Bromium Secure Platform

4.1.5 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 .................................................................................................................... 9
  Bromium Controller Requirements .................................................................................................. 9
  Supported Browsers .......................................................................................................................... 9
SQL Database Requirements ............................................................................................................... 9
Important Information Regarding the Intel CPU Vulnerability .......................................................... 9
What's New in 4.1.5? ............................................................................................................................. 9
  End of Support (EOS) / End of Life (EOL) Updates ......................................................................... 10
  New Isolation Support........................................................................................................................ 10
    Isolation Support for Google Chrome version 68 (4.1.5) ............................................................... 10
    Firefox Secure Browsing Extension (4.1.5) ..................................................................................... 10
    Improved ZIP Workflows (4.1.5) ................................................................................................. 10
Platform Enhancements ...................................................................................................................... 12
  Automatic Threat Forwarding to Bromium Cloud Services (4.1.5) ................................................. 12
  Threat Names Displayed on Threat Dashboard (4.1.5) ................................................................. 12
  Verbos Reporting for High Severity Events (4.1.5) ......................................................................... 13
  Threat Revision History and Notes (4.1.5) ...................................................................................... 13
  Forward to TAXII for Threat Actions (4.1.5) ................................................................................ 13
  Administrative Audit Trail for Disabling Isolation (4.1.5) .............................................................. 14
  Endpoints Revert to Original Factory Settings when Locally Managed (4.1.5) ............................. 14
  Reboot Reminder for Endpoint Upgrades (4.1.5) ........................................................................... 14
  Improved Adobe Reader User Experience (4.1.5) .......................................................................... 14
  Bromium License Expiration Details (4.1.5) ................................................................................... 14
  Bromium Controller Health Monitoring (4.1.5) ............................................................................. 14
  Not Installed Software Filter (4.1.5) ............................................................................................... 15
  Reboot as a Remote Management Command (4.1.5) ................................................................. 16
  New Threat Dashboard with Filters (4.1.5) .................................................................................... 16
  Threats from Deleted Devices Persist on Controller (4.1.5) ......................................................... 17
New Management Actions .................................................................................................................. 17
  License Expiration Advance Notification (4.1.5) ......................................................................... 17
Beta Features ..................................................................................................................................... 18
  Microsoft Edge Secure Browsing Extension (4.1.5) .................................................................... 18
What’s New in 4.1 GA – 4.1.4? .............................................................................................................. 19
  New Isolation Support ..................................................................................................................... 19
    Isolation Support for Microsoft Office 2019 (4.1.4) .................................................................. 19
    Isolation Support for Adobe Reader DC 2019 (4.1.4) ............................................................... 19
    Isolation Support for LNK files (4.1.4) ....................................................................................... 19
    Isolation Support for SLK files (4.1.4) ....................................................................................... 19
Controller Updates .............................................................................................................................. 19
  Bromium Cloud Services (4.1.4) ................................................................................................. 19
  Remote Updates of Bromium Rules Files (4.1.4) ......................................................................... 19
  Cloud Severity Results for File Hashes on Receipt of Threat (4.1.4) ............................................ 20
  Label Threats with Malware Classifications from Threat Intelligence (4.1.4) ......................... 20
  Automatically Classify True Positive Threats from Threat Intelligence (4.1.4) ......................... 20
  Save Default Filters on Data Tables (4.1.4) ................................................................................. 21
Notices

Copyright © 2018 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.

Bromium Secure Platform 4.1.5

December 11, 2018
Introduction

The release notes cover the Bromium 4.1 product release, 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.</td>
</tr>
<tr>
<td>Memory</td>
<td>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 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. Microsoft Windows 10 versions are supported as follows: • Anniversary Update, 64-bit (Professional, Enterprise) on Bromium Secure Platform 3.2 GA Update 8 and later • Fall Creators Update, 64-bit (Professional, Enterprise) on Bromium Secure Platform 4.0 Update 3 and later • April 2018 Update, 64-bit (Professional, Enterprise) on Bromium Secure Platform 4.0 Update 7 and later • October 2018 Update, 64-bit (Professional, Enterprise) on Bromium Secure Platform 4.1 Update 4 and later For information about security features and hardware recommendations for Windows 10 releases, refer to the Microsoft site: <a href="http://www.microsoft.com">http://www.microsoft.com</a> If you are running monitoring only (that is, without isolation), Windows Server 2008 and Windows Server 2012 are also supported.</td>
</tr>
</tbody>
</table>

Note: Refer to your system manufacturer’s documentation for details about enabling virtualization on Intel and AMD processors.
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, or you can use the included 21-day evaluation license
- To run isolation in a virtualized environment using:
  - Citrix Hypervisor 7.3
  - VMware, ESX 5.5 Update 2 or later. ESX 6.5 is recommended
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 Chrome Isolation supports the current and previous 4 versions of Chrome at the time of GA. Chrome support is detailed in the Bromium Support Knowledge base. Bromium 4.1.5 includes support for Chrome 68.
- Bromium Secure Browsing Extension for Firefox (Firefox SBX) supports the latest Mozilla-recommended version of Firefox (ESR or non-ESR, 64-bit only)
- Bromium Firefox Isolation supports Mozilla Firefox ESR 52 (32-bit) and Firefox ESR 60 (32-bit)
- 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 x64:
  - Standard, ProPlus
- Microsoft Office 2016, Click-to-Run, x64 and x64:
- Microsoft Office 2019, Click-to-Run, x64 and x64:

**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.

- Microsoft Outlook 2010, 2013, 2016 and 2019
- Adobe Reader versions 9, 10, 11, DC Classic 2015, DC Classic 2017, DC Continuous 2015, DC Continuous 2017, DC Continuous 2018, and DC Continuous 2019
- Adobe Acrobat Professional version 10 and 11, 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 4, 5, and 5.1
- Oracle Java 6, 7, and 8 (32-bit)
- Autonomy (FileSite or DeskSite) version 9
- Oracle VM VirtualBox on:
  - Windows 7 32 and 64-bit
  - Windows 8.1 and later 64-bit version with Intel

**Note:** VirtualBox is not supported on endpoints running AMD processors

- 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:

1. No support for Windows 10 machines running HVCI (HyperVisor Code Integrity)
2. 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 7.16 with Citrix Hypervisor 7.3)

Windows Defender Credential Guard

- McAfee DLP for Internet Explorer
- Symantec DLP
- McAfee Endpoint version 9.3 and later

Isolation has been tested with the following third-party endpoint security product solutions:

- Microsoft Security Essentials 4.0
- Symantec Endpoint Protection 11.0.6, 11.0.7, and 12
- McAfee Endpoint Protection or Total Protection 8.7 and 8.8
- Trend Micro OfficeScan 10.6
- Bit9 Parity

Other AV solutions are not yet certified for compatibility with isolation. 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.

**Supported Languages**

Isolation supports user interfaces in 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:** Isolation supports all Windows locales.

Please ensure that Bromium isolation is upgraded to the correct compatible version prior to updating to a new version of Windows.
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>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 management application</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>
<tr>
<td>Software</td>
<td>SQL Server 2008 R2 Service Pack 1 64-bit, SQL Server 2012 (all service packs), SQL Server 2014, SQL Server 2016 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 environment only)</td>
</tr>
<tr>
<td>StorageSpace</td>
<td>1 TB available space</td>
</tr>
</tbody>
</table>

Note: If you are using msiexec to install Bromium remotely, ensure you include the SERVERURL setting, otherwise installation will fail.

