Bromium Secure Platform

4.1.8 Patch 3 Release Notes
Contents

Notices ........................................................................................................................................4
Introduction ..................................................................................................................................5
Bromium Platform Requirements .................................................................................................5
  Required Software for Isolation .................................................................................................6
  Additional Isolation Requirements .............................................................................................6
  Supported Software ....................................................................................................................7
  Supported Languages ................................................................................................................8
Controller Requirements .............................................................................................................10
  Bromium Controller Requirements ..........................................................................................10
    Supported Browsers .................................................................................................................10
SQL Database Requirements ......................................................................................................10
What's New in 4.1.8 .......................................................................................................................11
Bromium acquisition by HP ..........................................................................................................11
End of Sale (EOS) / End of Life (EOL) Updates .............................................................................11
Platform Updates ..........................................................................................................................12
  Isolation Support for Google Chrome version 76 .................................................................12
  Microsoft Windows Operating System Support .................................................................12
  Initial installation ......................................................................................................................12
  Performance Improvements ......................................................................................................12
  Bromium Secure Browser Extension (SBX) for Microsoft Edge .............................................13
Controller Updates ......................................................................................................................14
  HP Branding ..............................................................................................................................14
  Forward individual threats to HP for triaging .........................................................................14
  Group devices by registry key ...................................................................................................15
  Fall back to using BrChromium / Bromium Secure Browser when Adobe Acrobat isn't available ..............................................................................................................................16
  Auto-trust attachments from internal devices that cannot run Bromium .................................17
  Default Policy Changes .............................................................................................................17
  New syslog event type for classification as True Positive .......................................................17
  Controller version numbers .......................................................................................................17
Limitations ....................................................................................................................................18
  General .......................................................................................................................................18
  Web Browsing with Internet Explorer ......................................................................................19
  Web Browsing with Chrome .......................................................................................................19
  Web Browsing with Firefox .........................................................................................................19
  Documents ..................................................................................................................................20
  Controller ..................................................................................................................................20
Issues Fixed in 4.1.8 Patch 3 ..........................................................................................................21
  Issue ID ......................................................................................................................................21
  Description .................................................................................................................................21
Issues Fixed in 4.1.8 Patch 2 ..........................................................................................................21
  Issue ID ......................................................................................................................................21
  Description .................................................................................................................................21
Issues Fixed in 4.1.8 Patch 1 ..........................................................................................................21
  Issue ID ......................................................................................................................................21
  Description .................................................................................................................................21
Issues Fixed in 4.1.8 .......................................................................................................................22
  Issue ID ......................................................................................................................................22
  Description .................................................................................................................................22
Bromium Secure Platform End of Life (EOL) Dates ....................................................................23
Bromium Secure Platform Deprecated Features .........................................................................23
Getting Help ..................................................................................................................................23

Bromium Secure Platform Release Notes
Notices

Copyright © 2020 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 4.1.8
Patch 1

July 6, 2020
Introduction

The Release Notes cover the Bromium 4.1 Update 8 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><strong>CPU</strong></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 are the Ryzen range of CPUs, and models that are 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>
</tbody>
</table>
| **Memory**           | Minimum: 4 GB RAM  
Recommended: 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 10 64-bit with 1800 MB available memory prior to installation |
| **Disk**             | 6 GB free disk space |
| **Operating System** | 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 11
  - Beginning January 12, 2016, only the most current version of Internet Explorer available for a supported operating system receives technical support and security updates from Microsoft (see https://support.microsoft.com/en-gb/help/17454/lifecycle-faq-internet-explorer)
  - As such, versions of Internet Explorer earlier than 11 are no longer supported on Desktop Operating Systems with Bromium Secure Platform 4.1.8 and later.

