



Bromium Secure Configuration Checklist

Version 1.0

Bromium Secure Platform 4.0

December 17th, 2017

Prepared by: Robert Wiggerhorn



Notices

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. RESTRICTED RIGHTS LEGEND: Terms and Conditions Applicable to Federal Governmental End Users. Bromium licenses products for ultimate end use by federal government agencies and other federal government customers ("federal government customers") only under the following conditions. Software and technical data rights in these products include only those rights customarily provided to end use customers of Software as defined in the Bromium Master Software License and Services Agreement and any exhibit thereto. This customary commercial license in technical data and software is provided in accordance with FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for Department of Defense purchases, DFAR 252.227-7015 (Technical Data - Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a federal government or other public sector customer has a need for rights not conveyed under these terms, it must negotiate with Bromium to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written agreement specifically conveying such rights must be executed by both parties.

The product 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 micro-VM®, micro-virtualization, and "Keep calm and keep clicking. vSentry®. Trustworthy by Design™." are registered trademarks or 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.

5 July 2016

Contents

Introduction.....	3
Document Overview	3
Bromium Secure Platform Overview	3
Bromium Secure Platform Use Cases.....	3
Bromium Secure Platform Architecture	3
Bromium Controller Deployment Scenarios	4
Bromium Lifecycle Management	4
Prerequisite Installation and Configuration	6
Overview	6
Configurations.....	6
Microsoft IIS and Microsoft SQL Server.....	8
Overview	8
Microsoft IIS Configurations	8
Microsoft SQL Server Configurations	9
Bromium Dashboard Configurations	10
Overview	10
Configurations.....	10
Bromium Secure Client Policy Configurations	12
Overview	12
Configurations.....	12
Appendix A: Baseline Policy Advanced Parameters.....	17
Overview	17
Configurations.....	17
Appendix B: Antivirus Exclusions.....	19
Overview	19
Configurations.....	19
Appendix C: Baseline Policy	21
Overview	21
Configurations.....	21
Appendix D: Client Certificate Authentication	23
Overview	23
Configurations.....	23

Introduction

Document Overview

The purpose of this document is to provide guidance on how to securely implement and configure the Bromium Secure Platform 4.0. This includes Bromium Secure Browsing, Bromium Secure Files, and the Bromium Dashboard. The Bromium Secure Monitoring component will be covered in a separate document for simplicity purposes. This document will be updated as new versions of the Bromium Secure Platform are released.

Bromium Secure Platform Overview

Bromium Secure Platform provides protection at the endpoint against advanced malware. Bromium automatically creates hardware-isolated micro-VMs that secure user tasks—such as visiting a web page, downloading a document, or opening an email attachment. Each task runs in its own micro-VM and all micro-VMs are separated from each other, and from the trusted enterprise network. If malware targets the end user, the threat is contained in the hardware-isolated micro-VM. Consequently, it is never able to steal or damage the user or enterprise's information, and is destroyed when the task is closed. Bromium is transparent to the end user and has no discernible impact on user experience or system performance.

Bromium Secure Platform Use Cases

Bromium isolates and prevents the most common threat vectors including: Web browsing, Internet downloads, Email attachments, and USB drives. By hardware isolating each untrusted activity, Bromium protects against: Spear phishing attacks, Ransomware, Kernel and 0-day exploits, and APTs (advanced persistent threats).

Bromium Secure Platform provides protection against application and system level vulnerabilities by isolating and containing vulnerable applications and content inside separate virtual machines. Bromium monitors the behavior of each micro-VM and provides alerts to the IT operations or security team if abnormal behavior is detected inside a micro-VM. The security team can leverage this forensic data to respond to potential threats in real-time and take preventative action across the enterprise.

Bromium Secure Platform Architecture

Figure 1 below shows the high-level Bromium Secure Platform architecture including the Bromium Secure Client, the Bromium Dashboard, and the integration points with existing infrastructure such as SQL servers, SIEMs, and CIFS shares. In addition, this diagram includes the standard ports and protocols that are used for the connections between each of these services.

The Bromium Secure Platform client 4.0 is supported on Windows 7, Windows 8.1, and Windows 10.

The Bromium Dashboard requires two Microsoft components: IIS and SQL Server. The Bromium Dashboard component loaded onto IIS is referred to as the Bromium Controller. The Bromium Controller can be installed on Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. The Bromium Controller requires Microsoft IIS 7.5 or later with the CGI module installed and .NET 4 Extended.

The Bromium Dashboard requires a backend SQL server to store configuration and alert data. Bromium supports the following versions of SQL: SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, and SQL Server 2016.

If multiple Bromium Controllers are used, a CIFS share should be leveraged to store the detailed Bromium threat data so that the data can be read/updated by each of the management servers.