### Important Information Regarding the Intel CPU Vulnerability

Microsoft security updates for Windows versions 7, 8.1, and 10 intended to fix hardware-based security vulnerabilities resulted in an incompatibility with Bromium isolation and impacts the creation of VMs. While Bromium Secure Platform is not affected directly by the CPU design flaw, the Microsoft updates affect Bromium software. For more information about this issue, see the [https://support.bromium.com/s/article/Intel-CPU-design-flaw](https://support.bromium.com/s/article/Intel-CPU-design-flaw) article on the Bromium Support site.
What's New in 4.1.5?

End of Support (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 support and maintenance for a specific version of the Product. EOS means that product is Supported but expect to be able to try to replicate any reported issue on the currently Supported version of the software in your production environment.

- **Bromium Isolation 4.1 Update 4 (EOS)**
  - EOS: 6 December 2018
  - EOL: 6 June 2019

- **Bromium Secure Platform v4.0 Update 7 (EOL soon)**
  - EOS: 12 July 2018
  - EOL: 12 January 2019

- **Bromium Secure Platform v4.0 Update 6 (EOL)**
  - EOL: 8 November 2018

- **vSentry 3.2 Update 8 (EOL soon)**
  - EOS: 29 June 2018
  - EOL: 29 December 2018
  - Note: This marks EOL of the 3.2 major version

New Isolation Support

This release adds isolation support for multiple new applications.

**Isolation Support for Google Chrome version 68 (4.1.5)**

Bromium isolation now supports Google Chrome version 68 when using the full Bromium Secure Browser.

**Firefox Secure Browsing Extension (4.1.5)**

This release adds support for the Firefox Secure Browsing Extension (Firefox SBX), as an additional option to the Chrome Secure Browsing Extension (Chrome SBX) that debuted in Bromium 4.1, delivering increased flexibility and choice for Secure User-Centric Browsing to users of Firefox 64-bit (ESR or non-ESR).

**Note:** Enabling Firefox SBX support now automatically installs and enables the Firefox Secure Browsing Extension. Previous beta support for Firefox SBX required you to manually enable the extension from the Firefox Add-ons menu.

On the Bromium Controller

- Set the advanced parameter `Browser.SBX.Firefox.Enabled` to “1” on top of the default use case policies.

![Browser.SBX.Firefox.Enabled](image)

The Bromium Secure Browsing icon will be shown in the Firefox menu bar, colored orange to show that it is enabled.

**Improved ZIP Workflows (4.1.5)**

Bromium Secure Platform now provides support for new ZIP file workflows, including the following capabilities:
• View the contents of a zip archive inside Windows Explorer
• Double click to extract and open a file in a micro-VM
• Extract individual files via:
  • Copy and paste
  • Drag and drop (Windows 10 only)
• View the properties of a file as a property sheet
• Extract password-protected files

Known limitations of ZIP workflows:
• Tree View is not supported
• Only the ZIP archive format is supported
• Modifying the untrusted archive is not supported (e.g. cannot add files to the archive)
• Drag and drop functionality is only supported on Windows 10

The advanced parameter is **Untrusted.EnableNativeShellArchiveBehaviour**

• The default value is 1 (disabled)
• Set this value to 2 to enable the new ZIP functionality: Requires user to logout / login again to take effect
Platform Enhancements
This release adds significant new functionality to the Bromium Controller and Bromium Secure Platform endpoints.

Automatic Threat Forwarding to Bromium Cloud Services (4.1.5)
Customers upgrading to Bromium Secure Platform 4.1.5 can now benefit from Automatic Threat Forwarding from their Bromium Controller to the Bromium Threat Cloud for automated triage and categorization by Bromium Cloud Services. Forwarding threat data to Bromium enables:
- Automatic classification of threats based on behavioral analysis using live threat data
- Manual analysis of threats by Bromium Threat Analysts for escalated cases, to help classify true or false positive threats and provide comments on threat provenance

Threat Forwarding is disabled by default, and is configured in your Controller via Settings > Cloud Services > Enable Threat Forwarding

Threat Names Displayed on Threat Dashboard (4.1.5)
Bromium Threat Cloud returns a threat name in a format similar to "Win32.Trojan.CVE-2017-0147" for each threat that it is able to identify. Not all threats will have a specific name. Some threats are identified generically. This information is included in the Threat Alert that is sent from the endpoint to the Bromium Controller and from the Bromium Controller to the Bromium Threat Cloud.

The Threat Dashboard now includes a new column for Top Threat Names received from the Bromium Threat Cloud, with counts for each named threat.
Verbose Reporting for High Severity Events (4.1.5)

For each threat, there is now a “Verbose” tab where a user can view the High Severity Events for a threat in great detail, including the time, process, and specific actions that occurred within the micro-VM (i.e. file write, launch process, network connection, etc.).

Threat Revision History and Notes (4.1.5)

A “Recent Activity” text box is now included on the “Summary” tab for each threat. This includes a time-stamped log of automated actions (i.e. First Received, Updated, Classified True Positive), along with sequential entries of user notes and manual changes of threat status between True Positive and False Positive as additional information is received.

Forward to TAXII for Threat Actions (4.1.5)

There is now a “Forward to TAXII” option for threat actions. Administrators select from the configured TAXII consumers. When deleting a TAXII consumer, a pop-up informs which threat actions are affected (either deleted or will stop forwarding threats to a TAXII consumer). TAXII Consumers are now configured in a dedicated part of the UI, in a sub-menu under ‘Threats’. TAXII consumers can now be configured with a collection too, so that you can use the same TAXII server to receive your threat data.
Administrative Audit Trail for Disabling Isolation (4.1.5)
Administrative users of the Bromium Controller must now enter a comment when disabling Bromium isolation for audit tracking.

Endpoints Revert to Original Factory Settings when Locally Managed (4.1.5)
When an endpoint leaves a Bromium Controller and becomes locally managed, the endpoint configuration now reverts to original factory settings. It no longer saves any settings from its previous Bromium Controller policy.

Reboot Reminder for Endpoint Upgrades (4.1.5)
When customers upgrade their endpoints—whether manually, from SCCM, or directly from the Bromium Controller—a reboot is necessary to benefit from the latest version. A daily reboot reminder is now enabled to alert users to restart their PCs to help ensure that they receive the new functionality promptly. The reminder appears like a Windows notification and does not mention Bromium.

Improved Adobe Reader User Experience (4.1.5)
Adobe Reader 2015 DC and later versions include a Sidebar populated with frequently used tools. This Sidebar is now minimized in untrusted (isolated) PDFs by default, since Bromium users have reported a strong preference for this experience.

Bromium License Expiration Details (4.1.5)
Expiration details for the Bromium Secure Platform are now provided on the Bromium Desktop Console, showing the number of days remaining in the license period.

