Bromium Secure Platform

4.1.7 Patch 1 Release Notes
Notices

Copyright © 2019 Bromium, Inc. All rights reserved.

The software and accompanying written materials are protected by U.S. and International copyright law. Unauthorized copying of the software, including software that has been modified, merged, or included with other software, or other written material is expressly forbidden. This software is provided under the terms of a license between Bromium and the recipient, and its use is subject to the terms of that license. Recipient may be held legally responsible for any copyright infringement that is caused or incurred by recipient’s failure to abide by the terms of the license agreement. US GOVERNMENT RIGHTS: Terms and Conditions Applicable to Federal Governmental End Users. The software and documentation are “commercial items” as that term is defined at FAR 2.101. Please refer to the license agreement between Bromium and the recipient for additional terms regarding U.S. Government Rights.

The software and services described in this manual may be protected by one or more U.S. and International patents.

DISCLAIMER: Bromium, Inc., makes no representations or warranties with respect to the contents or use of this publication. Further, Bromium, Inc., reserves the right to revise this publication and to make changes in its contents at any time, without obligation to notify any person or entity of such revisions or changes.

Intel® Virtualization Technology, Intel® Xeon® processor 5600 series, Intel® Xeon® processor E7 family, and the Intel® Itanium® processor 9300 series are the property of Intel Corporation or its subsidiaries in the United States and other countries.

Adobe and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Bromium, the Bromium logo, Bromium micro-VM®, Bromium micro-virtualization, Bromium µVM and Trustworthy by Design are registered trademarks, and Bromium Secure Platform, Bromium Secure Browser, Bromium Secure Files, Bromium Secure Monitoring are trademarks of Bromium, Inc.

All other trademarks, service marks, and trade names are the property of their respective owners. Bromium, Inc., disclaims any proprietary interest in the marks and names of others.

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation. https://attack.mitre.org/resources/terms-of-use/

Bromium Secure Platform 4.1.7

September 10, 2019
Introduction

The Release Notes cover the Bromium 4.1 product release, and subsequent updates, providing information about new functionality and the requirements for the Bromium platform. This document accompanies the Bromium Secure Platform Installation and Deployment Guide, which contains detailed setup and usage instructions for the platform.

Bromium Platform Requirements

The Bromium platform requires the following hardware and software for this release:

<table>
<thead>
<tr>
<th>Hardware or Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Core i3, i5, i7 with Intel Virtualization Technology (Intel VT) and Extended Page Tables (EPT) enabled in the system BIOS. AMD processor with Rapid Virtualization Indexing (RVI). Bromium supports most enterprise class AMD CPUs sold since 2011. Supported models have names of type A4/A6/A8/A10 (followed by a four-digit number in which the first digit is not 3.) Bromium recommends quad-core AMD CPUs for optimal performance. In VDI / nested virtualization environments, Bromium supports Intel CPUs only. Computers with vPro chipsets are highly recommended.</td>
</tr>
<tr>
<td>Memory</td>
<td>Minimum: 4 GB RAM 8 GB RAM  It is recommended that you check the amount of available memory by logging into a device after it has been powered on for a minimum of 30 minutes and before any applications have been launched. As a baseline, Bromium recommends that a typical device have the following amount of memory available before installing and enabling isolation:  Windows 7 32-bit with 1500 MB available memory prior to installation  Windows 7, 8.1, or 10 64-bit with 1800 MB available memory prior to installation</td>
</tr>
<tr>
<td>Disk</td>
<td>6 GB free disk space</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows 7 SP1 32-bit or 64-bit (Professional, Enterprise, or Ultimate) Ensure you have the following two prerequisites:  For Windows 7 32-bit, Physical Address Extension (PAE) must be supported and enabled in the BIOS  To use SHA-2 certificates, ensure you have Windows update KB3033929 or KB2949927 installed  Microsoft Windows 8.1 with Update 1 64-bit (Professional, Enterprise)  Note: The Japanese language version of Windows 8.1 is not supported.</td>
</tr>
</tbody>
</table>

Note: The Japanese language version of Windows 8.1 is not supported.

Microsoft Windows 10 versions are supported as documented in the Bromium Windows 10 Support policy: https://support.bromium.com/s/article/Bromium-Windows-10-Support-Policy

The Bromium Secure Platform EOL policy can also be referenced here: https://support.bromium.com/s/article/Product-Support-and-End-of-Life-Policy-EOL

Note: Refer to your system manufacturer’s documentation for details about enabling virtualization on Intel and AMD processors. If you are using msiexec to install Bromium remotely, ensure you include the SERVERURL setting, otherwise installation will fail.
Required Software for Isolation

- Microsoft Internet Explorer version 8, 9, 10, or 11

**Note:** On Windows 8.1, isolation does not protect web browsing sessions open in the Metro version of Internet Explorer. To allow or block browsing through Metro, add the `Browser.IEMetro.EnableIEHelperHook` setting with a value of 0 (allow) or 1 (block). For more information about adding settings to the policy, see the *Bromium Secure Platform Installation and Deployment Guide* or the online help in the Bromium Controller.