Bromium Ports and Protocols

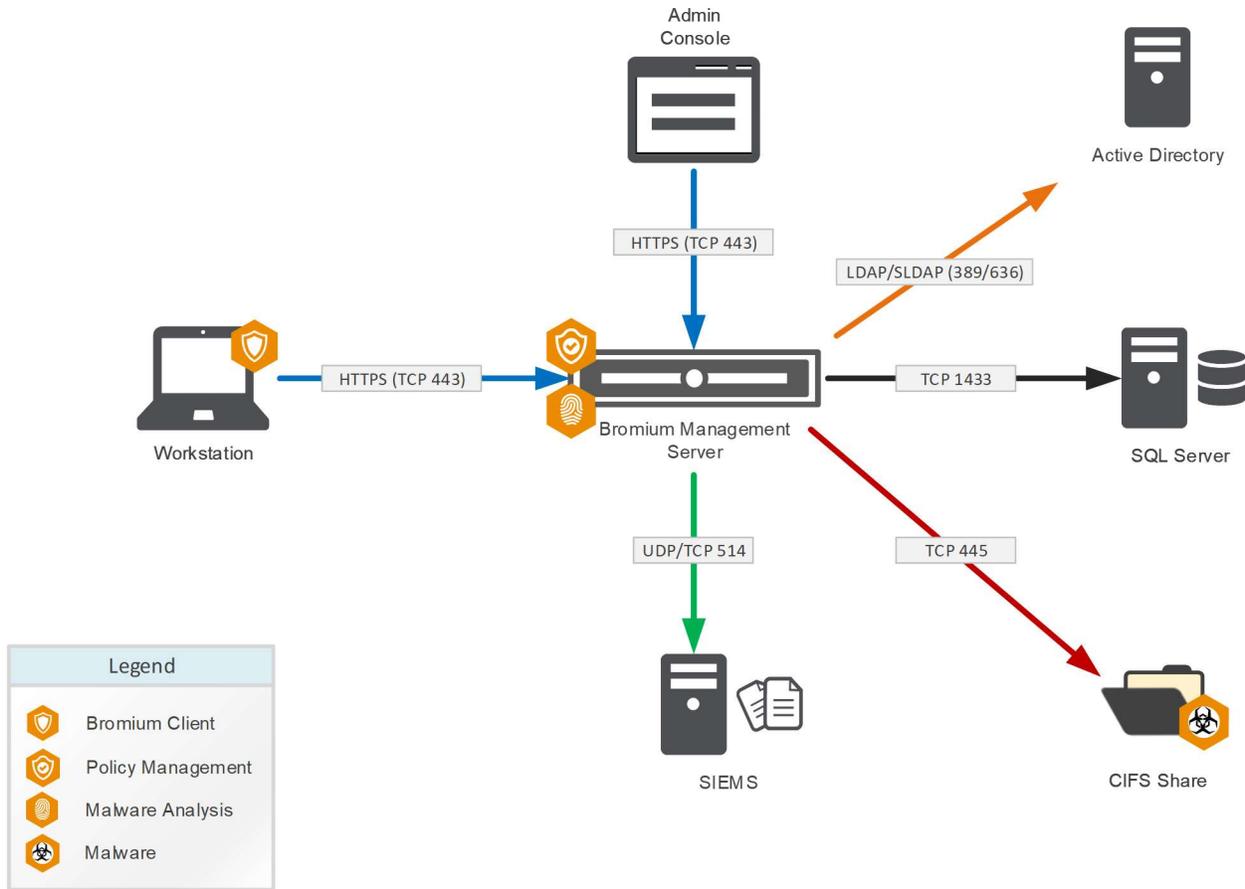


Figure 1

Bromium Controller Deployment Scenarios

The Bromium Controller is typically deployed on the corporate intranet to support Bromium management of internal workstations and laptops. However, the Bromium Controller also supports scenarios where devices such as laptops go “off network” and may or may not VPN back in to the corporate network. Client certificate authentication allows the Bromium Secure Platform clients to check-in securely while off of the corporate network without having to have a VPN connection. This method ensures that only devices with the properly configured and issued certificates are able to connect to the Bromium management infrastructure preventing rogue devices or agents from attempting to gain unauthorized access to the Bromium Controller servers. Additional information on the client certificate authentication deployment scenarios can be found in [Appendix D](#). Additional configuration and implementation details can be found in the *Bromium Secure Platform Deployment Guide*.

Bromium Lifecycle Management

A standard Bromium Secure Platform rollout includes 4 phases: Analyze, Design, Deploy, and Operate. The analysis phase typically includes requirements gathering and an initial validation testing of a small group of users. Based on the requirements and the results the user testing, an architecture and configuration design is created to best meet the security and usability needs of the organization. During the deployment phase, the Bromium management infrastructure including the Bromium Controller and SQL environment is built and tested. After the infrastructure has been built, a larger pilot phase of several hundred users begins. Once the pilot rollout is successful, the full enterprise rollout typically follows. After the Bromium Secure Platform has been deployed to all users, the operation phase begins which includes responding to

user tickets, investigating security alerts, and upgrading and patching the infrastructure and client software. A typical Bromium rollout takes anywhere from several weeks to several months depending on the size and complexity of the organization and its users.

Once the Bromium Secure Platform system is in the operational phase, significantly less resources are required to perform lifecycle management on the infrastructure than is typically needed to initially deploy the software. In general, the Bromium Secure Platform client and management infrastructure should only need to be updated 1-2 times per year. The frequency and urgency of these updates will depend on what additional features and improvements are included in each release and the needs and requirements of each organization. The Bromium Controller can typically be upgraded as an “in-place” upgrade and the Bromium Secure Platform client can be upgraded via the Bromium Controller or existing Electronic Software Distribution systems. It is also recommended that regular audits of the Bromium policies are performed to ensure compliance, change control and auditing procedures are followed.

Prerequisite Installation and Configuration

Overview

The Bromium Secure Platform infrastructure requires several prerequisites which will be discussed in further detail in this section. These configuration recommendations are to help ensure that the underlying infrastructure of the Bromium Secure Platform is properly secured prior to installing and configuring the Bromium software.

Configurations

This section includes the specific security configuration recommendations.