Bromium Controller Health Monitoring (4.1.5)
The Controller Status view now provides a summary of the Bromium Controller’s current health monitoring status, including disk space, device capacity, CPU utilization, available memory, and web service requests.
Not Installed Software Filter (4.1.5)

In the Devices table, an Installed Software filter for “Is not installed” is now available, enabling administrators to locate Bromium-managed endpoints that do not have the specified software installed.
Reboot as a Remote Management Command (4.1.5)

The ability to reboot any device managed by the Bromium Controller is now available as Remote Management command.

New Threat Dashboard with Filters (4.1.5)

The following tiles have been removed from the Threat Dashboard: Alerts, Isolated Alerts, Host Alerts, Blacklisted Files, User Trusted Files, User Trusted Websites, Opened Web Pages, Micro VMs Created, Device Alerts. See new Threat Dashboard below.
Filters are now available on the Threat Dashboard.

Threats from Deleted Devices Persist on Controller (4.1.5)

Threats are now associated with an installation rather than a device, so threats remain available on the Bromium Controller even if a device is deleted.

New Management Actions

Bromium Secure Platform 4.1.5 includes management updates that impact all upgrading customers.

License Expiration Advance Notification (4.1.5)

A management action is now sent to the Bromium Controller if a license for Bromium Secure Platform will soon expire.
Beta Features

This release includes beta support for additional isolated browsing flexibility.

Microsoft Edge Secure Browsing Extension (4.1.5)

Bromium Secure Platform 4.1.5 includes beta support for Secure User-Centric Browsing using Microsoft Edge. Bromium now supports user or organizational choice of Chrome, Firefox, or Edge for native browsing of safe or trusted websites, with automatically routing of risky or unknown websites to the Bromium Secure Browser using Secure Browsing Extension.
What’s New in 4.1 GA – 4.1.4?

This release provides the following new features that are focused on usability for end users and manageability for administrators.

New Isolation Support
This release adds isolation support for multiple new platforms and file types.

Isolation Support for Microsoft Office 2019 (4.1.4)
Bromium isolation now supports Microsoft Office 2019, including Word, Excel, and PowerPoint. Please see known Limitations.

Isolation Support for Adobe Reader DC 2019 (4.1.4)
Bromium isolation now supports Adobe Reader DC 2019.

Isolation Support for LNK files (4.1.4)
Bromium isolation now supports LNK files. A LNK file is a shortcut or “link” used by Windows as a reference to an original file.

Isolation Support for SLK files (4.1.4)
Bromium isolation now supports SLK files. Symbolic Link (SYLK) is a Microsoft file format typically used to exchange data between applications, specifically spreadsheets.

Controller Updates
This release adds Bromium Controller support for improved threat intelligence, system performance, and manageability.

Bromium Cloud Services (4.1.4)
Bromium Cloud Services enable a wide range of new features including augmented threat intelligence for automated threat triage and labelling, plus automatic rules file updates to ensure accurate detection and protection against the latest attack techniques.

**Important:** This property is global and is enabled by default:
- Communication with Bromium Cloud Services
- Malware presence check based on file hashes
- Automatic updates for Bromium Rules Files

Remote Updates of Bromium Rules Files (4.1.4)
Bromium Controller administrators can now update their Bromium Rules Files (BRF) from the Bromium Cloud Service to improve threat intelligence accuracy using the latest detection rules.
- Rules built using continuous inputs from our vast sensor network
- Increases detection accuracy and reduces false positive alerts
- Improves user experience through accurate threat determination
- Allows security teams to quickly identify and focus on true positive attacks
Cloud Severity Results for File Hashes on Receipt of Threat (4.1.4)

New file threats are no longer marked as "Pending" in the Bromium Controller. Instead, file hashes are now checked upon receipt and Threat Intelligence is immediately populated with a severity based on results from the Bromium Threat Cloud.

Label Threats with Malware Classifications from Threat Intelligence (4.1.4)

The Bromium Controller now displays malware classifications for file hashes on the Threat Summary page whenever the Bromium Threat Cloud returns a classification for a hash it has received.

Automatically Classify True Positive Threats from Threat Intelligence (4.1.4)

The Bromium Controller now labels alerts containing a file hash classified by the Bromium Threat Cloud as True Positive threats.
Save Default Filters on Data Tables (4.1.4)

Bromium Controller users can now create default views from saved filters that persist every time that user logs in or changes views. Everywhere a data table appears with filters to select the data, the option to save the filter is now available, including:

- Threats
- Devices
- Device Groups
- Events
- Users

Resizable Data Table Columns (4.1.4)

Data table columns in the Bromium Controller are now resizable using standard drag-and-drop functionality.

**Note:** Resized data table columns can be saved as part of the default filters.

New Management Actions

Bromium Secure Platform 4.1.4 includes management updates that impact all upgrading customers.

**Notification of Unprotected Default Web Browser (4.1.4)**

A management action is now sent to the Bromium Controller under Devices Requiring Attention, informing the administrator whenever a user has a default browser that is not protected by Bromium. The alert includes a link to a Knowledge Base article.
Notification of Older Rules in Use (4.1.4)

A management action is now sent to the Bromium Controller under Devices Requiring Attention, informing the administrator whenever an endpoint is using a Bromium Rules File (BRF) that is older than the most current version.

Newer rules files are released by Bromium and available in the download portal. Once downloaded, the updated rules file needs to be pushed to the endpoints using the rules pages on the Bromium Controller. Alternatively, customers can connect their controller to the Bromium Cloud Service to automatically receive the latest rules files without having to download and push manually.

Advanced Options for Remotely Installing a Package (4.1.4)

The Bromium Controller now provides advanced options for remotely installing a package onto a Bromium-protected endpoint.

These options allow a Bromium Controller administrator to avoid accidentally repairing or downgrading a current Bromium version.
Advanced Install Package Options include:

- Prevent repair install – Skips installation if the same version is already installed
- Prevent downgrade – Skips installation if a newer version is already installed
- Hide installation – Omits package from Add/Remove Programs list
- Switch Controller – Optionally switches to a different Bromium Controller address on installation (Bromium isolation only)
- Skip checks – Optionally checks names to ignore and install anyway (Bromium isolation only)
- Install disabled – Installs Bromium Secure Platform in a disabled state (Bromium isolation only)
- Retain previous packages – Leaves older Isolation Support packages on the PC (Isolation Support packages only)

Default Policy Changes

Bromium Secure Platform 4.1.4 includes changes to default policy settings that impact all upgrading customers.

Image Protection for Downloads and Attachments (4.1.4)

Images are now protected by default in the Download Protection and Attachment Protection policies.
GIF and TIF File Types No Longer Trusted Automatically (4.1.4)

Due to recent exploits in GIF and TIF files, these file types will now open in the Bromium Secure Image Viewer by default.

- **MimeHandler.Custom0.FileTypes** no longer includes .gif or .tif file types
- **Bromium Controller administrators** can choose to add these file types back manually
Email URL Threat Assessment after Third-Party Encoding (4.1.3)
Bromium threat assessment now takes place after email protection solutions have encoded the original URL. This enhancement now allows links to trusted sites from third parties to remain in the native browser, while links to untrusted sites are routed to the Secure Browser after being evaluated by solutions such as Mimecast, Proofpoint, Cisco IronPort, Microsoft Office 365, and other providers.