  **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 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 version of the Microsoft Edge Legacy 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
- Microsoft Office 2010, MSI x64/x86:
  - Standard, ProPlus
- Microsoft Office 2013, MSI x64/x86:
  - Standard, ProPlus
- Microsoft Office 2013, Click-to-Run x64/x86:
- Microsoft Office 2016, MSI, x64/x86:
  - Standard, ProPlus
- Microsoft Office 2016, Click-to-Run, x64/x86:
- Microsoft Office 2019, Click-to-Run, x64/x86: (Office 365 / Microsoft 365)

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 Flash (all versions)
- Windows Media Player 12 (32-bit and 64-bit)
- Microsoft Silverlight 5.1
- Oracle Java 8 (32-bit)
• Oracle 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 VirtualBox is not supported. Bromium Secure Platform can run alongside Oracle VirtualBox on the host computer from 4.1.6 and later, but only on Intel CPUs and only if Microsoft Hyper-V is disabled.

• 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.

• SINA WorkStation S 3.3 by Secunet Security Networks
  - Solution verified on SINA Workstation S 3.3.9.1

• 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.
- 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. In 4.1.8 Patch 1, the Controller version released is 4.1.9.634

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>Sandy Bridge 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, Edge Chromium, 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 2012 SP4+  
                       | SQL Server 2014 SP3+  
                       | SQL Server 2016 SP2+  
                       | 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 4.1.8
Bromium acquisition by HP

After the acquisition of Bromium by HP in Q4 2019, the Bromium Secure Platform will cease to exist after the 4.1 Update 8 release cycle is complete. During 2020, Bromium Secure Platform will be replaced by HP Sure Click Enterprise.

Bromium will continue to release App Packs and patches to Bromium Secure Platform during 2020 to support customers running 4.1 Update 8. The 4.1.8 cycle will EOL on November 8th 2020. Please contact your Bromium account team or Bromium Support for the latest news on migration and upgrading to the HP Sure Click Enterprise platform when released around mid 2020.

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 4.1.8 release are show below:

- HP Sure Click Enterprise
  - During 2020, HP will release Sure Click Enterprise 4.2.x which will replace Bromium Secure Platform 4.1.x

- Bromium Secure Platform 4.1 Update 8
  - During 2020, Bromium will support new Windows 10 and existing supported application versions by issuing App Packs and Patch releases to 4.1.8 as patches.
    - EOS: 08 Nov 2020
    - EOL: 08 Nov 2020

- Bromium Secure Platform 4.1 Update 7 (EOS)
  - EOS: 08 Nov 2019
  - EOL: 08 May 2020

- 4.0.8 is now EOS
  - EOS: 08 Nov 2019
  - EOL: 08 May 2020
  - This update to 4.1.8 means ALL versions prior to 4.1 Update 8 are now either EOS or EOL, please refer to the EOL policy link above for full details.

- All vSentry 3.x
  - EOL: 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 79

Bromium isolation now supports Google Chrome version 79 when using the full Bromium Secure Browser.

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 the 4.1.8 Release:

- No longer supported:
  - Windows 7 (x86 & x64)
  - Windows 8.1 (x86 & x64)
  - Windows 10 (Threshold 2) Version 1511 (OS build 10586)
  - Windows 10 (RedStone 2) Version 1703 (OS build 15063)

- New support added:
  - Windows 10 (20H1) Version 2004

Support was added for Windows 10 (19H2) Version 1909 (OS Build 18363) in the 4.1.8 release.

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.

Performance Improvements

Bromium Secure Platform 4.1 Update 8 additionally includes some performance and efficiency improvements to reduce the impact on the base system as well as providing an improved user experience.

- Improved user responsiveness when switching between multiple untrusted applications.
- Reduced user disruption when loading all types of untrusted applications into uVMs.
- Faster loading of all types of untrusted applications when introspection is enabled on some machines.
- Reduced impact on host processes when accessing 1000s of directories.
- Ensure audio from a uVM is automatically resumed after being paused due to low memory conditions.
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 have stopped all development on their own Edge architecture and have based the new Edge (released in early 2020) on the Google Chromium framework. This new Edge was introduced in the first quarter of 2020.

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 has moved development from supporting the Bromium Secure Browsing Extension from the old Edge architecture to the new Chromium based Edge. The current SBX release that supports Old 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. Bromium is working towards supporting the new Edge architecture and will provide early access releases of the SBX extension as soon as it is available.