1. Enable Virtualization Extensions

Recommendation	Enable virtualization extensions in BIOS of end user workstations.
Rationale	Bromium Secure Platform requires virtualization extensions to provide the hardware-based isolation of untrusted activity and allow for the creation of light-weight virtual machines called micro-VMs.
Implementation	Not Bromium Specific

2. Confirm vPro Support on W10 VBS Devices

Recommendation	Confirm vPro support on W10 VBS devices.
Rationale	If Bromium is being deployed to a Windows 10 workstation with Microsoft Virtualization Based Security enabled, Intel vPro is required for Bromium Isolation to function correctly.
Implementation	Not Bromium Specific

3. Confirm Application Compatibility

Recommendation	Use compatible application versions with Bromium Secure Platform.
Rationale	Bromium Secure Platform supports a wide array of applications and versions including Microsoft Office, Adobe Reader and Professional, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox. However, there are some specific requirements, for instance, Bromium Secure Platform requires Mozilla Firefox ESR.
Implementation	Refer to the Bromium Deployment Guide for additional information on the list of currently supported applications.

4. Patch Operating System

Recommendation	Ensure that the operating systems for the server infrastructure are patched.
Rationale	Applying operating system patches, especially security patches, will help protect against potential system vulnerabilities and reduce the risk of the server infrastructure being compromised.
Implementation	Not Bromium specific

5. Domain Join Servers

Recommendation	Ensure that the server infrastructure is domain joined.
Rationale	Domain joining the server infrastructure enables Active Directory (AD) authentication to the management servers and AD-based SQL service accounts.
Implementation	Not Bromium specific

6. Create SSL Certificate

Recommendation	Create an SSL certificate for client connections.
Rationale	The client and administrator connections should be secured
Implementation	Not Bromium specific

7. Create AD Service Account

Recommendation	Create AD service account for Controller and SQL connections
Rationale	The Bromium Controller IIS and SQL connection account should be an AD account versus a local account so that password and service account management can be performed at an enterprise level.
Implementation	Not Bromium specific

8. Create CIFS Share

Recommendation	Create a secure CIFS share for Bromium alert data
Rationale	A CIFS share should be created that allows the Bromium Controller service account to create and update files. This share should be locked down to ensure that unauthorized users do not have access to the Bromium generated threat data.
Implementation	Not Bromium specific

Microsoft IIS and Microsoft SQL Server

Overview

The Bromium Dashboard relies on two key infrastructure components. The first is Microsoft IIS for the Bromium Controller, which hosts the browser-based administrator console and the second is Microsoft SQL Server to store configuration and alert data. It is critical that security best practices are implemented for these components as part of a holistic security architecture.

Microsoft IIS Configurations

This section includes the specific security configuration recommendations.

1. Implement Microsoft IIS Security

Recommendation	Implement Microsoft IIS security best practices
Rationale	The Microsoft IIS security best practices should be implemented to help harden the underlying IIS infrastructure that the Bromium Dashboard runs on top of.
Implementation	The Microsoft IIS security best practices can be found at the NIST National Vulnerability Database. The latest configuration checklist can be found here: https://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=613 .

2. Require SSL Connections

Recommendation	Configure IIS to only accept SSL connections.
Rationale	Connections to the Bromium Dashboard include administrator logins. As a result, these connections should be protected using SSL to ensure that administrator passwords are not sent in plain text.
Implementation	Not Bromium Specific

3. Configure IIS Service Account Permissions

Recommendation	Configure the IIS service account with the necessary user right assignments needed to run the IIS service.
Rationale	In a locked down server environment, AD service accounts may not have the necessary user right assignments to correctly run IIS. The necessary user right assignments should be added to ensure proper functionality while maintaining a secure configuration.
Implementation	<p>The following user right assignments should be added to the service account used to run IIS for the Bromium Dashboard:</p> <ul style="list-style-type: none"> • Allow log on locally • Impersonate a client after authentication • Logon as a service • Logon as a batch job

Microsoft SQL Server Configurations

This section includes the specific security configuration recommendations.

1. Implement Microsoft SQL Server Security

Recommendation	Implement Microsoft SQL Server security best practices.
Rationale	The Microsoft SQL Server security best practices should be implemented to help harden the underlying SQL Server infrastructure that the Bromium Dashboard leverages to store configuration and alert data.
Implementation	The Microsoft SQL Server security best practices can be found at the NIST National Vulnerability Database. The latest configuration checklist can be found here: https://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=700

2. Configure SQL Database Service Account Permissions

Recommendation	Configure the account used (IIS service account) to connect to the Bromium SQL database with the necessary SQL permissions.
Rationale	In a locked down server environment, the accounts used to connect to a SQL database may not have the necessary database permissions. The service account used to connect to the Bromium database requires specific permissions to operate successfully.
Implementation	The following roles and schemas should be applied to the service account used to connect to the Bromium database: <ul style="list-style-type: none"> • Allocated the Public Role • Assigned all roles on the Bromium DB except db_denydatareader and db_denydatawriter • Owns all Schemas on the Bromium DB except db_denydatareader, db_denydatawriter, and guest

Bromium Dashboard Configurations

Overview

The Bromium Dashboard (Bromium Controllers) have several configurations that should be implemented to ensure that the servers are properly configured.

Configurations

This section includes the specific security configuration recommendations.