Devices Requiring Attention Drill-Downs (4.1.1)
There is now the ability to drill down into Devices Requiring Attention on the Dashboard and access the relevant linked KB article, making the troubleshooting workflow easier for administrators.

Faster Initializations (4.1)
In most instances, Bromium Secure Platform is fully initialized on the end user’s PC in ~5 minutes.
“Trust this file” is now “Remove protection” (4.1)

Previously if privileged users did not want a file to run in a Bromium micro-VM they would right click on the file and select ‘Trust this file’.

With Bromium Secure Platform 4.1 the privileged user will now see ‘Remove protection’ when they right click on the file. Additionally, administrators can set a configuration to request a reason of why protection was removed.

Secure User-Centric Browsing (4.1)

Enjoy greater web productivity and freedom with enhanced user satisfaction, without sacrificing security, using native Chrome on the host for low-risk browsing and the Bromium Secure Browser to isolate high-risk web activities. This new model of operation may better suit some of your users for whom Chrome is the default browser. It allows the use of native Google Chrome with redirection to the Bromium Secure Browser as needed. As a Bromium customer you may already be using the Bromium Secure Browser in place of Google Chrome for full secure defense grade protection. If defense-grade protection is suitable for your environment, then you do not need to change anything.

NOTE: Using any pre-defined use case policy (Downloads, Links, or Attachments) will implement Secure User-Centric Browsing.

The Bromium Secure Browser Chrome extension is designed to be used in conjunction with the Bromium Secure Browser. It provides protection for web browsing when Chrome is set as the default on endpoints. With this extension, when users click on potential phishing links to untrusted sites (for example, in an Outlook email or an untrusted PDF document), the site will open in an isolated Chrome tab running in a micro-VM.

Bromium Secure Browser Chrome extension can be installed via:

1. Default installation using local group policy mechanisms to stop user tampering, as part of normal the Bromium Secure Platform installation. The extension is not enabled until the applicable policy has been configured.
2. Active Directory group policy can be used to deploy Chrome extensions and configuration settings
3. Chrome force-installing using master_preferences, see the Chrome documentation at https://support.google.com/chrome/a/answer/188453?hl=en
4. Users can download the extension directly from the Google Chrome Web Store, accessible only via the direct link below:
   - Go to: https://chrome.google.com/webstore/detail/secure-browsing/fcbnoohifpffojhciofjaefgdpdjhmcf
   - Ensure that Allow access to file URLs is enabled.
NOTE: The extension is not enabled until one or more pre-configured use case policies have been turned on or the extension has otherwise been enabled by custom configuration.

**Using the Bromium Secure Browser (4.1)**

The Bromium Secure Browser window appears differently to native Chrome, as a visual indication to users (background is blue) that they are using a protected version of Chrome.

In native Chrome, a Bromium icon in the toolbar indicates that the Secure Browsing extension is installed and it is also listed in `chrome://extensions`.
The Bromium Secure Browser can be launched from the Windows Start Menu > Bromium Secure Browser or from the context menu (for example, when users right-click on a hyperlink). For more information, refer to the *Bromium Secure Platform Installation and Deployment Guide*. 
Targeted Use Case Deployment (4.1)

Deploy Bromium strategically to protect key attack vectors with pre-packaged use cases that isolate:

- Email Attachments
- Phishing Links
- Malicious Downloads

To simplify configuration and deployment, (4) four new preconfigured, read-only policies are provided to quickly and easily enable endpoint protection that is relevant to your environment and users, without having to configure settings individually. Using these pre-configured policies may simplify your deployment or expansion to new users. They are not editable, so you can continue to use Delta policies to layer on top any environment-specific settings you require.

Bromium recommends that you enable all four of these policies on your endpoints:

NOTE: Using any pre-defined use case policy (Downloads, Links, or Attachments) will implement Secure User-Centric Browsing.

Recommended Protection Settings: use this policy as a base policy on all of your endpoints in conjunction with the other three Bromium policies.

Download Protection: files downloaded and/or opened from websites are opened in a micro-VM. This includes files accessed through malicious web sites and URL redirects.

Link Protection: links contained in emails messages and attachments, shared links in supported chat clients (Skype, Skype for Business, HipChat, and Slack), and any other opened links are opened in an isolated browser tab.

Attachment Protection: email attachments in Outlook and webmail are isolated in a micro-VM. These attachments include executable files, Microsoft Office documents, and (if Adobe Reader or Adobe Acrobat are installed) PDFs.

Additional Policy Updates

- Policy control changes: the toggle now says Off / On, with a new Append checkbox. (4.1)
- It is now possible to add / apply policies to endpoints from the Device Groups page. (4.1)
- Administrators are now prompted for a reason when changing policies, which is also logged in the Policy Revision History on the policy page. (4.1)
- IE 9 is no longer supported for accessing the BEC; however, it is still supported for platform isolation. (4.1)

Single Platform Installer (4.1)

Bromium Secure Platform 4.1 has only one .msi and only one listing in Add/Remove Programs. Monitoring libraries are automatically installed but no longer enabled by default.
Actionable Dashboards and Reporting (4.1)

This release contains separate operational and threat dashboards, along with a summary report, providing up-to-date views and advanced filtering and data management tools.

![Dashboard Image]

Rather than counts, tiles have been introduced at the top of the dashboards to show key data and trends. For example:

![Tile Example]

Designed to be flexible in what they display, tiles are used to:

- Match the context of the dashboard content
- Give a quick overview of significant information that can be used to drill down to corresponding filtered views
- Highlight different levels of information and severity (through the use of red and amber highlights) allowing for a ‘top task’ approach
- Tiles on the Summary Report respond to any filter and date range changes

Tiles, dependent on the datatype are used to display the following content:

- Severity level (Alert, Warning, Default)
- Data type (Title)
- Count
- Trend (Percentage)
- Trend indicator (Sparkline)
- Total label
- Total count or percentage value of total

By default, the Operational Dashboard is opened when you click Dashboard in the left navigation. To change this, expand the menu next to the current user name in the upper left-hand corner of the controller interface. Select Preferences, then select Threat from the Default Dashboard options.

Additional dashboard improvements include:

- TV Mode – the header and navigation can be toggled off and on allowing for a dashboard to be viewed full-screen
- Focus mode – individual dashboard and report components can be viewed in isolated focus mode
Operational Dashboard (4.1)

The Operational Dashboard provides a status summary for the devices in your deployment. For example:

**Remote Commands**

This component displays a summary of the five most recently sent remote commands listed by command, overall status and the total of devices. Click a remote command to get a breakdown of the command and the details and status of any devices. Click View all to open the Remote Commands page.

**Devices Requiring Attention**

(Previously Management Actions.) This component gives a total of all management actions with a breakdown of actions by issue type. Only Product, Configuration and Environmental issues are displayed. Due to their nature, transient issues are not displayed; however, they can be viewed by clicking View all. Click on any of the issue type horizontal bars to open a filtered devices view.

**Licensing Compliance**

This is a new component, designed to be an indicator allowing administrators to easily view licensing compliance. The component displays the status of Bromium licensed devices in your deployment. In the Settings page, enter the number of Bromium licenses you own in the Number of devices licensed field. If the number of active devices exceeds the number of licenses you own, an alert is displayed in the dashboard.