You can read more about edge support on the Bromium knowledgebase here:
https://support.bromium.com/s/article/Bromium-Secure-Browser-Extension-SBX-for-Microsoft-Edge
Controller Updates

HP Branding
Since acquisition by HP Inc., the Bromium Controller has been rebranded to become the HP Sure Controller, as part of the HP Sure family of security features. This branding only affects the controller in the 4.1.8 Patch 1 release and does not affect the endpoint release in any way. All screens of the controller user interface use an updated color scheme, fonts and iconography to fit in with the new branding. All features and functionality remain unchanged both in function and location.

Forward individual threats to HP for triaging
If you have disabled the Threat Forwarding feature in the Controller, threats will not automatically be triaged for you by the HP Cloud Service and security team. As such, you will need to annotate and triage the threat events yourself. This can be challenging so a new feature has been developed to allow a customer to send one or many threat events to the HP Cloud Service as a one off, in order to get the threat intelligence augmented from our array of sources and triaged automatically, without having to opt-in to the Threat Forwarding feature, which forwards all threats to the service.

In order to use this:
1) Select a threat from the threats page using the checkbox, and select Options->Apply Action
2) Select “Forward to HP”, and then decide whether you want to send the entire malware manifest with the threat. While it is not compulsory to send the malware manifest information, it does provide valuable threat intelligence for the cloud service to identify the threat and provide you with the latest information, MITRE ATT&CK details and annotations where applicable.

3) Once selected, the threat will be forwarded to the HP Cloud Service. It will take a few minutes for the service to analyze the threat so check back on the threat report for the threats you sent regularly.

**Group devices by registry key**

While the controller provides a multitude of ways to group devices (name, user, ip etc) none of them can be controlled outside of the software environment, ie SCCM. Now you can use the addition and definition of a registry key to group devices into device groups based on something that has been set at imaging time for example. This can also be set at installation time using the “UNITCODE=<string value>” as part of the MSI installer parameters specified either on the command line or via SCCM for example.

1) A new registry string value called “Installer.UnitCode” should be added to “HKLM\Software\Bromium\vSentry\State” with a text string to be used for grouping.

   ![Edit String](image)

   Alternatively, the installer can be used to specify the string value as an argument to the MSI, “UNITCODE=<string value>”.
2) Now you can create a new group with an automatic grouping rule, specifying the string used in the registry

Add Group

![Group Information Form]

3) The device will be automatically added to the group on the next connection to the controller. The unitcode reference will also appear on the top of the device information page.

**Fall back to using BrChromium / Bromium Secure Browser when Adobe Acrobat isn’t available**

When an endpoint either does not have Adobe Acrobat Reader installed, or there was a problem putting the reader into the uVM template, the Bromium Secure Browser, or Isolated Chromium will be used to open an untrusted PDF file. This means customers no longer have to have Acrobat Reader installed to read untrusted PDF files if they do not want to. Trusted PDFs will be opened on the host as normal.

If neither Adobe Acrobat Reader, or Chrome is available in a uVM due to configuration or errors, the user will be presented with the “Remove Protection” workflow to open in a trusted application if allowed by configuration.

This fallback mechanism is ON by default but can be changed by setting the following advanced parameter:

*Untrusted.UseSecureBrowserAsFallbackPdfViewer = 0*
Auto-trust attachments from internal devices that cannot run Bromium

When a customer is 100% deployed on Bromium Secure Platform, it makes sense to configure outlook attachments to trusted only when the sender domain is trusted and the endpoint sending the attachment was also running Bromium.

This works very well when every endpoint sending email runs the Bromium software and hence sets the email headers correctly for example. However, this new feature allows endpoints NOT running the Bromium software, but still sending email from a local trusted email domain to have their attachments trusted when the above configuration is set.

The reason for this is to allow automated scanners that email the finished scan to a user to send the attachment as a trusted attachment rather than untrusted. This provides the user with a simplified workflow as the document was created within the same area of trust and hence protection does not need to be removed.

To utilize this feature you should add an advanced parameter to the Controller called "Untrusted.AlwaysTrustedSMTPDomains". This advanced parameter is a list type and should contain a list of the sender (from) addresses of the scanner device that the attachments should be trusted from. For example, this list should contain addresses like scanner4@mydomain.com etc.