1. Create Complex Password

Recommendation	Create a complex password for the root administrator account
Rationale	After installing the Bromium Controller, an administrator will be asked to configure a root admin account that is stored in the SQL DB. This account does not have a technical password complexity requirement, but based on NIST guidelines, this password should contain a combination of upper case, lower case, numbers, and special characters. Bromium also recommends a minimum length of 12 characters.
Implementation	This account is created when the Bromium Controller is first installed and configured. An additional root admin account can be added without logging into the dashboard using the following procedure: <ol style="list-style-type: none"> 1) Run the Bromium Dashboard Controller Settings Configuration Wizard 2) On the left hand pane, select <i>Database Settings</i> 3) Check the box for and <i>Request new administrator user</i> and click save 4) A <i>Create Admin User</i> dialog box will then appear. 5) Enter in the desired username and password and click <i>Create</i>. 6) Click ok on the <i>Settings Saved</i> dialog box that then appears. 7) The root admin account will then be created and can be used to log into the Bromium Dashboard.

2. Enable AD Authentication

Recommendation	Enable AD authentication for administration
Rationale	The Bromium Dashboard supports AD authentication for administrative access based on both AD accounts and/or AD security groups. AD authentication should be enabled to allow enterprise enforced management of administrative user accounts and passwords.
Implementation	AD authentication can be enabled by performing the following steps: <ol style="list-style-type: none"> 1) Log into the Bromium Dashboard with an administrator account 2) Click on the <i>Settings</i> drop down arrow and then select either <i>Users or User Groups</i> (based on desired configuration). 3) In the top right pane, click on <i>User Options</i> and then select <i>Add User or Add User Group</i> (based on desired configuration) 4) On the <i>Settings</i> page, select the <i>Active Directory</i> radio button for the <i>Authenticate against</i> option. 5) If an AD connection has been previously configured, select the connection from the drop down options and click <i>Add</i> after all of the information has been filled out. If an AD connection has not previously been configured, proceed to Step 6. 6) If an AD connection has not been configured, click on <i>Create New Connection</i>. 7) Specify the FQDN or IP address of the desired Domain Controller.

	<p>8) A username and password is required if the IIS service account does not have permissions to query the configured Domain Controller.</p> <p>9) For <i>Security</i>, select the desired security option. Simple should not be chosen unless configuring in a lab or test environment.</p> <p>10) After specifying the information, click <i>Test Connection</i> and then <i>Save Connection</i>.</p> <p>11) After all of the information has been entered, you can create the desired User or User Group account.</p>
--	---

3. Set up Role Based Access Control

Recommendation	Implement role based access control (RBAC) to explicitly limit permissions to the necessary user and/or user groups.
Rationale	Leveraging RBAC ensures that administrators only have the permissions and access required to perform their necessary job functions which helps reduce the risk associated with having numerous administrators with high level permissions.
Implementation	<p>RBAC can be configured by performing the following steps:</p> <ol style="list-style-type: none"> 1) Log into the Bromium Dashboard with an administrator account 2) Click on the <i>Settings</i> drop down arrow and then select <i>Roles</i> 3) In the top right pane, click on <i>User Options</i> and then select <i>Add Role</i> 4) Specified the desired permissions by selecting the corresponding check boxes and then click <i>Add Role</i>. 5) The configured role can then be applied to a user group which contains the desired set of users for the configured permissions.

4. Add a Syslog Destination Server

Recommendation	Add a syslog destination server for the Bromium Dashboard.
Rationale	A syslog destination server should be configured to ensure that all Bromium generated events including security alerts are stored/archived on a separate server outside of the Bromium environment for data integrity and availability purposes.
Implementation	<p>Syslog can be configured by performing the following steps:</p> <ol style="list-style-type: none"> 1) Log into the Bromium Dashboard with an administrator account. 2) Click on the Events drop down arrow and then select Destinations. 3) In the top right pane, click on <i>Add Syslog Destination</i>. 4) Specify the desired syslog server information and the desired alert levels. 5) When finished, click <i>Save</i>.

5. Archive History.log File

Recommendation	Archive the history.log file generated by the Bromium Dashboard servers.
Rationale	The history.log file contains all server history including client check-ins, administrator logins, policy changes, etc. Archiving this file ensures that environment audit requirements can be met.
Implementation	<p>The history.log file location is configured when the Bromium Controller is installed. It is called the <i>Logs Directory</i> in the configuration wizard. The default location is %ProgramData%\Bromium\BMS\Loggs.</p> <p>This file should be continuously archived using a SIEM or archived at regular intervals using a Windows Scheduled Task or other means.</p>

Bromium Secure Client Policy Configurations

Overview

The table below contains the recommended configurations for the client side configurations for the Bromium Secure Client.

Configurations

This section includes the specific security configuration recommendations.

1. Implement the Baseline Bromium Secure Client policy.

Recommendation	Implement the standard baseline Bromium Secure Client policy as a starting point for policy configuration.
Rationale	The baseline policy includes the best practice configurations that a majority of Bromium customers implement. In some cases, these best practice configuration may differ from default settings.
Implementation	<p>The baseline Bromium policy can be configured by performing the following steps:</p> <ol style="list-style-type: none"> 1) Use the attached/included Bromium policy file. 2) Log into the Bromium Dashboard with an administrator account. 3) Click on <i>Policy</i> in the left hand pane. 4) In the top right pane, click on <i>Add Policy</i> and then <i>Import Policy</i> 5) Specify the location of the Bromium policy XML file and click Import. 6) Provide a name for the policy and desired groups to apply the policy to and click Save and Deploy. <p>Note: Additional details on the configured advanced parameters can be found in Appendix A.</p> <p>Note: This policy requires additional configurations as detailed below and should be used as a starting point for policy configuration. If there is a question about a specific configuration, please refer to the Bromium documentation or contact Bromium Technical Support for additional information.</p>

2. Configure Trusted Websites

Recommendation	Specify the trusted websites which should open up natively.
Rationale	Certain enterprise websites such as GoToMeeting and AdobeConnect require access to the host workstation (screen sharing, microphone, etc..) to function properly. These enterprise applications typically do not pose significant risk to the enterprise and should be added to the trusted sites list for proper functionality.
Implementation	<p>Trusted websites can be configured by performing the following steps:</p> <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Web Browsing policy tab 3) Specify the <i>Trusted websites</i> 4) Click Save and Deploy after configuring.