**Isolation and Monitoring Deployment Status**

These components display the number of devices running specific Bromium product versions. Click on any of the bars to open a filtered devices view.
Isolation and Monitoring Health Status

These components provide the following device information for isolation and monitoring:

- **Running** - Registered devices with a fully operational deployment
- **Unknown** - Registered devices with an unknown status. This status may occur if the device has registered with the controller but has not yet sent a status.
- **Running (Re-initializing)** - Devices currently initializing isolation
- **Running (May Need Attention)** - Devices with a fully operational deployment but have a pending action that requires attention
- **Not Running (Maintenance)** - Registered devices that do not have isolation running
- **Disabled** - Registered devices with isolation disabled
- **Error** - Registered devices with errors

Isolation Initialization Status

For isolation, this component indicates the state of isolation initialization on devices and provides the following information:

- **Initialized** - Isolation is initialized
- **Initializing** - Isolation is currently initializing on the device
- **Unknown** - The information is not available
- **Blocked** - The initialization process is unable to continue

Isolation Security Status

This component indicates the state of isolation on devices and provides security status information:

- **Protected** - Isolation is initialized and enabled
- **Not Protected** - This status may occur, for example, when isolation is initializing or when a license is not applied
- **Unknown** - The information is not available
- **Disabled** - Isolation has been disabled on the device
- **No User Logged In** - No user is currently logged in to the device

Click on any of the bars to open a view of filtered devices.
Threat Dashboard (4.1)

The Threat Dashboard highlights key threat data and trends. For example:

**Alerts**
Displays a line graph of isolated and host alerts to date. Additionally, there are counts of the total of Micro-VMs created, and totals of isolated and host alerts.

**Recent Alerts**
This section lists the applications affected by the most recent isolated and/or host alerts. Click a threat to open it in the Threat Summary Details page.

**Process Risk**
For monitoring threats, this graph details the applications monitored and the number of threats detected for each application.

**Key Attack Vectors**
This component allows you to quickly view the most prevalent attack vectors by indicating the number of each. Click a vector to go to the Threats page and view results filtered by the threat type.

**Web Based File Based Attacks**
These sections list the top five web and file-based attack names and the number of occurrences for each. Click a threat to view filtered details on the Threats page.

**Device and User Alerts**
This section lists the top five devices and users with alerts. Click a device to view more details and any other threats associated with this device on the Threats page.
Summary Report (4.1)

The Summary Report dashboard provides the flexibility to create summary reports based on device filters and date ranges. It shows an overview of your deployment, including graphs and statistics about devices and threats. You can create customized reports for product versions, registrations, devices with management actions, threat totals, and overall operational statuses. For example:

To select which device information is displayed in the Summary Report:

1. Click Add Filter and select one of the following filters to display devices by:
   - Archive Status: either Active or Archived devices
   - Groups: one or more device groups
   - Isolation Version: the version of Bromium isolation running on the device
   - Licensed: either licensed or unlicensed devices

2. Click Report Range to display device information for specific dates. Select dates from the calendar or select one of the defined ranges (Today, Last 7 Days, Last 30 Days, or Last 90 Days.) Click Apply.

Creating Reports

Configured summary reports can be saved to PDF using the print to PDF option in the browser. To print a report using the Print option in, for example, internet Explorer, ensure you also print background colors and images. To do this:

1. Right-click on the Executive Summary dashboard.
2. Select Print preview...
3. Click Page Setup (the cog icon) and check the Print Background Colors and Images option.
4. Click OK then click the printer icon.

This release contains separate threat, operational, and a summary report, providing updated views, and improved filtering and data management tools.
Proactive Email Attachment Scanning (4.1)

Apply pre-emptive email security and threat intelligence sharing with full kill-chain reporting via pre-click email attachment analysis, applied earlier in the attack cycle, before the user can open or save malicious threats.

Emails arriving in a user’s inbox are now automatically queued for background scanning, resulting in security checking of file attachments often before the email is opened. The scanning, transparent to the user, takes place on a scrambled copy of the attachment so that it does not affect the opening of the attachment by the user. Scanning can be configured to either compare the file hash against a known list of malware and/or open the file in a VM to analyze its potential actions. If any threats are found, they are reported to the Controller.

PDF Supported Features
- Adobe Reader 2017 Classic (4.1)
- Digital signatures in Acrobat Pro and Reader (4.1)
- Users can digitally sign PDF documents using their SmartCard (PIV/CAC) credentials (4.1)
- Combining pages of trusted and untrusted PDF documents in Acrobat (4.1)

Additional IE Features
- Downloads in IE can be marked as trusted or untrusted based on domain, using Browser.IE.EnableTrustedDownloadSites, on by default (4.1)
- Untrusted IE downloads can now be forced to automatically go to a specific folder on the host (4.1)

Miscellaneous Features
- Files can now be automatically trusted based on a digital signature signer’s name or on the hash of the file itself (4.1)
  - Example: Online meeting software issues frequent updates but the signer doesn’t change and you want to always trust it
- When untrusted files are zipped, the zip archive is now shown as untrusted (4.1)
- Alerts based on signature checks are now generated when a file downloaded, not just when it is accessed (4.1)
- Microsoft Edge will now auto-trust downloads from the Trusted Download Sites list when Edge is listed an ingress application (4.1.1)
- Fixed an issue some customers were seeing where Chrome bookmarks, history and profile information was being lost due to a clean-up process. This process has been disabled. (4.1.1)
Limitations

General

- Excel 2019 files shared using ‘Send as PDF’ file sends the email with a text file attachment instead of a PDF.
- If host monitoring is enabled on a PC running Windows 10 Redstone 5 with user mode hooking for host monitoring enabled, the Platform will raise a management action saying that hooks on Redstone 5 are not currently supported.
- 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.
- The installation interface is not localized for other languages; the interface is displayed in English only.
- 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 Desktop Console or the Bromium download dialog 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.
Web Browsing with Chrome

- The Flash plug-in must be downloaded from the Adobe site to enable Flash functionality in Chrome
- Uploading and synchronization of browsing-related user data to Google (such as history and bookmarks) is disabled
- Skype extension is not supported
- To use the Widevine Content Decryption Module with video streaming sites such as Netflix, you must add the site to the trusted sites list

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:
  1. 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.
  2. Close Firefox and restart Bromium isolation.
  3. 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 Trust this 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, trust 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

Autonomy

- For Autonomy, isolation supports trusted log in mode only
- Links to documents saved in Autonomy cannot be previewed in Microsoft Outlook
- In Autonomy, the compare/combine functionality in Excel does not work
## Issues Fixed in 4.1.5