Default Policy Changes

Bromium Secure Platform 4.1.8 Patch 1 includes some 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.

• Added to the “Ingress Applications” list (Untrusted.IngressApplications)
  o Skype App
  o Windows Mail App
  o Slack
• Added to “File types requiring elevation of privilege to trust”
  o .mht
• Set “Isolate trusted sites when not on the corporate network”
  o Enabled and turned OFF. This stops inheriting the setting from the endpoint and sets it to OFF.

New syslog event type for classification as True Positive

In 4.1.7, Bromium introduced a new syslog event type for True Positive alerts. This message has now been augmented in 4.1.8 with the addition of the HASH of the file where the threat originated.

Controller version numbers

The version number of the Controller may not directly match the version number of the endpoint software, as it used to. Bromium & HP now offer a cloud controller hosted service to our customers. As such, the controller is deployed as a SaaS offering, incrementing versions often and differing from the endpoint software version. This is normal and should not cause concern. As such, the version number of the controller has also moved from the bottom of the web pages, to the “Controller Status” dashboard, which can be found under the Dashboards controller menu item. If you have multiple nodes here, click on the nodes to display the details, including the version number.
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/ 2016 / O365
- 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
- Temporary trust operation will not trust sites that use “guce-advertising.com” redirect capabilities. The redirects used by this advertising network break lots of web and software workflows. Bromium is working to resolve this, but it is a workflow introduced by Verizon Media on most of their web properties. (See https://www.verizonmedia.com/policies/ie/en/verizonmedia/privacy/topics/adserving/index.html)
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` was deprecated in version 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:
  - 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.
  - Close Firefox and restart Bromium isolation.
  - 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 4.1.8 Patch 3

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>58937</td>
<td>Guest WMI error could cause init failure “LAST_BOOT_PIC_START_FAILURE”</td>
</tr>
<tr>
<td>55752</td>
<td>“OleGetClipboard” hook can break Office automation</td>
</tr>
<tr>
<td>57851</td>
<td>Printing comments in an untrusted PDF file, could result in a uVM quitting un-expectedly</td>
</tr>
<tr>
<td>60403</td>
<td>Secure Browsing Extension could incorrectly re-write a URL which some applications can’t parse</td>
</tr>
<tr>
<td>59385</td>
<td>Add support for Windows 10 20H1</td>
</tr>
<tr>
<td>60455</td>
<td>Add support for Microsoft 365 (Office rebranding)</td>
</tr>
</tbody>
</table>

### Issues Fixed in 4.1.8 Patch 2

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>59491 / 59493</td>
<td>Fixed an issue where a Microsoft KB can cause a “Failure to initialize error 88” on some endpoints.</td>
</tr>
</tbody>
</table>

### Issues Fixed in 4.1.8 Patch 1

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54866</td>
<td>Fixed an issue where Adobe Reader 2019 wasn’t correctly viewing in full-screen mode</td>
</tr>
<tr>
<td>55411</td>
<td>Fixed a race condition which causes explorer to restart when untrusted and trusted files are selected to trust in the same operation.</td>
</tr>
<tr>
<td>56179</td>
<td>Resolved an issue where Chrome might fail to start due to a race condition regarding the redirection.</td>
</tr>
<tr>
<td>56844</td>
<td>Issue resolved where a user might have seen “cannot access Bromium Isolation” while using the Secure Browser</td>
</tr>
<tr>
<td>57210</td>
<td>Reported issue resolved, where in some situations, a user might not have been able to open an untrusted PDF.</td>
</tr>
</tbody>
</table>
## Issues Fixed in 4.1.8