3. Configure Bromium Recommended Trusted Websites

Recommendation	Configure the Bromium recommended trusted website feature.
Rationale	This feature allows customers to trust a small subset of common business websites recommended and maintained by Bromium which can simplify deployment efforts versus managing an individual trusted sites list.
Implementation	Bromium Recommended Trusted Websites can be configured by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Web Browsing policy tab 3) Check (or uncheck the box) for <i>Trust sites recommended by Bromium?</i> 4) Click Save and Deploy after configuring.

4. Configure Intranet

Recommendation	Specify the intranet sites that represent the internal enterprise network.
Rationale	Enabling network isolation and specifying the intranet sites prevents untrusted micro-VMs from accessing these resources at the network level. This creates a network firewall protecting the trusted enterprise intranet from untrusted internet activity.
Implementation	Intranet can be configured by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Web Browsing policy tab 3) Confirm that Allow network isolation is enabled (checked) 4) Specify the enterprise intranet using both domain (*.company.net) and netblocks (10.0.0.0/8). 5) Click Save and Deploy after configuring.

5. Specify Administrative MIME Types

Recommendation	Specify the MIME types which require administrative privilege to trust.
Rationale	Executable MIME types such as .exe, .msi, .hta, .ps1, etc... should be added to ensure that only users with local administrative privileges on their workstation are able to trust and execute executable MIME types that are downloaded or saved from an ingress application. At a minimum the following MIME types should be present: .exe, .msi, .bat, .cmd, .vbs, .js, .ps1, .wsf, .hta, .scr, .vbe, .jse, .py, .chm, .dll, .com, .cpl, .msp, .reg, .iso, .vhd, .vhdx.
Implementation	Administrative MIME Types can be configured by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Documents policy tab 3) Add the desired MIME types to the <i>File types requiring administrative privilege to trust</i> setting. 4) Click Save and Deploy after configuring.

6. Specify Trusted MIME Types

Recommendation	Specify the MIME types which should automatically be trusted.
Rationale	Numerous MIME types that are commonly used such as .jpg and .gif typically pose little security risk due to the simplicity of the file format and the type of data that it is able to contain. As a result, Bromium typically recommends the following MIME types be automatically trusted: .jpg, .png, .gif, .bmp, .tif. However some customers may choose to add or remove additional MIME types based on their specific security and end user requirements.

Implementation	<p>Trusted MIME Types can be configured by performing the following steps:</p> <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Documents policy tab 3) Configure the desired MIME types in the <i>File (MIME) types to automatically trust</i> setting. <p>Click Save and Deploy after configuring.</p>
-----------------------	--

7. Configure Outlook Email Attachment Policy

Recommendation	Configure the desired Microsoft Outlook email attachment policy.
Rationale	<p>The default Outlook email attachment behavior is that all supported email attachments are considered untrusted. However, in many cases, it may be acceptable and preferred to not open all attachments in a micro-VM (such as internal trusted email).</p> <p>There are two important configurations when configuring the desired email attachment policy. These email configurations support Microsoft Outlook using Microsoft Exchange Server.</p> <p>The first is specifying the list of “trusted” email domains. This is typically the internal email domains for an organization.</p> <p>The second configuration is the email attachment security level. This advanced parameter (Untrusted.OutlookAttachmentSecurityLevel) has two common configurations that are as follows:</p> <ol style="list-style-type: none"> 1) Trusting attachments sent from the trusted domain list if the sender has Bromium Isolation running (default setting). 2) Trusting attachments sent from the trusted domain list regardless of whether sender has Bromium running. <p>The standard recommendation is to specify the trusted email domains and use the default setting for the Outlook Attachment Security Level. However, in some cases, customers may choose to trust all internal email even if the sender does not have Bromium running on their workstation to reduce the number of micro-VMs created for email attachments.</p> <p>The default value (option 1) for Untrusted.OutlookAttachmentSecurityLevel = 2. The value for option 2 for is Untrusted.OutlookAttachmentSecurityLevel = 4.</p>
Implementation	<p>Email Policy can be configured by performing the following steps:</p> <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Documents policy tab 3) Add the desired trusted email domains to <i>Trusted internal email domains</i>. <p>Click Save and Deploy after configuring.</p> <p>If modifying the Outlook Attachment Security Level, an advanced parameter should be created for Untrusted.OutlookAttachmentSecurityLevel and the policy should then be saved.</p>

8. Configured Desired Clipboard Policy

Recommendation	Configure desired clipboard policy based on security requirements.
Rationale	The default clipboard policies are typically deployed in customer environments. However, some customers have use cases which require a stricter clipboard policy. In these cases, the clipboard policy should be configured based on the security and end user requirements.
Implementation	Clipboard policy can be configured by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Documents policy tab 3) Configure the <i>Clipboard access policy</i> and <i>Clipboard data protection</i> policy as desired. 4) Click Save and Deploy after configuring. <p>Note: Additional information on the specific settings for the clipboard policy can be found in the Bromium Deployment Guide.</p>