- Internet Explorer 11 Enterprise Mode and the Enterprise Mode site list

**Note:** If you configure enterprise mode using the EMIE site list, ensure you do the following:

1. If the EMIE site list is configured to be on a network path, that network path should be marked as trusted.
2. If the EMIE site list is hosted on a web URL, the TLD should be trusted.

- Microsoft .NET Framework 3.5 or later (pre-installed with Windows 7)
- Microsoft .NET Framework 4.5 (pre-installed with Windows 8.1)
- Microsoft .NET Framework 4.6.2 (pre-installed with Windows 10 Anniversary Edition)
- Visual Basic for Applications (a shared feature in Microsoft Office installation for secure printing from Office)
- XPS Services must be enabled and the Microsoft XPS Document Writer must be present to use secure printing

Additional Isolation Requirements

Bromium installation requires the following:

- Local administrator privileges (if installing on specific machines for evaluation)
- Active Directory administrator privileges (if installing in the enterprise for production use)
- A license provided by your Bromium Sales or Customer Support representative.
- To run isolation in a virtualized environment using:
  - Minimum supported versions:
    - Citrix Hypervisor 7.6
    - VMWare ESX 6.0
  - While customers can run Bromium Secure Platform on the minimum supported versions of the above hypervisors, Bromium always recommends the latest versions of hypervisors as they generally improve performance and stability.
Supported Software

Isolation can be used with any file type (extension) that is associated with the following supported applications:

- Bromium Secure Browsing Extension for Chrome (Chrome SBX) supports the latest Google-recommended version of Google Chrome
- Bromium Secure Browsing Extension for Firefox (Firefox SBX) supports the latest Mozilla-recommended version of Firefox (ESR or non-ESR, 64-bit only)
- Bromium Secure Browsing Extension for Edge (Edge SBX) supports the latest Microsoft-recommended version of the Edge browser.
- Bromium Chrome Isolation is supported with an N-3 policy such that the current shipping version, and the 3 prior versions of Chrome are Supported. Chrome support is detailed in the Bromium Support Knowledge base
- Bromium Firefox Isolation supports Mozilla Firefox ESR 60 (32-bit) release. Bromium is working on supporting on the newly released ESR 68 and its new architecture. Support will be announced in a future version of Bromium Secure Platform
- Microsoft Office 2010, MSI, x86 or x64:
  - Standard, ProPlus
- Microsoft Office 2013, MSI, x86 or x64:
  - Standard, ProPlus
- Microsoft Office 2013, Click-to-Run, x64 and x86:
- Microsoft Office 2016, MSI, x64 and x86:
  - Standard, ProPlus
- Microsoft Office 2016, Click-to-Run, x64 and x86:
- Microsoft Office 2019, Click-to-Run, x64 and x86:

**Note:** Microsoft Office shared computer activation licensing is supported; however, on some systems, when opening an isolated Word document, users may temporarily see a banner stating Office has not been activated.

- Adobe Reader versions DC Classic 2015, DC Classic 2017, DC Continuous 2015, DC Continuous 2017, DC Continuous 2018, and DC Continuous 2019
- Adobe Acrobat Professional version DC Classic 2015, DC Continuous 2015, 2017 Classic, and 2018
- Adobe Flash (all versions)
- Windows Media Player 12 (32-bit and 64-bit)
- Microsoft Silverlight 5.1
- Oracle Java 8 (32-bit)

- Oracle VM VirtualBox
  - While Oracle VirtualBox claims to have nested-VT support, it is implemented in such a way as to be incompatible with Bromium Secure Platform and thus running Bromium Secure Platform in a guest VM inside vBox is not supported. However, Bromium Secure Platform can run alongside Oracle vBox on the host computer from 4.1.6 and later

- Support for endpoints running virtualization-based security (VBS) with the following configuration:
  - Windows 10 64-bit with virtualization-based security (VBS) enabled
  - UEFI Secure Boot enabled
  - The Fast Startup power option in Windows must be disabled
  - Intel vPro 4th generation Core (i3/i5/i7) and newer or AMD Ryzen
  - Trusted Platform Module (TPM) is recommended

- Support for non-vPro Intel chipsets

  **Note:** Bromium Secure Platform previously required vPro chipsets supporting Intel VMCS Shadowing, a feature that improves performance of hypervisors running nested virtual machines by reducing nesting-induced VM exits. Bromium 4.1.4 introduced support for Intel-based chipsets without this technology. Running Bromium without VMCS Shadowing will result in performance degradations vs. vPro systems, however Bromium has taken steps to mitigate performance differentials to all extents possible.