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>51324</td>
<td>Added the ability to upload threats to the Bromium Cloud Service individually, even when the Threat Forwarding feature is not enabled</td>
</tr>
<tr>
<td>43482</td>
<td>Allow automatic grouping using a registry key (see above in release notes)</td>
</tr>
<tr>
<td>50526 / 52955</td>
<td>Automatic fallback to Bromium Secure Browser for untrusted PDF files &amp; attachments</td>
</tr>
<tr>
<td>44886</td>
<td>Added support for email addresses for trusted attachments from devices such as network scanners that email scans to users.</td>
</tr>
<tr>
<td>51604</td>
<td>Added blocking support for .MHT files</td>
</tr>
<tr>
<td>52176</td>
<td>“Isolate Trusted Sites” is now OFF by default in the Recommended Settings policy</td>
</tr>
<tr>
<td>53830</td>
<td>When a True Positive threat is sent via syslog, the message now contains the hash of the file.</td>
</tr>
<tr>
<td>50952</td>
<td>Fixed an issue which changed the default behavior when an MS Word file was marked as “Final”</td>
</tr>
<tr>
<td>52061</td>
<td>Bromium Secure View version of Adobe Acrobat starts with the tool pane closed, regardless as to a previous configuration.</td>
</tr>
<tr>
<td>52535</td>
<td>Trusted HTML files with long path names were being opened untrusted.</td>
</tr>
<tr>
<td>52108</td>
<td>Sometimes, the trust file by certificate signature didn’t auto trust some files.</td>
</tr>
<tr>
<td>53651</td>
<td>Some DOCX files were being incorrectly detected</td>
</tr>
<tr>
<td>53624</td>
<td>Some users would see a timeout error when a threat had been detected in a uVM but the user was attempting to remove protection.</td>
</tr>
<tr>
<td>53532</td>
<td>Added support for Bitbox 5.3.0</td>
</tr>
<tr>
<td>53703</td>
<td>Capped the audio recording workflow in an untrusted PowerPoint file.</td>
</tr>
<tr>
<td>49639</td>
<td>Only show Controller drive status for drives in use by the Bromium Controller software</td>
</tr>
<tr>
<td>54432</td>
<td>Add better and more performant support for development environments using compilers.</td>
</tr>
<tr>
<td>54200</td>
<td>Fixed a situation where some Japanese dates are not shown correctly.</td>
</tr>
<tr>
<td>54363</td>
<td>Standby uVMs now load updated BRF rules updates when available.</td>
</tr>
<tr>
<td>54901</td>
<td>Added support for MS Office Home and Business 2019 SKU for untrusted documents.</td>
</tr>
<tr>
<td>52237</td>
<td>Fixed a situation where a Chrome System Error could occur</td>
</tr>
<tr>
<td>55554</td>
<td>Add User workflow now contains the Active Directory user flow</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 Secure Platform 4.1.8 Patch 1 is supported with an N-1 end of life (EOL) policy for Bromium Secure Platform versions, where N is the current shipping version and N-1 represents the previous GA release. Previous GA releases are marked as EOS when a newer release is marked Generally Available (GA).

Versions are classified as follows:

- Major Version [DOT] Minor Version [DOT] Update version. (e.g. 4.1.8)

**Product Support Policy**

- The latest update of the current Major Version of the Product is Supported.

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Release Date</th>
<th>EOS Date</th>
<th>EOL Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bromium Secure Platform v4.1 Update 8 Patch 3</td>
<td>2 Jun 2020</td>
<td>08 Nov 2020</td>
<td>31 Mar 21</td>
<td>Current</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 8</td>
<td>4.1 Update 8 Patch 3 immediately supersedes all 4.1.8 versions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 7</td>
<td>11 Jul 2019</td>
<td>08 Nov 2019</td>
<td>08 May 2020</td>
<td>EOL</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>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 6</td>
<td>4.1 Update 6 Patch 1 immediately supersedes all 4.1.6 versions</td>
<td></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>All vSentry releases earlier than v4.1</td>
<td></td>
<td></td>
<td></td>
<td>EOL</td>
</tr>
</tbody>
</table>


**Bromium Secure Platform Deprecated Features**

Bromium is deprecating older platforms and features from the latest versions of the Bromium Secure Platform, and HP Sure Click. Customers should read the KB article that explains the platforms and features being deprecated and the timeframes/versions in scope.

Specific examples of deprecated platforms are Windows 7 and all x86 platforms.

The latest information regarding deprecated features and platforms: [https://support.bromium.com/s/article/Deprecated-Features](https://support.bromium.com/s/article/Deprecated-Features)

**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