9. Enable Bromium Threat Intelligence

Recommendation	Enable Bromium Threat Intelligence.
Rationale	Bromium Threat Intelligence allows Bromium to automatically check if an executable flagged as being suspicious is a known good or known bad file based on its MD5. Enabling this feature helps reduce false positives for known good files such as trusted third party software and provides additional information for known bad files. No customer sensitive data is transmitted or kept when using this feature. <p>Additional Information on Bromium Threat Intelligence can be found here: https://support.bromium.com/s/article/ka10B000000bpe8QAA/Bromium-Threat-Cloud</p>
Implementation	Bromium Threat Intelligence can be configured by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Security policy tab 3) Check (or uncheck) the <i>Enable Bromium Threat Intelligence</i> setting. 4) Click Save and Deploy after configuring.

10. Configure Alert Behavior

Recommendation	Configure the desired alert behavior if a Bromium protected VM generates a security alert based on the behavior of the application.
Rationale	Most enterprises chose to <i>Continue operation silently</i> if an alert is generated in a protected VM as the user and the enterprise is still protected due to the hardware enforced isolation and alerting users can cause increased help desk tickets. However, some organizations may choose to stop the operation and/or alert the user based on their specific security and end user requirements.
Implementation	Alert behavior can be configured by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Security policy tab 3) Select the desired behavior for the <i>Alert user on LAVA event</i> setting. 4) Click Save and Deploy after configuring.

11. Add Product License Keys

Recommendation	Add your customer specific product license key to ensure proper product functionality.
Rationale	A Bromium generated license key is required for Bromium Secure Platform to function properly.
Implementation	The license key can be added by performing the following steps: <ol style="list-style-type: none"> 1) Browse to the desired policy in the Bromium Dashboard 2) Select the Manageability policy tab 3) Add the <i>Product license key</i> 4) Click Save and Deploy after configuring.

12. Leverage Protected Application GPOs

Recommendation	Implement security best practices for protected applications such as Microsoft Office, Adobe Reader, Internet Explorer, and Google Chrome.
Rationale	Bromium Secure Platform protected applications honor a majority of application specific GPOs. For instance, the Microsoft Office and Google Chrome secure baseline policy settings are typically honored in a Bromium protected VM.
Implementation	Not Bromium specific

Appendix A: Baseline Policy Advanced Parameters

Overview

This section discusses the behaviour and uses cases for the pre-configured advanced parameters and the security and/or performance benefits associated with the configuration.

Configurations

This section includes the specific advanced parameters that are recommended and the corresponding configuration and explanation.

Setting	Browser.Firefox.UsePersistentCache
Value	0
Explanation	Disabling browser caching can improve browser performance in a majority of use cases where users have access to a reliable internet connection.

Setting	Browser.IE.UsePersistentCache
Value	0
Explanation	Disabling browser caching can improve browser performance in a majority of use cases where users have access to a reliable internet connection.

Setting	Browser.IE.UsePersistentCacheOnWin10OrLater
Value	0
Explanation	Disabling browser caching can improve browser performance in a majority of use cases where users have access to a reliable internet connection.

Setting	Browser.UseWebCache
Value	0
Explanation	Disabling browser caching can improve browser performance in a majority of use cases where users have access to a reliable internet connection.

Setting	Containment.EnableIntranetDetection
Value	1
Explanation	Enable's automatic intranet detection for Bromium devices. If a device is determined to be on the intranet, Bromium will honor the intranet site list.

Setting	Browser.OpenTrustedSitesAndNetblocksInVMWhenNotOnIntranet
Value	0
Explanation	Continues to allow trusted sites and trusted netblocks to open natively when not on intranet.

Setting	MimeHandler.Default.TrustFile
Value	3
Explanation	A value of 3 will perform a mime validation check before trusting a file.

Setting	MimeHandler.Zip.TrustLevel
Value	0
Explanation	A value of 0 allows administrators to trust an entire zip file, but not regular users. However the contents of the zip file can be extracted and each file individually trusted.

Setting	BEM.MinimumUpdateInterval
Value	120
Explanation	Configures the update interval for the upload of Bromium Host Monitoring alerts.

Setting	BEM.UpdateInterval
Value	900
Explanation	Configures the check-in interval for the Bromium Host Monitoring feature.

Appendix B: Antivirus Exclusions

Overview

Antivirus and other third-party security tools can provide security to workstations by scanning for the presence of malicious or potentially malicious files and activity. However, in many cases, the continuous scanning of known trusted files can cause performance and stability issues with other products. Bromium recommends several exclusions be implemented to support Bromium Secure Platform. Without these exclusions in place, Bromium engineering has seen several issues arise in production customer environments including but not limited to slower website rendering, slower opening of untrusted documents, and reduced network throughput.

In general, these exclusions should be implemented with all security products including but not limited to Symantec Endpoint Protection, McAfee Virus Scan, McAfee HIPS, Digital Guardian, and Trend Micro. As with all exclusions, customers should evaluate the benefit versus the potential risk when implementing these exclusions. With that being said, Bromium has seen significant improvement in the performance of customer environments when these exclusions have been implemented.

Depending on the security program, additional configurations may be required; however, the baseline configurations below should work for a majority of use cases. Additional exclusions may also be needed for future versions of Bromium Secure Platform as additional features are added.

