Bromium Secure Platform

4.1.1 Release Notes

Contents

Notices

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.

Bromium Secure Platform 4.1

August 2, 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.

AppPack Contents

This release contains support for isolated Chrome version 66, including 32-bit and 64-bit versions. (4.1.1)

Note: The Flash plug-in must be downloaded separately from the Adobe site to enable Flash functionality in isolation protected Chrome.

Bromium Platform Requirements

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

Hardware or Software	Description
CPU	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.
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 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

Hardware or Software	Description
Disk	6 GB free disk space
Operating System	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 For information about security features and hardware recommendations for Windows 10 releases, refer to the Microsoft site: http://www.microsoft.com

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 6.0 is recommended

Supported Software

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

- Google Chrome versions 54, 55, 56, 58, 59, 60, 61, 62, 64, 65, and 66
- Mozilla Firefox ESR 52 (32-bit), with beta support for Firefox ESR 60 (32-bit)

Firefox ESR 60 (32-bit), with Group Policy support for enterprise deployments, is now supported as a beta release but has the following known issues:

- Download page not listing downloads - the Firefox download manager does not show any downloads from protected sites.
- Favicons do not always appear within the browser.

Note: Firefox ESR 60 (32-bit) needs to be installed as a pre-requisite. As this is a beta release, Customers should back up their Firefox bookmarks and profile prior to installation.

- 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:
  - Standard, ProPlus, Home Business, Home Student, Personal, Professional, O365 ProPlus, O365 Business, O365 Small Business Premium, O365 Home Premium
- Microsoft Office 2016, MSI, x64 and x86:
  - Standard, ProPlus
- Microsoft Office 2016, Click-to-Run, x64 and x86:
  - Standard, ProPlus, Home Business, Home Student, Personal, Professional, O365 ProPlus, O365 Business, O365 Small Business Premium, O365 Home Premium

> **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, and 2016
- Adobe Reader versions 9, 10, 11, DC Classic 2015, DC Classic 2017, DC Continuous 2015, DC Continuous 2017, and DC Continuous 2018
- Adobe Acrobat Professional version 10 and 11, DC Classic 2015, and DC Continuous 2015
- 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
- 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 controller, back up your current database.

Bromium Controller Requirements

Hardware or Software	Description
CPU	Sandy Bridge Intel Xeon Quad-core or better
Disk	1 TB free disk space
Network	Port 443 on the web server must be available for the management application
Operating System	Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Memory	16 GB RAM
Software	Microsoft IIS 7.5+ with CGI module, IIS Manager, static content, and anonymous authentication installed .NET 4 Extended (server)
SSL	Valid SSL certificate trusted by endpoints (For testing only, the server may be configured insecurely to run in HTTP mode)

Supported Browsers

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

SQL Database Requirements

Hardware or Software	Description
Performance	200 IOPS sustained per 1000 endpoints
Software	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)
Storage Space	1 TB available space

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 article on the Bromium Support site.

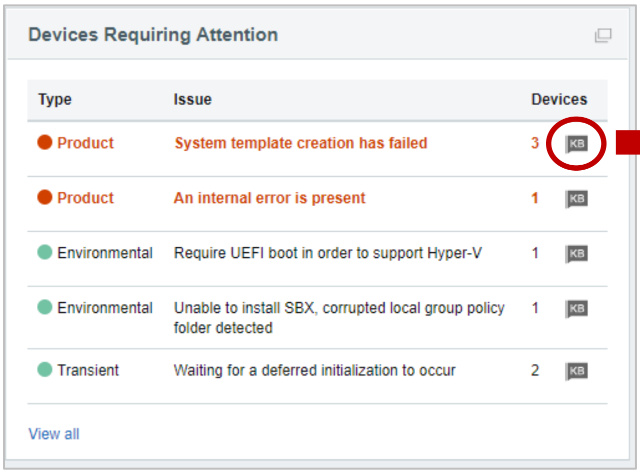
What's New?

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

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.

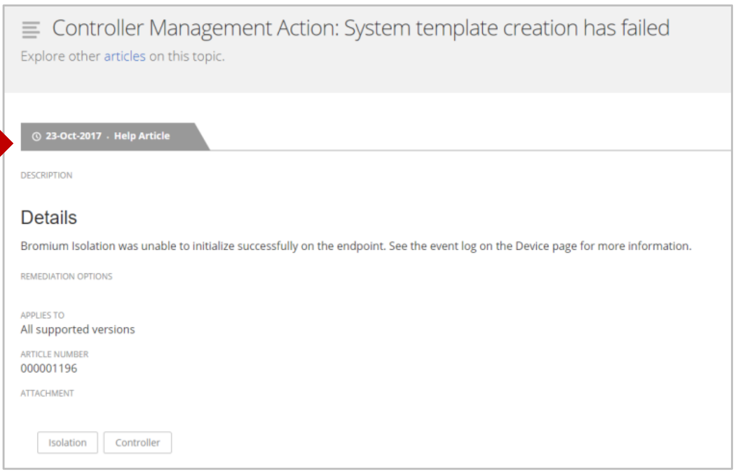
Controller Dashboard 4.1.1



Devices Requiring Attention

Type	Issue	Devices
● Product	System template creation has failed	3 KB
● Product	An internal error is present	1 KB
● Environmental	Require UEFI boot in order to support Hyper-V	1 KB
● Environmental	Unable to install SBX, corrupted local group policy folder detected	1 KB
● Transient	Waiting for a deferred initialization to occur	2 KB

Drill-Down into KB Article



Controller Management Action: System template creation has failed

Explore other articles on this topic.