  Limitations of support for non-vPro chipsets:
  - Hibernation / S4 capabilities are disabled and hidden on the host

- VDI deployments on:
  - VMWare Horizon View 7.x (last validated with version 7.3 with ESX 6.5)
  - Citrix Virtual Desktops 7.x (last validated with version 7.18 with Citrix Hypervisor 7.6)

Intel CPUs are fully supported when running the above hypervisors using nested virtualization (nested VT). AMD CPUs running the above hypervisors are considered by Bromium to be in BETA support. Bromium has validated the solution works at a functional level using AMD CPUs. Bromium is continuing to test this configuration and hopes to fully support AMD CPUs and nested virtualization in a future release.

- Windows Defender Credential Guard
- McAfee DLP for Internet Explorer
- Symantec DLP
- McAfee Endpoint version 9.3 and later

Other AV solutions are not yet certified for compatibility with Bromium Secure Platform. If you encounter issues, check the product’s software alert logs.

**Important:** Ensure you create appropriate exclusions in the configuration of installed endpoint security products so as not to interfere with or prevent the normal operation of Bromium products. Necessary actions may consist of excluding all Bromium processes and binaries from the third-party endpoint security product. To create exclusions, refer to your third-party product documentation. The absence of exclusions may result in failed Bromium initialization and slow or blocked browsing and opening of isolated documents. Refer to the Bromium Secure Platform Installation and Deployment Guide for information about creating exclusions.
Please ensure that Bromium isolation is upgraded to the latest version prior to updating to a new version of Windows and you have checked the latest version supports the version of the operating system you are upgrading to.

**Supported Languages**

Bromium Secure Platform endpoint software supports the following languages on the specified version of Windows:

- English US (en-US), all supported versions of Windows
- English UK (en-GB), Windows 8 and later.
  
  On Windows 7, GB is supported as a locale, not a language.

- French (fr-FR), all supported versions of Windows
- French Canadian (fr-CA), Windows 10 and later
- German (de-DE), all supported versions of Windows
- Spanish (es-ES), all supported versions of Windows
- Swedish (sv-SE), all supported versions of Windows
- Italian (it-IT), all supported versions of Windows
- Brazilian Portuguese (pt-BR), all supported versions of Windows
- Japanese (ja-JP). all supported versions of Windows

**Note:** Bromium Secure Platform supports all Windows locales.
Controller Requirements

The following tables list the hardware and software requirements for the server running the controller and the SQL database on which it relies.

Important: Before installing a new version of the Bromium Controller, make sure to back up your current database.

### Bromium Controller Requirements

<table>
<thead>
<tr>
<th>Hardware or Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>SandyBridge Intel Xeon Quad-core or better</td>
</tr>
<tr>
<td>Disk</td>
<td>1 TB free disk space</td>
</tr>
<tr>
<td>Network</td>
<td>Port 443 on the web server must be available for the endpoints to communicate to the controller.</td>
</tr>
<tr>
<td>Internet</td>
<td>Controller is recommended to have https (port 443) access to the Bromium Cloud Service in order to receive Bromium Rules File updates, as well as Threat Intelligence Reports, Malware names and recent attack information. See: <a href="https://support.bromium.com/s/article/Bromium-Threat-Intelligence-Cloud-Service">https://support.bromium.com/s/article/Bromium-Threat-Intelligence-Cloud-Service</a> for more information</td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB RAM</td>
</tr>
<tr>
<td>Software</td>
<td>Microsoft IIS 7.5+ with CGI module, IIS Manager, static content, and anonymous authentication installed .NET 4 Extended (server)</td>
</tr>
<tr>
<td>SSL</td>
<td>Valid SSL certificate trusted by endpoints (For testing only, the server may be configured insecurely to run in HTTP mode)</td>
</tr>
</tbody>
</table>

**Supported Browsers**

The Controller Web Interface is supported on the latest versions of Internet Explorer, Chrome, and Firefox ESR.