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>47210</td>
<td>Users are now able to trust multiple untrusted files at the same time.</td>
</tr>
<tr>
<td>47220</td>
<td>Users are now able to copy untrusted PDFs from their desktops to an IFS shared drive.</td>
</tr>
<tr>
<td>47478</td>
<td>Users can now copy data out of an untrusted XLS sheet into a trusted XLS sheet.</td>
</tr>
<tr>
<td>47680</td>
<td>When a user downloads a Word document in native Chrome with SBX link protection on from a trusted site, the file will no longer be tagged as untrusted.</td>
</tr>
<tr>
<td>48235</td>
<td>When a customer’s site fails to have IIS running, “HTTP Error 500” is no longer shown, but an error stating that “Restarting IIS gave an error” is presented to users instead.</td>
</tr>
<tr>
<td>47641</td>
<td>On a very small number of machines initialisation no longer fails due to SECOND_BOOT_IPC_START_FAILURE. Error 124.</td>
</tr>
<tr>
<td>47096</td>
<td>The numbers on the Unprotected vs Protected widget on the Controller have now been made more consistent.</td>
</tr>
<tr>
<td>47006</td>
<td>.CSV files in \ProgramData...\stats are now being cleared out.</td>
</tr>
<tr>
<td>46346</td>
<td>On a small number of Windows 10 machines, they no longer fail to boot due to missing Windows Boot Manager.</td>
</tr>
<tr>
<td>45581</td>
<td>Rarely, after upgrading Bromium, the Task Manager no longer shows that BrService is stuck in a restart loop.</td>
</tr>
</tbody>
</table>

## Issues Fixed in 4.1.4

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>47247</td>
<td>On the Controller, it is now possible to export a CSV file from the Devices tab when viewing Events associated with a particular endpoint.</td>
</tr>
<tr>
<td>47055</td>
<td>Trusted PDFs can now be saved correctly to a network file share.</td>
</tr>
<tr>
<td>46866</td>
<td>When the Platform is installed using a silent install and the user is not logged in, a reboot required management action is now shown in the Controller.</td>
</tr>
<tr>
<td>46691</td>
<td>The Atovisor boot order no longer causes the PXE (Preboot Execution Environment) to fail.</td>
</tr>
<tr>
<td>46634</td>
<td>Threat false positives are no longer generated when links in Adobe take a user to a “page not found”</td>
</tr>
<tr>
<td>46622</td>
<td>The issue that in some instances caused untrusted PDFs to open an empty Adobe reader no longer occurs.</td>
</tr>
<tr>
<td>45948</td>
<td>The error message “UPDATEGUEST_GUEST_AGENT_INSTALL_REJECTED” is no longer seen during installation in machines that have has the Microsoft August Window Update applied.</td>
</tr>
<tr>
<td>44649</td>
<td>When a machine uses Office 365 set to Shared Computer Licensing, the user no longer has to re-initialize.</td>
</tr>
<tr>
<td>42398</td>
<td>Untrusted PowerPoint files no longer hang and show an error when shared via email.</td>
</tr>
<tr>
<td>34256</td>
<td>When installing new versions of the Bromium Secure Platform, the old versions of the Platform plugins are no longer listed within IE and Outlook.</td>
</tr>
<tr>
<td>34036</td>
<td>Password-protected PDF files no longer generate false threat alerts when opened in Outlook.</td>
</tr>
<tr>
<td>42056</td>
<td>Isolated untrusted tabs in Internet Explorer now show an informative message when the device loses network connectivity, rather than a blank page.</td>
</tr>
<tr>
<td>45261</td>
<td>When a user clicks a trusted site link in an email, it now opens in their default browser instead of native Chrome.</td>
</tr>
<tr>
<td>47593</td>
<td>When installing the OES client for Open Enterprise Server (Novell / MicroFocus), it no longer generates a Blue Screen when the Bromium platform is installed.</td>
</tr>
<tr>
<td>46705</td>
<td>When the X header check is enabled, untrusted email attachments no longer become trusted when forwarded within the trusted domain.</td>
</tr>
</tbody>
</table>
# Issues Fixed in 4.1.3

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>41526</td>
<td>HTTP GET requests returning a 404 status no longer generate a false positive Threat Alert.</td>
</tr>
<tr>
<td>46135</td>
<td>When using a 3-button mouse and using the middle button to click on a link, it no longer opens in host Chrome but now opens in the Secure Browser.</td>
</tr>
<tr>
<td>45958</td>
<td>IE and Firefox browsers no longer show a blank screen immediately on opening after certain upgrade paths have been followed.</td>
</tr>
<tr>
<td>46211</td>
<td>The Firefox Export button now correctly downloads Blobs (Binary Large Objects), such as images from websites including WhatsApp and Salesforce.</td>
</tr>
<tr>
<td>42754</td>
<td>When a printer crashes or breaks during printing and is later brought back on line, it no longer remains permanently blacklisted.</td>
</tr>
<tr>
<td>45948</td>
<td>The Desktop Console no longer reports &quot;UPDATEGUEST_GUEST_AGENT_INSTALL_REJECTED&quot; on some machines that had the Windows August update applied.</td>
</tr>
<tr>
<td>46049</td>
<td>Old threat events that were deleted after passing the default threshold of 30 days are no longer sent to Syslog.</td>
</tr>
<tr>
<td>46249</td>
<td>Outlook no longer fails during initialization when a certain Message Class of email is received.</td>
</tr>
</tbody>
</table>

# Issues Fixed in 4.1.2

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45552</td>
<td>Favicons are now displayed on tabs in Firefox 60.</td>
</tr>
<tr>
<td>40151</td>
<td>The correct sites are now reached when using the forward or back button to navigate amongst browser history in the Secure Browser.</td>
</tr>
<tr>
<td>42677</td>
<td>Font size setting is now correctly honored within the Secure Browser.</td>
</tr>
<tr>
<td>44676</td>
<td>The &quot;Site Settings&quot; button has been removed from the Secure Browser.</td>
</tr>
<tr>
<td>40402</td>
<td>Users can now successfully download files from sites such as secure.dome9.com, when using the Secure Browser.</td>
</tr>
<tr>
<td>42594</td>
<td>When a user orders using the business portal of &quot;Deutsche Bahn&quot; they will no longer see the &quot;payment not secure&quot; message when entering their credit card details.</td>
</tr>
<tr>
<td>33673</td>
<td>Chrome page analytics and tag extensions now work correctly.</td>
</tr>
<tr>
<td>41072</td>
<td>Secure Browser zoom levels are now set correctly when dealing with DPI differences on multiple monitors.</td>
</tr>
<tr>
<td>42999</td>
<td>Word no longer freezes in some instances when opening links in an untrusted document.</td>
</tr>
<tr>
<td>44873</td>
<td>Trusted Office documents stored in Exchange (public) folders no longer become untrusted when edited and saved.</td>
</tr>
<tr>
<td>44768</td>
<td>Word documents containing Chinese fonts no longer incorrectly categorized as a threat.</td>
</tr>
<tr>
<td>45979</td>
<td>A user can no longer attach documents to Outlook emails that are tagged as malicious when they have advanced parameter Untrusted.DenyAccessToMaliciousFile = 1 turned on.</td>
</tr>
<tr>
<td>45717</td>
<td>TrendMicro program files no longer show an untrusted icon overlay on trusted files.</td>
</tr>
<tr>
<td>45925</td>
<td>A user will no longer see HTTP 403 Forbidden error when accessing go.microsoft.com or ieonline.microsoft.com with Chrome or IE.</td>
</tr>
<tr>
<td>45787</td>
<td>During initialization, opened untrusted PDFs now remain open.</td>
</tr>
<tr>
<td>45895</td>
<td>Fixed the erroneous message that displayed in some cases when the Controller is upgraded, &quot;Please install Bromium Controller version 2.5 first to bring the database up to date, before installing this version again&quot;.</td>
</tr>
<tr>
<td>45719</td>
<td>BSODs seen on a very small number of endpoints running 4.0.7 are no longer seen.</td>
</tr>
<tr>
<td>45492</td>
<td>On the Controller when list entries are appended in a delta policy to the base policy, for example to add Trusted Websites, the resultant policy is now shown as being extended from the base policy.</td>
</tr>
<tr>
<td>44741</td>
<td>On the Controller a user can now filter on Disabled Event Types</td>
</tr>
</tbody>
</table>
# Issues Fixed in 4.1.1