23-Oct-2017 · Help Article

DESCRIPTION

Details

Bromium Isolation was unable to initialize successfully on the endpoint. See the event log on the Device page for more information.

REMEDIATION OPTIONS

APPLIES TO
All supported versions

ARTICLE NUMBER
000001196

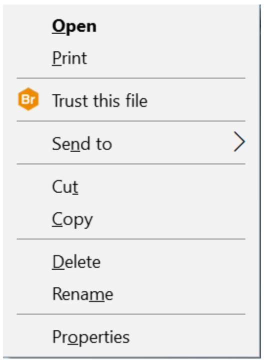
ATTACHMENT

Faster Initializations (4.1)

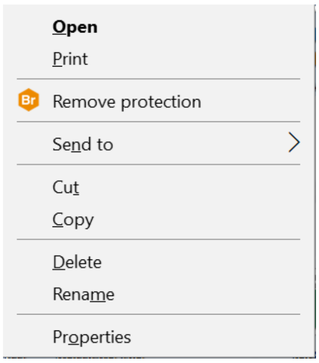
In most instances, Bromium Secure Platform is fully initialized on the end user's PC in ~5 minutes.

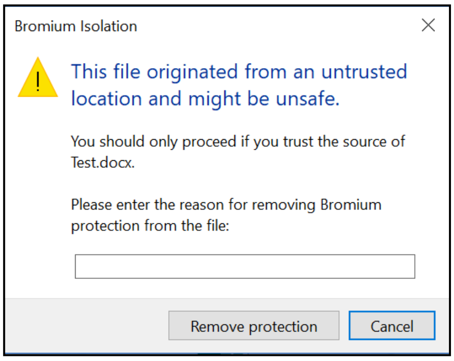
"Trust this file" is now "Remove protection" (4.1)

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.





Bromium Isolation

This file originated from an untrusted location and might be unsafe.

You should only proceed if you trust the source of Test.docx.

Please enter the reason for removing Bromium protection from the file:

Secure User-Centric Browsing (4.1)

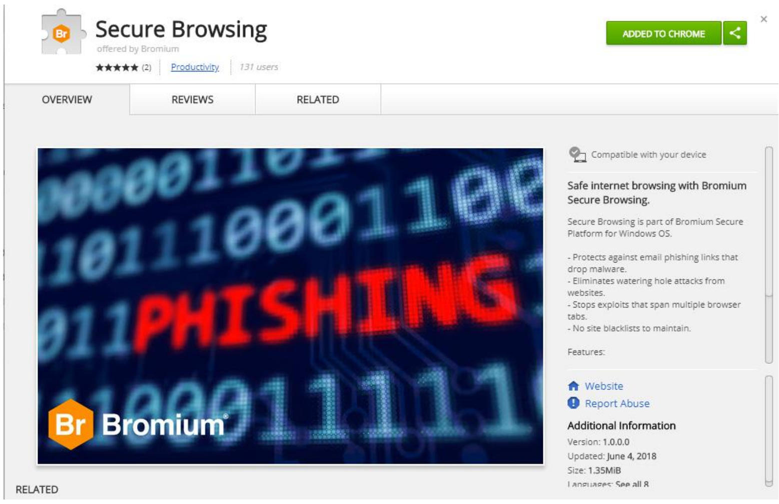
Enjoy greater web productivity and freedom with enhanced user satisfaction, without sacrificing security, using native Chrome on the host for low-risk browsing and the Bromium Secure Browser to isolate high-risk web activities. This new model of operation may better suit some of your users for whom Chrome 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/fcbnoohifpjfjohaciofjaefgpdjmhcf
    - Ensure that **Allow access to file URLs** is enabled.



Secure Browsing

offered by Bromium

★★★★★ (2) | Productivity | 131 users

Compatible with your device

Safe internet browsing with Bromium Secure Browsing.

Secure Browsing is part of Bromium Secure Platform for Windows OS.

- Protects against email phishing links that drop malware.
- Eliminates watering hole attacks from websites.
- Stops exploits that span multiple browser tabs.
- No site blacklists to maintain.