### SQL Database Requirements

<table>
<thead>
<tr>
<th>Hardware or Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>200 IOPS sustained per 1000 endpoints</td>
</tr>
</tbody>
</table>
| Software             | SQL Server 2008 R2 Service Pack 3 64-bit  
                        SQL Server 2012 SP4+  
                        SQL Server 2014 SP2+  
                        SQL Server 2016 SP1+  
                        SQL Server 2017  
                        Standard and Enterprise editions are supported  
                        Server Management Studio (SSMS) as the management suite for the controller database  
                        SQL Express should be used in a limited test or evaluation environment only |
| Storage Space        | 1 TB available space |

**Note:** Customers are reminded that they may need to exclude the controller uploads directory from existing AV tools as it contains files that can look like malware and this can confuse other tools, and block Bromium Secure Platform from working properly.
What's New in 4.1.7?

End of Sale (EOS) / End of Life (EOL) Updates

Per Bromium EOL policy (https://support.bromium.com/s/article/Product-Support-and-End-of-Life-Policy-EOL), EOL is the process of discontinuing sales and maintenance for a specific version of the Product. EOS means that product is supported but customers are expected to try to replicate any reported issue on the current version of the software in your production environment. Any fixes released will be applicable to the current version only.

Updates to the Bromium EOL triggered by the 4.1.7 are show below:

- Bromium Secure Platform 4.1 Update 6 (EOS)
  - EOS: 11 Jul 2019
  - EOL: 11 Jan 2020
- vSentry 3.2
  - EOS: 3.2 all updates to 3.2 and all previous releases
    (If you have any versions of vSentry 3.2.x installed in your organization, please contact your Bromium account team, or Bromium Support, to upgrade as a matter of priority)

Platform Updates

Isolation Support for Google Chrome version 74

Bromium isolation now supports Google Chrome version 74 when using the full Bromium Secure Browser. Chrome 74 is also available as an AppPack to be applied to other versions of the Bromium Secure Platform to bring them up to Chrome 74 as per our AppPack support policy https://support.bromium.com/s/article/Product-Support-and-End-of-Life-Policy-EOL.

Microsoft Windows Operating System Support

Bromium regularly updates which operating system versions are supported based on the latest information from Microsoft: https://docs.microsoft.com/en-gb/windows/release-information/

The overall Bromium Windows 10 support policy:
https://support.bromium.com/s/article/Bromium-Windows-10-Support-Policy

Updates in this 4.1.7 release
- No longer supported:
  - Windows 10 (Threshold 2) Version 1511 (OS build 10586)
- New support added:
  - Windows 10 (19H1) Version 1903 (OS Build 18362)

Initial installation

By default, the initial installation of the endpoint software will result in the software being disabled and unconfigured. As a result, the endpoint must connect to a Bromium Controller to receive its configuration and license which may happen during installation (at the prompt or using msiexec parameters) or post-installation using the “brmanage” command: “brmanage management-server <controller name>”.

Until the endpoint receives a license, the software will remain in a disabled state. Once the endpoint has been correctly configured to communicate to a Controller, it will receive a license and initial configuration via policy. At this point, the endpoint software will initialize and will then be available for use (unless marked explicitly as disabled).

This allows the administration team to roll out the endpoint software onto all endpoints in a benign state. The administrator is then able to move devices into Device Groups to receive their license and configuration. This allows an admin to see the entire endpoint estate with enabled/disabled devices in one simple view. This allows customers to complete a single rollout, but phased enablement of software as all disabled devices will appear in the Controller.
Controller Updates

Remote Command Reasons
Remote commands now have a “Reason” box for admins to enter information pertaining to issuing a remote command. This can help organizations understand why a remote command was issued and by whom. This appears in the controller audit log.

Password generator for new user
There is now a password generator button on the new user page to enable faster and easier setting of secure passwords for new accounts.

‘Last seen date’ has been moved.
On the controller status overview pane, the “last seen date” has been moved from the right-hand side, to be under the node name as it refers to the node and not the errors/warning.

Auto Enable Secure Platform
It is now possible to automatically re-enable the Secure Platform after an upgrade or restart/login.
Threat Telemetry

Threat Reports

The Bromium Controller now supports the ability to create custom Threat Reports for a given time period. This report summarizes the threats seen, categories, severity, malware families, MITRE ATT&CK™ framework techniques seen (and protected against) as well as some trend information for the previous time period, days of the week and application attack vectors.

The threat reports can be generated for custom timeframes and can be saved and regenerated at will by customers to reflect and include the latest information available from the Bromium Threat Intelligence Services (if both ‘Threat Forwarding’ and ‘Cloud Services’ features are enabled).

This report is interactive both as HTML and exported as PDF. Recipients can click on the MITRE ATT&CK information to get the latest updates on techniques. The threat report is managed by the standard delegated administration configuration so users must be given access to the threat reports in order to generate and view them.