Configurations

This section includes the specific antivirus exclusions that should be implemented to improve the performance and stability of the endpoint devices.

For an easier configuration, the following directories can be excluded:

Executables and Processes	
%userprofile%\AppData\LocalLow\Bromium	%programfiles%\Bromium
%userprofile%\AppData\Local\Bromium	%programdata%\Bromium

For higher security environments that prevent the exclusion of folder directories, Bromium recommends the following processes/executables to be explicitly excluded:

%ProgramFiles%\Bromium\vsentry\servers		
ax_installer.exe	BrHostDrvSup.exe	BrRemoteMgmtSvc.exe
BrAxService.exe	BrHostSvr.exe	BrService.exe
BrDesktopConsole.exe	BrInstaller.exe	BrStatusMonitor.exe
BrConsole.exe	BrManage.exe	
BrExeScanner.exe	BrRemoteManagement.exe	

%ProgramFiles%\Bromium\vSentry\bin		
Br-init-a.exe	Br-init-o.exe	uxenctx.exe
Br-init-c.exe	Br-init-w.exe	uxendm.exe
Br-init-l.exe	Br-uxendm.exe	
Br-init-n.exe	uxenctl.exe	

%ProgramFiles%\Bromium\BEM\bin		
BemAgent.exe	BemMan.exe	BemSvc.exe

Appendix C: Baseline Policy

Overview

The policy included in this section is the recommended baseline policy for standard customer deployments. This policy can be copied and pasted into an xml file and then imported into the Bromium Dashboard using the instructions provided in the Bromium Secure Client Policy Configuration section.

Configurations

The policy in Table 1 includes the recommended configurations for the baseline Bromium policy.

```
<root><vSentry>
  <key name="MimeHandler.Winword.InstalledOnHost">-1</key>
  <key name="Untrusted.Editing.Enabled">1</key>
  <key name="MimeHandler.Zip.TrustLevel">0</key>
  <key name="Untrusted.OutlookAttachmentTrustLevel">0</key>
  <key name="UserInteraction.UILevel">1</key>
  <key name="MimeHandler.Acrobat.EscapeOut">7</key>
  <key name="Untrusted.ClipboardPolicy">3</key>
  <key name="Untrusted.NativeIESettingIEDDownloadedFileTrustLevel">1</key>
  <key name="Browser.ChromeShouldExtractIcon">1</key>
  <key name="Browser.IEAdBlock">1</key>
  <key name="Browser.IE">1</key>
  <key name="Browser.TrustSitesInIETrustedZone">0</key>
  <key name="MimeHandler.Custom1.TrustLevel">0</key>
  <key name="Untrusted.TrustDrivePermissionsRequired">1</key>
  <key name="Reporting.Enabled">0</key>
  <key name="MimeHandler.Other.EscapeOut">2</key>
  <key name="Containment.EnableIntranetDetection">1</key>
  <key name="BEM.Search.ExtractSearchData">0</key>
  <key name="Untrusted.TrustedSMTPDomains" />
  <key name="LCM.DeferrableTemplateCreationPolicy">4</key>
  <key name="BEM.MonitorActivity">0</key>
  <key name="LAVA.Cloud">1</key>
  <key name="Untrusted.FileSystems">1</key>
  <key name="Browser.TrustedSites" />
  <key name="Untrusted.ShowUntrustedFileIcons">0</key>
  <key name="Browser.TreatIEIntranetZoneAsIntranet">0</key>
  <key name="Untrusted.UntrustWebDavShares">0</key>
  <key name="MimeHandler.Powerpnt.InstalledOnHost">-1</key>
  <key name="LAVA.Cloud.WebConfiguration.Trusted.Enable">0</key>
  <key name="Untrusted.UnsupportedApplicationVersions.EscapeOutAllFiles">1</key>
  <key name="Untrusted.DisplaySecureViewRibbon">0</key>
  <key name="MimeHandler.Script.BackgroundLavaCheck">1</key>
  <key name="BEM.UpdateInterval">900</key>
  <key name="vSentry.ProductLicenseKeys" />
  <key name="MimeHandler.Zip.EscapeOut">7</key>
  <key name="Browser.ProductName">Chromium</key>
  <key name="Security.MalwareManifest">1</key>
  <key name="Quarantine.Enabled">0</key>
  <key name="MimeHandler.Executable.BackgroundLavaCheck">1</key>
  <key name="Containment.Enabled">1</key>
  <key name="Untrusted.WarnUserOnAttemptToTrustFile">1</key>
```

```

<key name="Security.DetailedView">1</key>
<key name="vSentry.AllowDisableFromConsole">1</key>
<key name="Containment.DisplayContainmentErrors">0</key>
<key name="MimeHandler.Excel.InstalledOnHost">-1</key>
<key name="Browser.CheckDefaultBrowser">0</key>
<key name="Browser.CloudSaaSites" />
<key name="Browser.IntranetSites">192.168.0.0/16,172.16.0.0/12,10.0.0.0/8</key>
<key name="MimeHandler.Custom0.EscapeOut">2</key>
<key name="ShowPrintConfirmDialog">0</key>
<key name="MimeHandler.Custom0.FileTypes">.jpg,.png,.gif,.bmp,.tif</key>
<key
name="MimeHandler.Custom1.FileTypes">.exe,.msi,.bat,.cmd,.vbs,.js,.ps1,.wsf,.hta,.scr,.vbe,.jse,.py,.chm,.dll,.com,.cpl,.msp,.reg,.iso,.vhd,.vhdx</ke
y>
<key name="Browser.Firefox">-1</key>
<key name="Browser.Firefox.UsePersistentCache">0</key>
<key name="Untrusted.PersistDriveTrustState">1</key>
<key name="Browser.TrustIntranetSites">1</key>
<key name="Security.FullForensics">1</key>
<key name="MimeHandler.Photoviewer.EscapeOut">7</key>
<key name="Browser.TemporaryTrust.Mode">0</key>
<key name="Untrusted.Enabled">1</key>
<key name="LAVA.Enabled">1</key>
<key name="Browser.UseWebCache">0</key>
<key name="vSentry.AllowUntrustedAccessDuringInitialization">1</key>
<key name="Browser.OpenTrustedSitesAndNetblocksInVMWhenNotOnIntranet">0</key>
<key name="MimeHandler.Executable.EscapeOut">7</key>
<key name="Log.RemoveSensitiveInformation">0</key>
<key name="Browser.IE.UsePersistentCacheOnWin10OrLater">0</key>
<key name="Clipboard.FormatsPolicyVM2Host">0</key>
<key name="MimeHandler.Default.BackgroundLavaCheck">1</key>
<key name="Browser.IE.UsePersistentCache">0</key>
<key name="MimeHandler.Default.TrustFile">3</key>
<key name="BMS.UpdateInterval">900</key>
<key name="MimeHandler.Default.TrustLevel">0</key>
<key name="Untrusted.IngressApplications">"Microsoft Internet Explorer","Microsoft Edge","Microsoft Office Outlook",Skype,"Skype for
Business","Microsoft Office Lync","Google Chrome","Mozilla Firefox","Lotus Notes"</key>
<key name="UserInteraction.ShowTrayIcon">1</key>
<key name="Browser.Chrome">-1</key>
<key name="BEM.MinimumUpdateInterval">120</key>
<key name="BMS.IgnoreInvalidServerCertificate">0</key>
<key name="MimeHandler.Wmplayer.EscapeOut">7</key>
</vSentry></root>