Features:

Additional Information

Version: 1.0.0.0

Updated: June 4, 2018

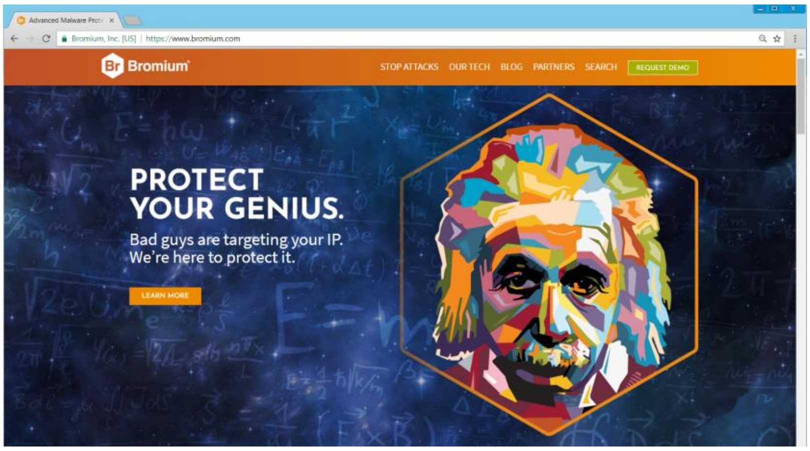
Size: 1.35MiB

Languages: See all 8

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 Secure Browser (4.1)

The 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.

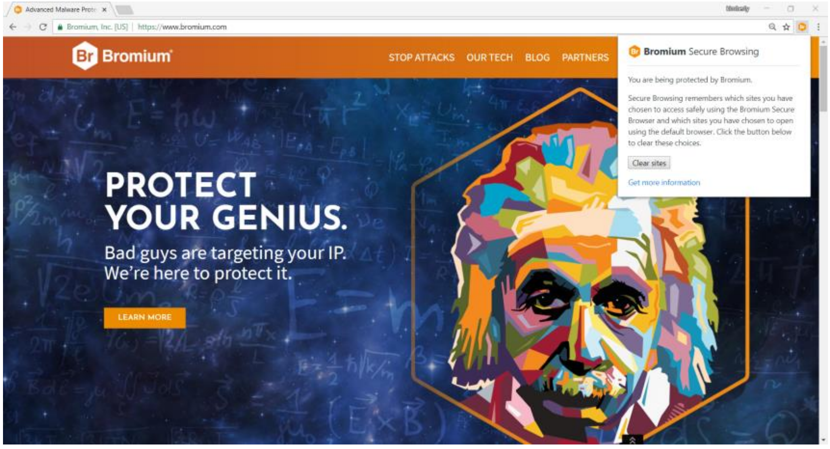


Bromium, Inc. [US] | https://www.bromium.com

PROTECT YOUR GENIUS.

Bad guys are targeting your IP. We're here to protect it.

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.



Bromium Secure Browsing

You are being protected by Bromium.

Secure Browsing remembers which sites you have chosen to access safely using the Bromium Secure Browser and which sites you have chosen to open using the default browser. Click the button below to clear these choices.

The 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*.

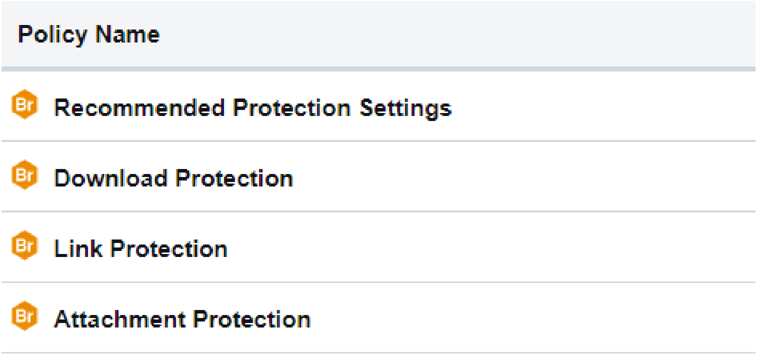
Targeted Use Case Deployment (4.1)

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:



Policy Name
Recommended Protection Settings
Download Protection
Link Protection
Attachment Protection

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

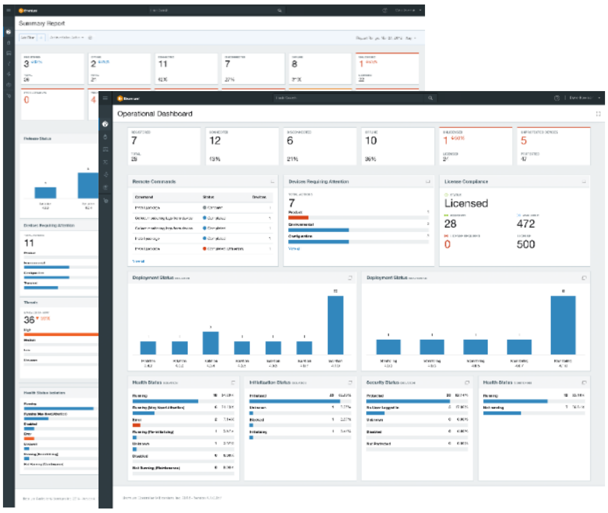
- Policy control changes: the toggle now says Off/On, with a new Append checkbox. (4.1)
- It is now possible to add/apply policies to endpoints from the Device Groups page. (4.1)
- Administrators are now prompted for a reason when changing policies, which is also logged in the Policy Revision History 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)