The report is made up of 4 distinct panels:
Panel 1: Summary information and malware families
Panel 2: Malware family details

Panel 3: MITRE ATT&CK Framework and Techniques
Panel 4: Trending Information

Threat Intelligence Reminders
In order to maximize the amount and quality of threat intelligence information customers have and can use to better protect their businesses, Bromium has added many features over the past few releases (Threat Forwarding and Cloud Services). In order to make this clearer, a reminder has been added to the controller when these features are not yet enabled. When the Threat Intelligence Services are enabled, this reminder disappears. This reminder can also be silenced for a period of time in settings.

Filter threats by hash
It is now possible to filter threats on the main threats table by file hash. This can take the form of MD5, SHA1 or SHA256. Security admins can now easily see if multiple threats have come from the same source. Additionally, admins can also filter by Annotations and Annotation Type, allowing further detailed filtering in the UI.
Threat Summary
For each threat, the threat summary information page has been improved to show the MITRE ATT&CK™ techniques used in the attack. These can be drilled into for more information and link to various 3rd party sources for the latest information for a given technique. The “Threat Forwarding” feature must be enabled to be able to see the MITRE ATT&CK panels for threat summaries.

Threat Intelligence: Files, Behavioral View & Network Tabs
Additional views have been added to the threat pages, which allows security analysts to view the all of the files and hashes related to an attack, a compete behavioral analysis of the threat using the unique micro-VM introspection technology and a comprehensive list of the Network activity captured during the time of the attack. These pages can be stepped through so the analyst can better understand the intent of the malware.

There are also some new additional filters which allow better customization of the pages and reports.
- Event Type (file, process, network etc.)
- Event Action Type (delete registry key, execute, http response, etc.)
- Process (1299: cmd.exe etc.) which process the events occurred in.
- Severity (High, Medium, Low etc.)
- Selected (those events which have been selected)
- Text (String search within path and target process info)
Default Policy Changes

Bromium Secure Platform 4.1.7 includes changes to default policy settings that impact all upgrading customers. If previous settings are required, a delta policy can be used to overwrite the default behavior.

- In order to reduce user friction, normal users are now able to temporarily trust IE websites, where previously they needed administrator rights to do this. Users must enter a reason when temporarily trusting a site.

- Users are now allowed to remove protection from a file without being prompted for a reason, but they will still have to click “yes” when actually removing the protection.

- Only users with administrator privilege are now able to disable Bromium isolation.
New syslog event type for classification as True Positive
This can be enabled by an administrator with sufficient privileges by setting the severity level of the new Threat Intelligence source to Informational or Warning from the default (ignore).

This event message is of the format:

- Device Event Class ID: 2050
- Name: Threat Intelligence True Positive
- Severity: 4
- CEF extension fields as for all our syslog messages (src, shost, rt, msg)

And some Extension Fields specific to this message:

- externalId - the database ID of the threat in the BEC’s db
- cs1 - the threat’s UUID
- cs2 - the threat’s "resources" (document path, URL etc)
- cs3 - the URL for viewing the threat in the BEC UI

Bromium Secure Browser Extension (SBX) for Microsoft Edge
Microsoft recently announced a change to the way their Edge browser will work in the future. Microsoft are stopping all development on their own Edge architecture and will be basing future versions (expected in 2019) on the Google Chromium framework.

You can read more about this in the Microsoft blog here:
https://blogs.windows.com/windowsexperience/2018/12/06/microsoft-edge-making-the-web-better-through-more-open-source-collaboration

What this means for Bromium customers:
In response, Bromium is also moving development from supporting the Bromium Secure Browsing Extension from the current Edge architecture to the new Chromium based product. As such, the current SBX release that supports Edge will remain in BETA release status until EOL. It will be supported for use where customers are happy with the current limitations and user experience, but it will not receive updates as indicated above, as Microsoft themselves are moving away from the current architecture.

Bromium is working towards supporting the new Edge architecture and will provide early access releases of the SBX extension for this new version of Edge as soon as we can after the new browser is available to vendors and customers alike. Please speak to your Bromium rep for the latest news in this area.
Limitations