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>44949</td>
<td>Fixed an issue some customers were seeing where Chrome bookmarks, history and profile information was being lost due to a clean-up process. This process has been disabled.</td>
</tr>
<tr>
<td>44748</td>
<td>Untrusted .LNK files now launch in a micro-VM when run directly from a .ZIP archive.</td>
</tr>
<tr>
<td>44967</td>
<td>Standard users are no longer potentially able to access service executable paths on the end platform.</td>
</tr>
<tr>
<td>44621</td>
<td>Files copied from an untrusted WebDAV share are no longer treated as being trusted.</td>
</tr>
<tr>
<td>44696</td>
<td>When using IE to access an untrusted webpage using HTTP authentication, the authentication dialogue no longer gets hidden behind a blank window.</td>
</tr>
<tr>
<td>45343</td>
<td>There is a change of language for “Remove Protection” in Japanese.</td>
</tr>
<tr>
<td>43519</td>
<td>An error is no longer generated when a user right-clicks over a PDF and clicks ‘Open with Adobe Acrobat Reader DC’ when the user also has Adobe Acrobat Pro installed on the same machine.</td>
</tr>
<tr>
<td>43719</td>
<td>When opening an untrusted PDF, a user can now access the properties dialogue using (CTRL+D)</td>
</tr>
<tr>
<td>39755</td>
<td>Users using the Persona Management application will no longer experience a partial or complete loss of their profile or loss of pinned items.</td>
</tr>
<tr>
<td>43622</td>
<td>Smart label printers are now correctly shown within a micro-VM.</td>
</tr>
<tr>
<td>44402</td>
<td>When using IE, users can now save a text page in text file TXT format where previously they only had the option to save it in HTML format.</td>
</tr>
<tr>
<td>44905</td>
<td>Chrome ICO files no longer default to being untrusted.</td>
</tr>
<tr>
<td>45145</td>
<td>Encrypted Word files are now correctly shown with the Br Untrusted File Overlay Icon.</td>
</tr>
<tr>
<td>45402</td>
<td>Downloads using Chrome are now correctly marked as trusted, when the site they are download from is marked as trusted.</td>
</tr>
<tr>
<td>45367</td>
<td>False threat alerts are no longer generated when certain registry keys are changed.</td>
</tr>
<tr>
<td>42393</td>
<td>When a user selects the “Export Selection As” function in Adobe Acrobat, they no longer see an error reported when they specify a file name.</td>
</tr>
<tr>
<td>41849</td>
<td>False alerts are no longer generated from HTTP requests which lack details in their commands.</td>
</tr>
<tr>
<td>44949</td>
<td>Chromium Secure Browser bookmarks and other profile data is no longer deleted for some users.</td>
</tr>
<tr>
<td>44736</td>
<td>Remediation of CVE-2018-6148: Incorrect handling of CSP header within the Chrome browser.</td>
</tr>
<tr>
<td>44629</td>
<td>Platform end-points with VirtualBox installed are no longer shown with the installed version number as 0 when the device is view from the Controller.</td>
</tr>
<tr>
<td>44623</td>
<td>The trusted down load site list can now be enabled for IE.</td>
</tr>
<tr>
<td>44516</td>
<td>A client PC can now connect to the Controller via a WinHTTP proxy</td>
</tr>
<tr>
<td>41849</td>
<td>A HTTP OPTIONS request no longer generates a false Threat Alert.</td>
</tr>
<tr>
<td>40891</td>
<td>Renaming a file via Outlook&gt;New Mail&gt;Attach File no longer leads to trusted file becoming untrusted.</td>
</tr>
<tr>
<td>40097</td>
<td>When trusting large Excel files, the operation no longer timeouts.</td>
</tr>
</tbody>
</table>
## Issues Fixed in 4.1 GA