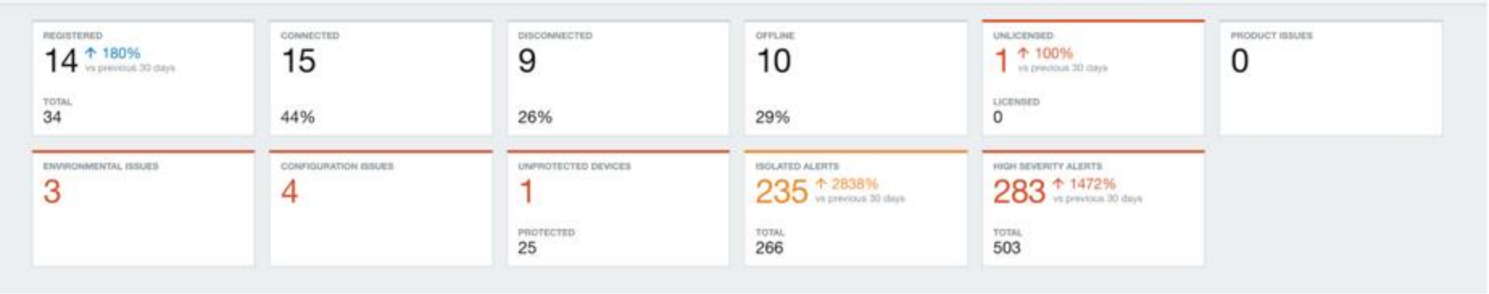
Bromium Secure Platform 4.1 has only one .msi and only one listing in Add/Remove Programs. Monitoring libraries are automatically installed but no longer enabled by default.

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.



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



REGISTERED
14 ↑ 180% vs previous 30 days
TOTAL
34

CONNECTED
15
44%

DISCONNECTED
9
26%

OFFLINE
10
29%

UNLICENSED
1 ↑ 100% vs previous 30 days
LICENSED
0

PRODUCT ISSUES
0

ENVIRONMENTAL ISSUES
3

CONFIGURATION ISSUES
4

UNPROTECTED DEVICES
1
PROTECTED
25

ISOLATED ALERTS
235 ↑ 2838% vs previous 30 days
TOTAL
266

HIGH SEVERITY ALERTS
283 ↑ 1472% vs previous 30 days
TOTAL
503

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

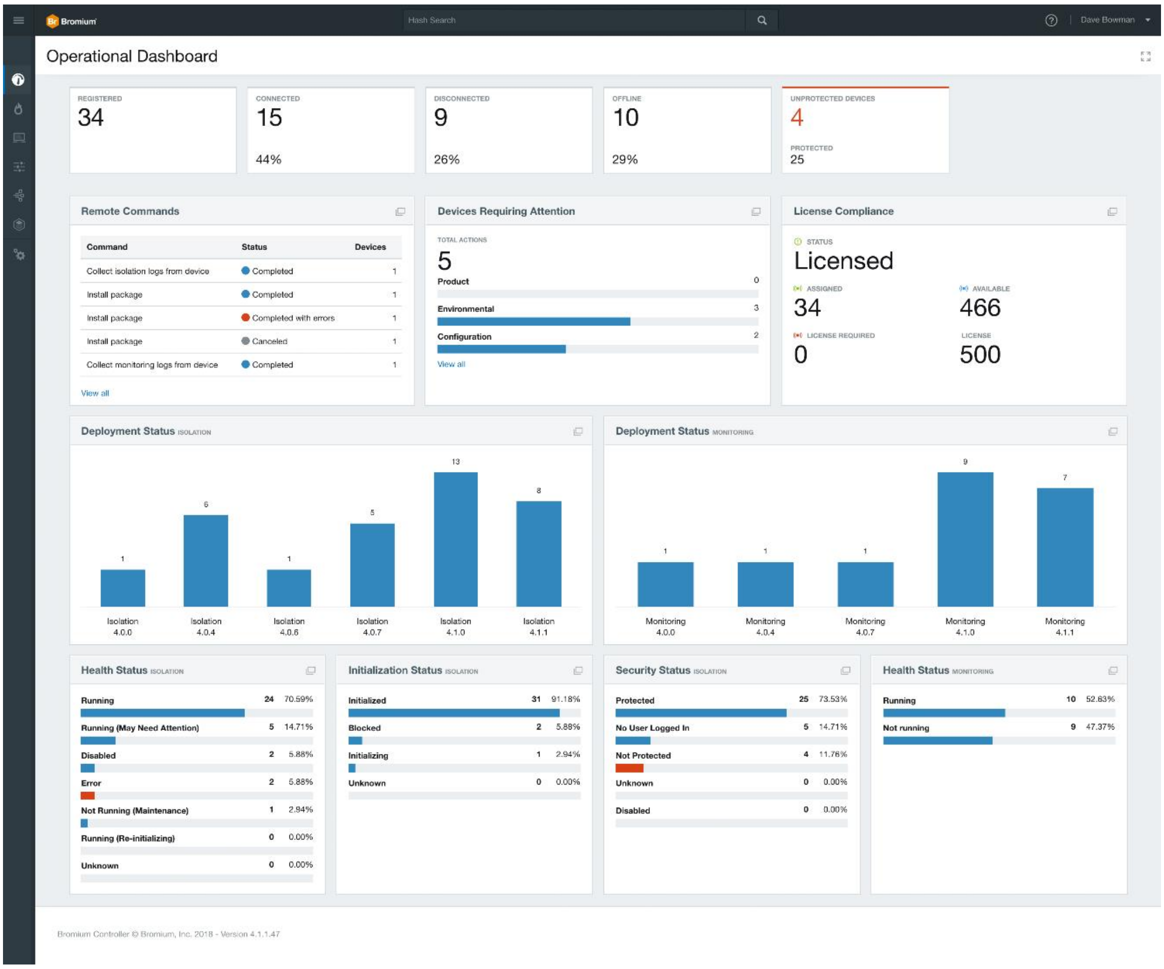
By default, the Operational Dashboard is opened when you click Dashboard in the left navigation. To change this, expand the menu next to the current user name in the upper left-hand corner of the controller interface. Select Preferences, then select Threat from the Default Dashboard options.