General

- Excel 2019 files shared using ‘Send as PDF’ file sends the email with a text file attachment instead of a PDF
- Applications opened in isolation (that is, in a micro-VM) are not available to assistive technology such as JAWS and ZoomText Magnifier/Reader
- If the Bromium Platform installation fails on systems running Windows 7, install Microsoft patch KB3033929 and install Bromium again
- Do not install Bromium software from a removable drive, such as a USB drive. Removable drives are not trusted by default and, when the initialization stage occurs, the installer will fail because it can no longer read the data on the removable drive
- On some systems, the isolation Desktop Console and Live View user interfaces can take over 30 seconds to open. If you experience slow display times on a system running Windows Presentation Foundation, open the Services management window and disable Windows Presentation Foundation Font Cache 3.0.0.0. You can also purge the font cache as described in http://support.microsoft.com/kb/937135
- If you are using RDP to access a physical system, you may not be able to interact with the Bromium Desktop Console, Download Manager or Live View because they are "transparent." To resolve this issue, install .NET 4.0 on the endpoint
- Some online meeting websites such as WebEx, Adobe Connect Pro and Live Meeting may not work when opened in isolation. This is because these websites attempt to run executable content on the desktop that is blocked by isolation. To allow these websites to work, mark them as trusted
- Saving to and opening from the cloud is not supported for Office 2013
- If isolation is not already initialized on the system, users that have roaming profiles will see initialization occur the first time they log in to the system
- To install Symantec Endpoint Protection after Bromium, restart the machine first
Web Browsing with Internet Explorer

- Isolated websites are not permitted to run ActiveX controls. If a website does not work due to an ActiveX error and the site is known to be trustworthy, it can be added to the trusted websites list so that it will be run on the local system without isolation.
- Site pinning is not supported.
- Some Internet Explorer settings cannot be modified. If a setting is unavailable, a message is displayed to the user.
- Isolated websites that use a custom file download or upload manager may not work. If the download/upload manager on a website fails and the site is known to be trustworthy, it can be added to the trusted websites list so that it will be run on the local system without isolation. Refer to the Bromium Secure Platform Installation and Deployment Guide for details.
- Isolation does not support TabProcGrowth settings in Internet Explorer.
- Browsing with isolation does not work if Internet Explorer security settings are set to High or if file downloads are disabled.
- On Windows 8, if you attempt to play a movie on the Netflix site, an error page may be displayed, particularly on slow computers.
- Browser.IEAltDownloadAddresses has been deprecated in 4.1.7. If this is set to a list of domains, this is unsupported and should be removed so the product can use its defaults.

Web Browsing with Chrome

- The Flash plug-in must be downloaded from the Adobe site to enable Flash functionality in Chrome.
- Skype extension is not supported.

Web Browsing with Firefox

- If Firefox is already installed on endpoints and has not been launched prior to installing the Bromium platform, you must do the following to ensure browser sessions are isolated in a micro-VM:
  o Launch Firefox to create a new profile for the user. If you have multiple users or if you create new users, you must launch Firefox for each new or additional user.
  o Close Firefox and restart Bromium isolation.
  o You can now launch Firefox in an isolated micro-VM.
- These steps also need to be performed if you create more than one Firefox profile per user.
Documents

- Isolation prevents users from opening any isolated files that cannot be opened by one of the supported applications. If a downloaded file is not currently supported but is known to be trustworthy, right-click the file and select the “Remove Protection” file menu option.

  **Note:** This operation may require administrative access.

- Bromium isolates documents from accessing corporate resources or files stored on the desktop or intranet. As a result, if a document open in isolation attempts to connect to a database on the intranet or a linked file on the desktop, it will fail and produce an error. To enable this functionality, you must remove Bromium protection from the document.

- ASX video files and Windows Update Standalone Installer (MSU) files cannot be opened in micro-VMs.

- Isolation does not support multiple, simultaneous Microsoft Office installations of the same version (for example, Office 2010 Standard in one location and Office 2010 Professional Plus in another).

- Users may receive an error when opening an isolated file with paths containing more than 214 characters.

Controller

- The controller continues to display last known device health status even when the device has not been recently reconnected.
Issues Fixed in 4.1.7 Patch 1

