only contained, downloaded files. This prevents browsers from uploading any potentially sensitive files to the internet.
- **Network separation:** Prevent uncontained applications, which can access organizational resources, from accessing the internet; and prevent contained applications, which can access the internet, from accessing organizational network resources.
- **Clipboard Isolation:** Blocking pasting from uncontained applications to contained applications can help prevent data loss from trusted resources, when network separation or organizational proxy prevents internet access from outside the container.

Agent Doesn't Load

If suddenly the Safe Workspace™ agent unloads due to a fatal error and then can't be loaded, this may be due to a conflict with an endpoint security product (for example, McAfee).

In this case, add either all of the following processes or the whole directories below to the security product's exception list:

- clntsvc.exe
- bzsvc.exe
- clientgui.exe
- bzdcmlaunch.exe
- bzrpcss.exe
- rlhook32/64.dll

Alternatively, add the whole directories:

- %PROGRAMFILES%\bufferzone
- %PROGRAMFILES(X86)%\bufferzone

Agent Installation Fails

If installing the Safe Workspace™ agent fails, locally run the installer interactively (double-click, or command **without** /quiet), and check which of the following error messages appears.

There is problem with this Windows installer package. A program for this install to complete could not be run. Contact your support personnel or package vendor.

Cause: UAC is preventing the installation.

Solution: Run the installer as an Administrator.

A file that is required cannot be installed because the cabinet file... has an invalid digital signature. This may indicate that the cabinet file is corrupt.

Cause: The endpoint is not connected to the internet, so Windows cannot verify the Safe Workspace™ installer's certificate with the Certificate Authority (Symantec).

Solution: Either connect the endpoint to the internet, or manually install the Symantec certificate. For assistance please contact BUFFERZONE support.

Warning 1909. Could not create Shortcut Browse With BUFFERZONE.Ink. Verify that the destination folder exists and that you can access it.

Followed by:

Operation ixoShortcutPropertyCreate called out of sequence.

and rollback.

Cause: Windows 10 Controlled folder access (ransomware protection) conflicts with BUFFERZONE.

Solution: In the Windows Defender Security Center, go **Virus & threat protection** and turn off **Controlled folder access**.

High CPU on Windows 10

If CPU consumption on Windows 10 is very high, this may be due to an issue with the Windows Store (for apps) auto-update.

To resolve the issue, [turn off Store auto-update](#).

This will not affect updates for Windows itself.

General Endpoint Issues

In rare cases, endpoints with a particular version of the Safe Workspace™ agent may experience general hardware (driver) or software issues.

Note: This solution relates to problems appearing throughout relevant organizational endpoints. For an issue appearing on a single endpoint, see other relevant solutions.

In the case of a hardware operation issue that may have been caused by Safe Workspace™ agent installation, there may be a problem with a device driver. In this case, revert Windows to the restore point that was automatically created by Safe Workspace™ before agent installation. Contact BUFFERZONE support for further remediation.

In cases of general (user-mode) software issues that may have been caused by the Safe Workspace™ agent, try the following ways of lowering Safe Workspace™ activity on the endpoint, in order of degree of agent interruption, and contact BUFFERZONE support for further remediation:

- **Pause Safe Workspace™:** The agent continues running and applying other aspects of its policy, but stops already-contained processes and temporarily stops containment. To pause Safe Workspace™, use the /BZDISABLE command (see [Agent Command Reference on page 20](#))

- On the endpoint, right-click the Safe Workspace™ tray icon and select **Pause process container** (if enabled by policy).
- In the organizational policy , select **Pause Safe Workspace™**. When the policy is applied to endpoints, the agent will be paused.
- **Stop Safe Workspace™**: Stop the agent process, in one of the following ways:
 - On the endpoint, right-click the Safe Workspace™ tray icon and select **Unload** (requires administrative credentials).
 - Use the /BZSTOPUP command (see [Agent Command Reference on page 20](#)).

Can't View Files in Contained Locations

If on an agent endpoint files do not appear in contained locations such as the **Contained files** folder or removable storage, the endpoint may be missing a required Certificate Authority (CA).

The required CAs exist in Windows by default, but may have been removed for some reason. To check, on the endpoint run with Administrative privileges:

certlm.msc

In the opened Certificate Manager, go to **Trusted Root Certification Authorities > Certificates**, and make sure the following CAs are listed. Check their thumbprints by double-clicking > **Details > Thumbprint**.

- | | | | | | |
|---|-------------|------------------|----------------|-------------|-----------|
| • DigiCert | High | Assurance | EV | Root | CA |
| Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25 | | | | | |
| • DigiCert | EV | Code | Signing | | CA |
| Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3 | | | | | |

If a CA is missing, download it from [DigiCert](#) and import it to the above location:

- To do this for an individual endpoint, in the Certificate Manager (above), under **Trusted Root Certification Authorities** right-click **Certificates** and select **All Tasks > Import**.
- To do this for organizational endpoints, use GPO as in: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy>

File Viewer / Editor Crashes

If the BUFFERZONE Viewer / Editor is frequently crashing, you may need to clean your disk by removing temporary files.

For more information on how to do this, see:

support.microsoft.com/en-gb/windows/disk-cleanup-in-windows-8a96ff42-5751-39ad-23d6-434b4d5b9a68

About BUFFERZONE

BUFFERZONE endpoint security solutions protect enterprises from advanced threats including zero-day, drive-by downloads, phishing scams and APTs. With cutting-edge containment, bridging and intelligence, BUFFERZONE gives employees seamless access to internet applications, mail and removable storage – while keeping the enterprise safe.

BUFFERZONE (formerly Trustware) has been used by thousands of people around the world to protect their endpoints from constantly changing threats. A free home edition is available on popular download sites.

For more information, visit www.bufferzonesecurity.com, or follow BUFFERZONE on:



twitter.com/BufferZoneSec



www.linkedin.com/company/bufferzone-security



www.facebook.com/BufferZonePro



bufferzonesecurity.com/contact-us

Copyright and Trademarks

Copyright © 2023 BUFFERZONE Security Ltd. All rights reserved. No part of this publication may be copied without the express written permission of BUFFERZONE Security Ltd

This document has been carefully compiled. The information in this document does not constitute a warranty of performance. Furthermore, BUFFERZONE Security reserves the right to revise this publication and make changes from time to time in the content thereof, without obligation to notify any person of such revisions or changes. BUFFERZONE Security assumes no liability for losses incurred as a result of out-of-date or incorrect information in this document.

BUFFERZONE, SafeBridge and the BUFFERZONE logo are trademarks of BUFFERZONE Security Ltd. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Updated September 21, 2023