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:



REGISTERED	CONNECTED	DISCONNECTED	OFFLINE	UNPROTECTED DEVICES
34	15	9	10	4
	44%	26%	29%	PROTECTED 25

Remote Commands

Command	Status	Devices
Collect isolation logs from device	● Completed	1
Install package	● Completed	1
Install package	● Completed with errors	1
Install package	● Canceled	1
Collect monitoring logs from device	● Completed	1

View all

Devices Requiring Attention

TOTAL ACTIONS 5

Product	0
Environmental	3
Configuration	2

View all

License Compliance

STATUS Licensed

ASSIGNED 34

AVAILABLE 466

LICENSE REQUIRED 0

LICENSE 500

Health Status ISOLATION

Running	24	70.59%
Running (May Need Attention)	5	14.71%
Disabled	2	5.88%
Error	2	5.88%
Not Running (Maintenance)	1	2.94%
Running (Re-initializing)	0	0.00%
Unknown	0	0.00%

Initialization Status ISOLATION

Initialized	31	91.18%
Blocked	2	5.88%
Initializing	1	2.94%
Unknown	0	0.00%

Security Status ISOLATION

Protected	25	73.53%
No User Logged In	5	14.71%
Not Protected	4	11.76%
Unknown	0	0.00%
Disabled	0	0.00%