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54480</td>
<td>Controller threat view continues to show &quot;Analysis in Progress&quot; until reloaded</td>
</tr>
<tr>
<td>53918</td>
<td>Custom proxy will fall back to DIRECT mode when PAC URL is unreachable, ie due to a network change, when configured</td>
</tr>
<tr>
<td>53397</td>
<td>Unable to open Office 2019 files on Windows 10 with de-CH language pack</td>
</tr>
<tr>
<td>52730</td>
<td>Failed test boot when enabling support for Hyper-V</td>
</tr>
<tr>
<td>51916</td>
<td>Using ‘CStartMenuCache’ for AUMID resolution causes a crash on 32 bit builds.</td>
</tr>
<tr>
<td>50633</td>
<td>Inconsistent file trust behavior in IE on downloads from Microsoft Team</td>
</tr>
<tr>
<td>54111</td>
<td>Chromium updated to version 74</td>
</tr>
<tr>
<td>53125</td>
<td>False positive discovered when using Windows Media Player in guest on Windows 10 RS6</td>
</tr>
<tr>
<td>54502</td>
<td>No output from the Controller ‘migratedb’ process until it has finished</td>
</tr>
<tr>
<td>54354</td>
<td>Powershell stopped running due to an update on x86 machines</td>
</tr>
<tr>
<td>53981</td>
<td>Some performance issues encountered on Microsoft Surface Pro’s running Windows 10 with Credential Guard and Windows Hypervisor Platform enabled</td>
</tr>
<tr>
<td>53249</td>
<td>Bromium Secure Platform failed to install when Windows BitLocker service is Disabled</td>
</tr>
<tr>
<td>54689</td>
<td>In specific circumstances a Windows 10 could error with &quot;KMODE EXEPTION NOT HANDELED&quot;</td>
</tr>
<tr>
<td>51783</td>
<td>Under some situations, when using an encrypted disk, Bromium Secure Platform cannot open untrusted files (PPTX etc).</td>
</tr>
<tr>
<td>50840</td>
<td>Untrusted documents loaded with Microsoft Office will sometimes show a licensing warning after Bromium Secure Platform has been installed</td>
</tr>
</tbody>
</table>

Issues Fixed in 4.1.7

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28248</td>
<td>When scanning password protected files for malware the operation no longer times out, as the user is now either given the option of trusting the file and entering the password or if the file is deemed to be malicious blocked from removing protection</td>
</tr>
<tr>
<td>43424</td>
<td>When Outlook is set to HTML email format and a trusted or untrusted PowerPoint file is opened and File -&gt; Share -&gt; Email is selected with the 'Send as...' option, the new Outlook message is now sent correctly in HTML format.</td>
</tr>
<tr>
<td>47290</td>
<td>Windows file permission errors are now more clearly explained to the user via a revised Bromium pop-up.</td>
</tr>
<tr>
<td>48248</td>
<td>Splitting untrusted PDFs with Acrobat Pro can now be successfully saved.</td>
</tr>
<tr>
<td>49321</td>
<td>A user will no longer see the message &quot;Need to install a printer&quot; when trying to print a PDF from Bromium in certain limited circumstances.</td>
</tr>
</tbody>
</table>
| 49851    | On the Controller when selecting a device and drilling down to Events, the Messages column
<table>
<thead>
<tr>
<th>Release Number</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49971</td>
<td>When using the SnagIT Editor application, a user is no longer denied access to .PNG files.</td>
</tr>
<tr>
<td>50104</td>
<td>Keyboard input no longer freezes for a number of seconds when editing Excel files on some occasions.</td>
</tr>
<tr>
<td>50117</td>
<td>When outputting an untrusted Word document in PDF format, the PDF no longer opens on both the host and in the VM.</td>
</tr>
<tr>
<td>50121</td>
<td>Fixed an issue where certain non-vPro CPUs failed to allow the machine to boot.</td>
</tr>
<tr>
<td>50152</td>
<td>When a user trusts Excel files with a “Save changes” dialog, it no longer takes some time to save as a trusted file.</td>
</tr>
<tr>
<td>50283</td>
<td>When Excel is pinned to the taskbar and an untrusted work sheet opened, if it is unpinned and then later re-pinned, a user will no longer see a different list of frequently opened files.</td>
</tr>
<tr>
<td>50483</td>
<td>Office 365 encrypted emails now open correctly, and user is not redirected to the secure browser.</td>
</tr>
<tr>
<td>50559</td>
<td>When remnants of previous Office installs are left in an undefined state on a user’s PC, Word no longer closes and offers a Repair pop-up.</td>
</tr>
<tr>
<td>50605</td>
<td>A user no longer sees &quot;File could not be trusted due to its location&quot; when using a file name with a path of over 255 characters.</td>
</tr>
<tr>
<td>50617</td>
<td>When using Adobe Reader DC19 to read a PDF which requires a user to click through a button to access the main document body, Adobe Reader no longer exits.</td>
</tr>
<tr>
<td>50651</td>
<td>Users using Dell OptiPlex PCS no longer, in a very limited number of cases, see the message “Failed to Start MokSBstarteRT” during the boot process.</td>
</tr>
<tr>
<td>50703</td>
<td>On a very limited number of PCs, with Credential Guard enabled, a user will no longer be stuck in an endless loop of the machine requiring a re-boot.</td>
</tr>
<tr>
<td>50704</td>
<td>Brand new laptops will no longer report Second Boot Power On Failure during initialization.</td>
</tr>
<tr>
<td>50954</td>
<td>Attempting to login to the Controller with the wrong password for an Active Directory user no longer generates an &quot;AD Authentication error attempting to bind&quot; event in certain circumstances.</td>
</tr>
<tr>
<td>51134</td>
<td>When a user uses IE to try to access a web page restricted by ACL of proxy they will no longer see the message &quot;unable to display this page.&quot;</td>
</tr>
<tr>
<td>51414</td>
<td>When links from browsers get intercepted by URL rewriting software used by customers, it no longer forces a redirect to the Secure Browser</td>
</tr>
<tr>
<td>51553</td>
<td>When a user uses a shortcut to a file system which requires authentication they will no longer see a Bromium dialog box asking them if they want to remove protection, which cannot be removed.</td>
</tr>
<tr>
<td>51603</td>
<td>Controller no longer maintains very long-lived TCP connections to syslog servers, for more reliable delivery.</td>
</tr>
<tr>
<td>51822</td>
<td>False Positives will no longer be reported on untrusted Office documents for “maninject32”.</td>
</tr>
<tr>
<td>51832</td>
<td>When a user joins a Webex meeting, the Webex exe installer downloads will no longer be shown as untrusted even though the Webex site is trusted.</td>
</tr>
<tr>
<td>51993</td>
<td>When using Adobe Pro 17 the Fill and Sign option now correctly works on Protected PDFs.</td>
</tr>
<tr>
<td>52063</td>
<td>Users will no longer see a pop-up showing “BrHostHelperBridge.exe stopped working”, which only appeared for a very limited number of users.</td>
</tr>
</tbody>
</table>