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17639</td>
<td>An event is now sent to the BMS when a file is trusted by entering a user’s admin credentials at the UAC prompt, when logged in as a non-admin.</td>
</tr>
<tr>
<td>35850</td>
<td>When an Outlook Add-In is disabled, an event is now sent to the BEC.</td>
</tr>
<tr>
<td>35971</td>
<td>Performance of VBS in a micro VM in Windows 10 has been improved.</td>
</tr>
<tr>
<td>36032</td>
<td>An untrusted file down loaded onto a file share by a user, is no longer seen as trusted by another user who has access to the same file share.</td>
</tr>
<tr>
<td>36269</td>
<td>AFDS no longer requests a user to re-enter their credentials on a regular basis.</td>
</tr>
<tr>
<td>36576</td>
<td>Office 365 no longer reports “Couldn't Verify Subscription” when opening untrusted Office documents.</td>
</tr>
<tr>
<td>36819</td>
<td>When using Secure Boot with Windows 10 a hibernating machine now resumes the session prior to hibernating instead of re-booting.</td>
</tr>
<tr>
<td>36982</td>
<td>In Windows 7, when running in 32-bit mode on a 64-bit machine Micro VM errors are no longer seen.</td>
</tr>
<tr>
<td>37392</td>
<td>Copying trusted files from Outlook to a Windows folder no longer copies them as untrusted.</td>
</tr>
<tr>
<td>37658</td>
<td>External drives can now be accessed without disabling Bromium Monitoring.</td>
</tr>
<tr>
<td>39643</td>
<td>There is now an option to mark digital signed documents as trusted which is defaulted to off. To enable Untrusted.AdobeDigitalSigning.Enabled to 1.</td>
</tr>
<tr>
<td>40034</td>
<td>False positive threats from broken Word files are no longer identified as threats.</td>
</tr>
<tr>
<td>40143</td>
<td>Searching using the BEC Events tab is now faster and now completes instead of failing in some instances.</td>
</tr>
<tr>
<td>40369</td>
<td>Files downloaded with IE no longer become trusted when saved to FideAS encrypted location.</td>
</tr>
<tr>
<td>40405</td>
<td>When you trust a file (executable), it is no longer tagged as malicious.</td>
</tr>
<tr>
<td>40557</td>
<td>LAST_BOOT_IPC_START_FAILURE is no longer reported preventing initialization from occurring.</td>
</tr>
<tr>
<td>40607</td>
<td>Archived PDF attachment which are converted to HTML attachments can now be opened successfully.</td>
</tr>
<tr>
<td>10420</td>
<td>There is now an option to mark digital signed documents as trusted which is defaulted to off. To enable Untrusted.AdobeDigitalSigning.Enabled to 1.</td>
</tr>
<tr>
<td>40760</td>
<td>The platform no longer locks up immediately after initializing, in some very limited circumstances.</td>
</tr>
<tr>
<td>40798</td>
<td>A user no longer loops back to the SSO sign-in page when using Chrome to access the Alacrity website.</td>
</tr>
<tr>
<td>40800</td>
<td>Untrusted websites no longer appear too big (“zoomed in”) when using IE.</td>
</tr>
<tr>
<td>40813</td>
<td>Trusted websites now prompt for a certificate and for a user to enter their PIN when using VDI.</td>
</tr>
<tr>
<td>40909</td>
<td>“Tracking protection introduction” no longer appears on each new website opened.</td>
</tr>
<tr>
<td>40971</td>
<td>When analyzing lava alerts the Bromium Cloud no longer responds with an error state.</td>
</tr>
<tr>
<td>40989</td>
<td>The platform no longer reports “VTx not supported” when configured to run in quarantine only mode on non VTsx machines.</td>
</tr>
<tr>
<td>41004</td>
<td>The platform can now be enabled / disabled from the System Tray.</td>
</tr>
<tr>
<td>41069</td>
<td>A trusted, password-protected emailed Word documented no longer becomes untrusted when emailed.</td>
</tr>
<tr>
<td>41112</td>
<td>Ad blocking re-worded to “Disable ad blocking for this site.”</td>
</tr>
<tr>
<td>41252</td>
<td>The platform no longer forces the email body into plain text when using ”Send as attachment” in Excel and Word.</td>
</tr>
<tr>
<td>41679</td>
<td>Key combinations in micro-VMs / untrusted sites now work for customers using German (Switzerland) keyboard layout.</td>
</tr>
<tr>
<td>Ticket</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>41765</td>
<td>Untrusted PPT documents no longer fail to send and show an error message when using the File → Share → Email → Send as Attachment function.</td>
</tr>
<tr>
<td>41963</td>
<td>Chrome now supports the open source ticketing system OTRS combined with Shibboleth single sign on.</td>
</tr>
<tr>
<td>42012</td>
<td>Box Sync Files now open normally.</td>
</tr>
<tr>
<td>42111</td>
<td>SharePoint Word documents now open in the same way in Chrome as when a user opens them in Edge.</td>
</tr>
<tr>
<td>42263</td>
<td>When accessing sites using certificate authentication they should no longer intermittently fail with the ERR_SSL_CLIENT_AUTH_CERT_NO_PRIVATE_KEY message.</td>
</tr>
<tr>
<td>42281</td>
<td>Documents can now be successfully saved on SharePoint or Sharepoint on Office 365.</td>
</tr>
<tr>
<td>42294</td>
<td>Untrusted PDFs can now be sent as email attachments when using the envelope icon from within Adobe Reader.</td>
</tr>
<tr>
<td>42489</td>
<td>Threats are no longer not processed when the system restarts after previously running out of disk space.</td>
</tr>
<tr>
<td>42537</td>
<td>There is now configuration to offer Firefox certification revocation checks in micro VMs.</td>
</tr>
<tr>
<td>42550</td>
<td>Performance handling of cookies has been improved within IE.</td>
</tr>
<tr>
<td>42662</td>
<td>Trusted attachments no longer arrive untrusted when attached from a network location.</td>
</tr>
<tr>
<td>43151</td>
<td>Threats previously identified in the BEC cloud are now correctly correlated with any new threats when identifying the threat associated with a new document.</td>
</tr>
<tr>
<td>43213</td>
<td>Nested Active Directory groups are now supported via configuration settings.</td>
</tr>
<tr>
<td>43966</td>
<td>The speed taken to open Windows Explorers has been improved when accessing a network share.</td>
</tr>
<tr>
<td>43582</td>
<td>Chrome no longer fails when attempting to log into an external website when selecting a cached username.</td>
</tr>
<tr>
<td>43909</td>
<td>The platform no longer gets stuck in a reboot loop when using Windows 10 with BitLocker and Credential Guard enabled.</td>
</tr>
<tr>
<td>36322</td>
<td>A ghost IE micro-VM is no longer shown in Live View under certain conditions.</td>
</tr>
<tr>
<td>41031</td>
<td>Installing Google Chrome after installing the platform no longer causes the platform to re-initialize.</td>
</tr>
<tr>
<td>41085</td>
<td>Untrusted webpages now always correctly resize when in a micro VM.</td>
</tr>
<tr>
<td>41356</td>
<td>A client PC can now connect to the Controller via a WinHTTP proxy.</td>
</tr>
<tr>
<td>41241</td>
<td>When adding a trusted site, the prefix is now consistent with the prefixes of Trusted Sites already in the system.</td>
</tr>
<tr>
<td>41713</td>
<td>When setting the DPI to 175% the Desktop Console window is now fully visible.</td>
</tr>
<tr>
<td>42633</td>
<td>The platform no longer shows “Failed test boot when enabling support for Hyper-V” during installation message.</td>
</tr>
</tbody>
</table>
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. 4.1.5)

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 4</td>
<td>13 Nov 2018</td>
<td>13 Nov 2018</td>
<td>13 May 2019</td>
<td>EOS</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.1 Update 1</td>
<td>02 Aug 2018</td>
<td>02 Aug 2018</td>
<td>02 Feb 2019</td>
<td>EOS</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>EOS</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 8</td>
<td>12 Jul 2018</td>
<td>12 Jul 2018</td>
<td>12 Jan 2019</td>
<td>EOS</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 7</td>
<td>08 May 2018</td>
<td>08 May 2018</td>
<td>08 Nov 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 6</td>
<td>04 Apr 2018</td>
<td>04 Apr 2018</td>
<td>02 Oct 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 5</td>
<td>02 Mar 2018</td>
<td>02 Mar 2018</td>
<td>02 Sep 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 4</td>
<td>09 Jan 2018</td>
<td>09 Jan 2018</td>
<td>09 Jul 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 3</td>
<td>21 Nov 2017</td>
<td>21 Nov 2017</td>
<td>21 May 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 2</td>
<td>30 Aug 2017</td>
<td>30 Aug 2017</td>
<td>02 Mar 2018</td>
<td>EOL</td>
</tr>
<tr>
<td>Bromium Secure Platform v4.0 Update 1</td>
<td>23 Jul 2017</td>
<td>23 Jul 2017</td>
<td>23 Nov 2017</td>
<td>EOL</td>
</tr>
<tr>
<td>vSentry 3.2 Update 8</td>
<td>29 Mar 2017</td>
<td>29 Jun 2018</td>
<td>29 Dec 2018</td>
<td>EOS</td>
</tr>
<tr>
<td>vSentry 3.2 Update 7</td>
<td>06 Mar 2017</td>
<td>29 Mar 2017</td>
<td>29 Sep 2017</td>
<td>EOL</td>
</tr>
<tr>
<td>All vSentry 3.2 releases prior to Update 7</td>
<td>EOL</td>
<td>-</td>
<td>-</td>
<td>EOL</td>
</tr>
<tr>
<td>All vSentry 3.1 releases</td>
<td>EOL</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. If you need an account, please contact your Account Executive or Customer Support.
- Email questions to support@bromium.com
- Visit https://support.bromium.com/s/contactsupport for more contact options