Health Status MONITORING

Running	10	52.63%
Not running	9	47.37%

Bromium Controller © Bromium, Inc. 2018 - Version 4.1.1.47

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

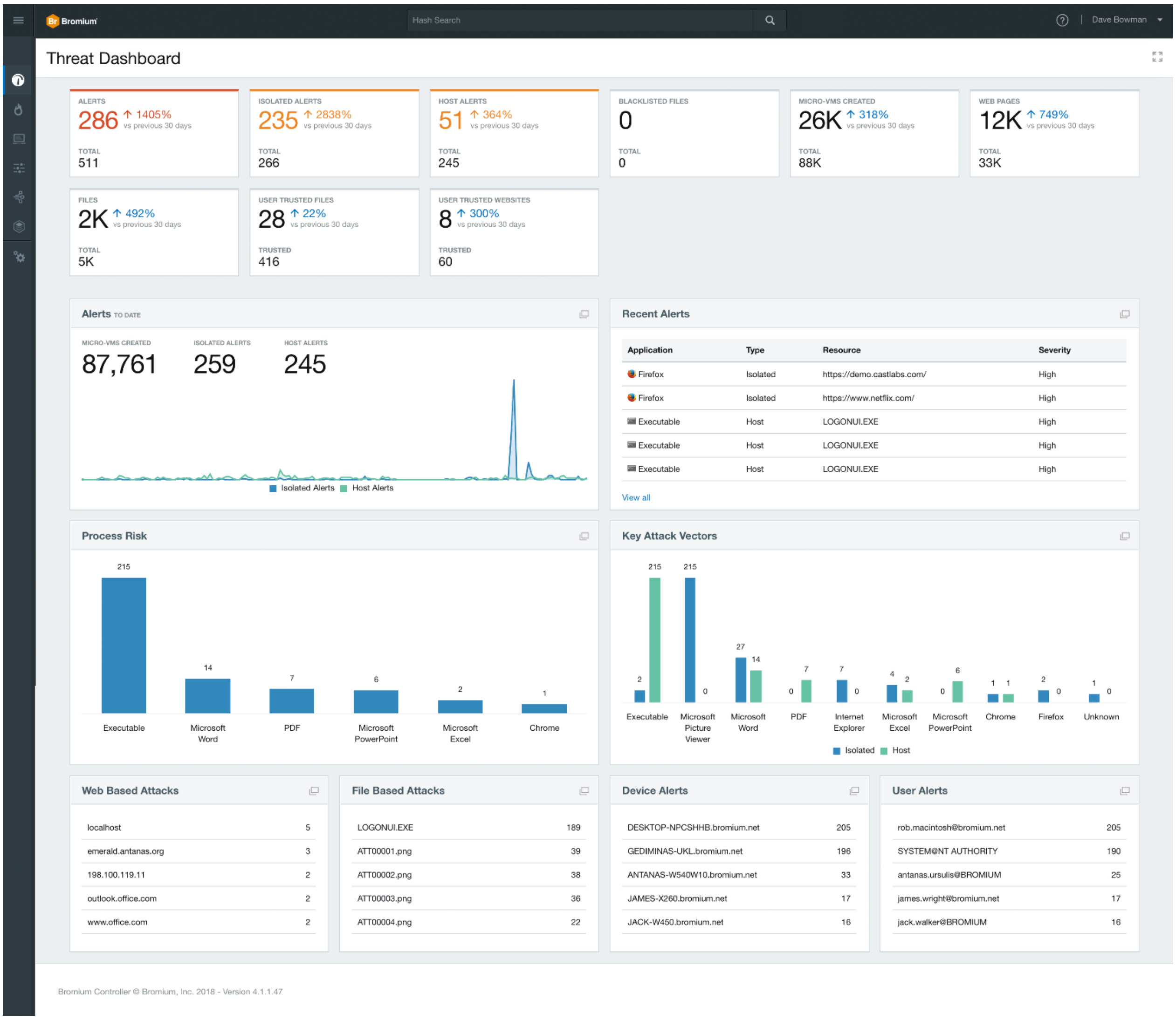
This component indicates the state of isolation on devices and provides security status information:

- 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:



Threat Dashboard

ALERTS 286 ↑ 1405% vs previous 30 days	TOTAL	511
ISOLATED ALERTS 235 ↑ 2838% vs previous 30 days	TOTAL	266
HOST ALERTS 51 ↑ 364% vs previous 30 days	TOTAL	245
BLACKLISTED FILES 0	TOTAL	0
MICRO-VMS CREATED 26K ↑ 318% vs previous 30 days	TOTAL	88K
WEB PAGES 12K ↑ 749% vs previous 30 days	TOTAL	33K
FILES 2K ↑ 492% vs previous 30 days	TOTAL	5K
USER TRUSTED FILES 28 ↑ 22% vs previous 30 days	TRUSTED	416
USER TRUSTED WEBSITES 8 ↑ 300% vs previous 30 days	TRUSTED	60

Alerts TO DATE

MICRO-VMS CREATED	ISOLATED ALERTS	HOST ALERTS
87,761	259	245

Recent Alerts

Application	Type	Resource	Severity
Firefox	Isolated	https://demo.castlabs.com/	High
Firefox	Isolated	https://www.netflix.com/	High
Executable	Host	LOGONUI.EXE	High
Executable	Host	LOGONUI.EXE	High
Executable	Host	LOGONUI.EXE	High

View all

Process Risk

Key Attack Vectors

Web Based Attacks

localhost	5
emerald.antanas.org	3
198.100.119.11	2
outlook.office.com	2
www.office.com	2

File Based Attacks

LOGONUI.EXE	189
ATT00001.png	39
ATT00002.png	38
ATT00003.png	36
ATT00004.png	22

Device Alerts

DESKTOP-NPCSHHB.bromium.net	205
GEDIMINAS-UKL.bromium.net	196
ANTANAS-W540W10.bromium.net	33
JAMES-X260.bromium.net	17
JACK-W450.bromium.net	16

User Alerts

rob.macintosh@bromium.net	205
SYSTEM@NT AUTHORITY	190
antanas.ursulis@BROMIUM	25
james.wright@bromium.net	17
jack.walker@BROMIUM	16