Please review earlier release notes for earlier fixes.

Release notes are available from [https://support.bromium.com/s/documentation/](https://support.bromium.com/s/documentation/)
Bromium Secure Platform End of Life (EOL) Dates

Bromium supports an N-2 end of life (EOL) policy for Bromium Secure Platform versions, where N is the current shipping version and N-2 represents the 2 previous GA releases. Versions are classified as follows:

- Major Version [DOT] Minor Version [DOT] Update version. (e.g. 4.1.7)

**Product Support Policy**

- The latest update of the current Major Version of the Product is Supported.
- The latest update of the current Minor Version of the Product (if applicable) is Supported.

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Launch Date</th>
<th>EOS Date</th>
<th>EOL Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bromium Secure Platform v4.1 Update 7</td>
<td>11 Jul 2019</td>
<td></td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 6 Patch 1</td>
<td>10 May 2019</td>
<td>11 Jul 2019</td>
<td>11 Jan 2020</td>
<td>EOS</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 6</td>
<td></td>
<td>4.1 Update 6 Patch 1 immediately supersedes 4.1.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 4</td>
<td>13 Nov 2018</td>
<td>11 Dec 2018</td>
<td>11 Jun 2019</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 3</td>
<td>4 Oct 2018</td>
<td>13 Nov 2018</td>
<td>13 May 2019</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 2</td>
<td>30 Aug 2018</td>
<td>4 Oct 2018</td>
<td>04 Apr 2019</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 1</td>
<td>02 Aug 2018</td>
<td>30 Aug 2018</td>
<td>28 Feb 2019</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1</td>
<td>29 Jun 2018</td>
<td>02 Aug 2018</td>
<td>02 Feb 2019</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 8</td>
<td>12 Jul 2018</td>
<td></td>
<td></td>
<td>Current - Legacy</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 7</td>
<td>08 May 2018</td>
<td>12 Jul 2018</td>
<td>12 Jan 2019</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 6</td>
<td>04 Apr 2018</td>
<td>08 May 2018</td>
<td>08 Nov 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 5</td>
<td>02 Mar 2018</td>
<td>04 Apr 2018</td>
<td>02 Oct 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 4</td>
<td>09 Jan 2018</td>
<td>02 Mar 2018</td>
<td>02 Sep 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 3</td>
<td>21 Nov 2017</td>
<td>09 Jan 2018</td>
<td>09 Jul 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 2</td>
<td>30 Aug 2017</td>
<td>21 Nov 2017</td>
<td>21 May 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 1</td>
<td>23 Jul 2017</td>
<td>30 Aug 2017</td>
<td>02 Mar 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>All vSentry releases earlier than v4.0</td>
<td></td>
<td></td>
<td></td>
<td>EOL</td>
</tr>
</tbody>
</table>


**Getting Help**

If you have questions that are not covered in the documentation, please contact Bromium:

- Visit [https://support.bromium.com](https://support.bromium.com). If you need an account, please contact your Account Executive or Customer Support.
- Email questions to support@bromium.com
- Call Bromium Customer Support at 1-800-518-0845
- Call your technical account representative directly