Bromium Controller © Bromium, Inc. 2018 - Version 4.1.1.47

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

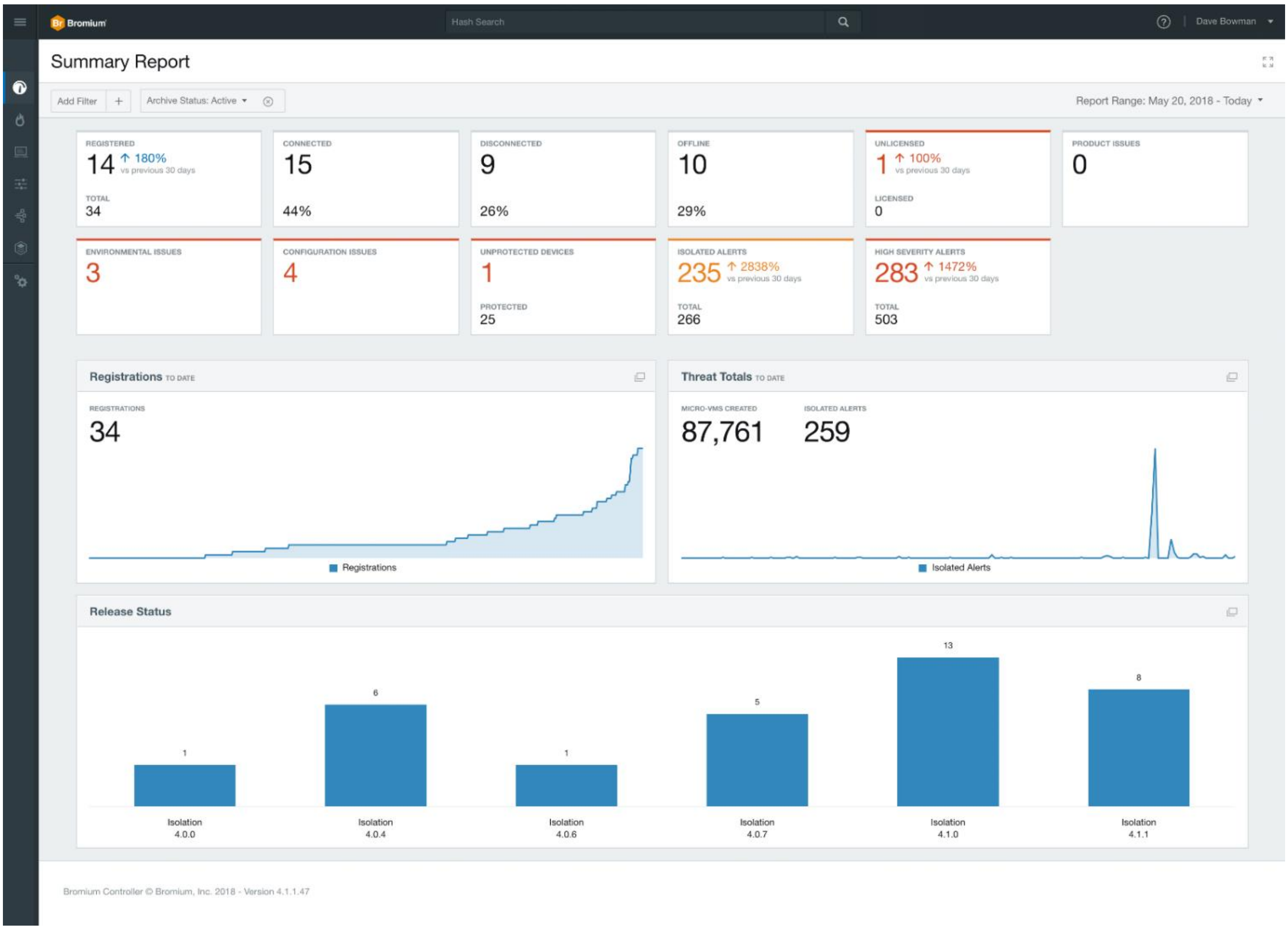
These sections list the top five web and file-based attack names and the number of occurrences for each. Click a threat to view filtered details on the Threats page.

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

- If Bromium Secure Monitoring version 4.0 Update 4 and later is installed on a device without isolation (that is, you have removed isolation from the device after running the Bromium Secure Platform installer), the remote commands **Install Package** and **Uninstall Package** will remain in a Sending state in the controller and will not be run
- 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

- On Windows 10, Internet Explorer is not automatically set to the default browser, even when Browser.CheckDefaultBrowser is set to 1. To avoid this issue, configure your file associations using group policy. Refer to https://technet.microsoft.com/en- us/library/mt269907.aspx and https://technet.microsoft.com/en-us/library/hh825038.aspx?f=255&MSPPError=-2147217396 for more information about configuring group policy for default browsers.
- 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 4.1.1

Issue ID	Description
44748	Untrusted .LNK files now launch in a micro-VM when run directly from a .ZIP archive.
44967	Standard users are no longer potentially able to access service executable paths on the end platform.
44621	Files copied from an untrusted WebDAV share are no longer treated as being trusted.
44696	When using IE to access an untrusted webpage using HTTP authentication, the authentication dialogue no longer gets hidden behind a blank window.
45343	There is a change of language for “Remove Protection” in Japanese.
43519	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.
43719	When opening an untrusted PDF, a user can now access the properties dialogue using (CTRL+D)
39755	Users using the Persona Management application will no longer experience a partial or complete loss of their profile or loss of pinned items.
43622	Smart label printers are now correctly shown within a micro-VM.
44402	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.
44905	Chrome ICO files no longer default to being untrusted.
45145	Encrypted Word files are now correctly shown with the Br Untrusted File Overlay Icon.
45402	Downloads using Chrome are now correctly marked as trusted, when the site they are download from is marked as trusted.
45367	False threat alerts are no longer generated when certain registry keys are changed.
42393	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.
41849	False alerts are no longer generated from HTTP requests which lack details in their commands.
44949	Chromium Secure Browser bookmarks and other profile data is no longer deleted for some users.

Issues Fixed in 4.1 GA

Issue ID	Description
17639	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.
35850	When an Outlook Add-In is disabled, an event is now sent to the BEC.
35971	Performance of VBS in a micro VM in Windows 10 has been improved.
36032	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.
36269	AFDS no longer requests a user to re-enter their credentials on a regular basis.
36576	Office 365 no longer reports “Couldn't Verify Subscription" when opening untrusted Office documents.
36819	When using Secure Boot with Windows 10 a hibernating machine bow resumes the session prior to hibernating instead of re-booting.
36982	In Windows 7, when running in 32-bit mode on a 64-bit machine Micro VM errors are no longer seen.
37392	Copying trusted files from Outlook to a Windows folder no longer copies them as untrusted.
37658	External drives can now be accessed without disabling Bromium Monitoring.
39643	TASKENG.EXE which is signed by Microsoft, no longer causes a host threat detection.
39953	Event sorting in the BEC is now consistently ordered by “Reported” date.
40034	False positive threats from broken Word files are no longer identified as threats.
40143	Searching using the BEC Events tab is now faster and now completes instead of failing in some instances.
40369	Files downloaded with IE no longer become trusted when saved to FideAS encrypted location.
40405	When you trust a file (executable), it is no longer tagged as malicious.
40557	LAST_BOOT_IPC_START_FAILURE is no longer reported preventing initialization from occurring.
40607	Archived PDF attachment which are converted to HTML attachments can now be opened successfully.
10420	There is now an option to mark digital signed documents as trusted which is defaulted to off. To enable Untrusted.AdobeDigitalSigning.Enabled to 1.
40760	The platform no longer locks up immediately after initializing, in some very limited circumstances.
40798	A user no longer loops back to the SSO sign-in page when using Chrome to access the Alacrity website.
40800	Untrusted websites no longer appear too big (“zoomed in”) when using IE.
40813	Trusted websites now prompt for a certificate and for a user to enter their PIN when using VDI.
40909	"Tracking protection introduction" no longer appears on each new website opened.
40971	When analyzing lava alerts the Bromium Cloud no longer responds with an error state.
40989	The platform no longer reports “VTx not supported” when configured to run in quarantine only mode on non VTsx machines.
41004	The platform can now be enabled / disabled from the System Tray.
41069	A trusted, password-protected emailed Word documented no longer becomes untrusted when emailed.
41112	Ad blocking re-worded to "Disable ad blocking for this site."
41252	The platform no longer forces the email body into plain text when using "Send as attachment" in Excel and Word.
41679	Key combinations in micro-VMs / untrusted sites now work for customers using German (Switzerland) keyboard layout.

41765	Untrusted PPT documents no longer fail to send and show an error message when using the File → Share → Email → Send as Attachment function.
41963	Chrome now supports the open source ticketing system OTRS combined with Shibboleth single sign on.
42012	Box Sync Files now open normally.
42111	SharePoint Word documents now open in the same way in Chrome as when a user opens them in Edge.
42263	When accessing sites using certificate authentication they should no longer intermittently fail with the ERR_SSL_CLIENT_AUTH_CERT_NO_PRIVATE_KEY message.
42281	Documents can now be successfully saved on SharePoint or SharePoint on Office 365.
42294	Untrusted PDFs can now be sent as email attachments when using the envelope icon from within Adobe Reade.
42489	Threats are no longer not processed when the system restarts after previously running out of disk space.
42537	There is now configuration to offer Firefox certification revocation checks in micro VMs.
42550	Performance handling of cookies has been improved within IE.
42662	Trusted attachments no longer arrive untrusted when attached from a network location.
43151	Threats previously identified in the BEC cloud are now correctly correlated with any new threats when identifying the threat associated with a new document.
43213	Nested Active Directory groups are now supported via configuration settings.
43996	The speed taken to open Windows Explorers has been improved when accessing a network share.
43582	Chrome no longer fails when attempting to log into an external website when selecting a cached username.
43909	The platform no longer gets stuck in a reboot loop when using Windows 10 with BitLocker and Credential Guard enabled.
36322	A ghost IE micro-VM is no longer shown in Live View under certain conditions.
41031	Installing Google Chrome after installing the platform no longer causes the platform to re-initialize.
41085	Untrusted webpages now always correctly resize when in a micro VM.
41356	A client PC can now connect to the Controller via a WinHTTP proxy.
41241	When adding a trusted site, the prefix is now consistent with the prefixes of Trusted Sites already in the system.
41713	When setting the DPI to 175% the Desktop Console window is now fully visible.
42633	The platform no longer shows “Failed test boot when enabling support for Hyper-V” during installation message.

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
- Call Bromium Customer Support at 1-800-518-0845
- Call your technical account representative directly