```

Table 1

Appendix D: Client Certificate Authentication

Overview

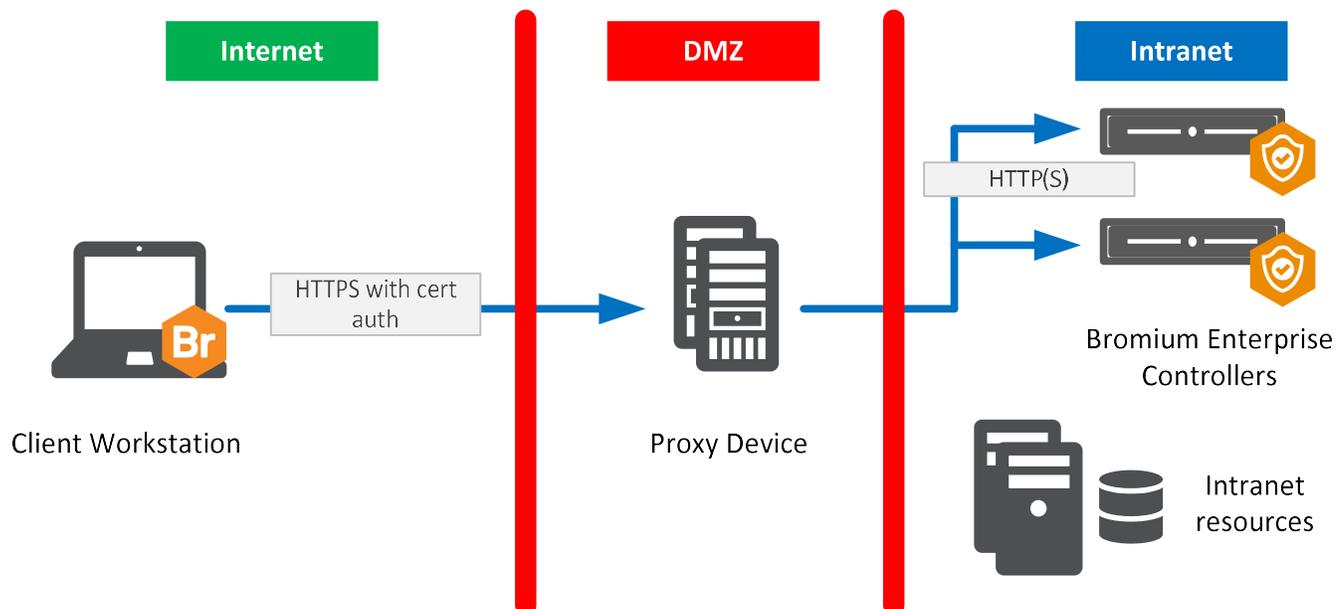
The purpose of this appendix is to explain how to implement client certificate authentication for the Bromium Dashboard. Client certificate authentication allows the Bromium Secure Platform clients to check-in securely while off of the corporate network without having to have a VPN connection. This method ensures that only devices with the properly configured and issued certificates are able to connect to the Bromium management infrastructure preventing rogue devices or agents from attempting to gain unauthorized access to the Bromium management infrastructure.

Configurations

There are two primary methods to configure client certificate authentication for the Bromium management infrastructure. The first method is to have the client certificate authentication to occur at a network proxy device (such as a Citrix NetScaler or F5 BIG-IP) before handing the connection to the Bromium dashboard. The other method is to configure the Bromium Controller server (which runs IIS) to handle the client certificate authentication itself. In both of these scenarios, additional consideration may be needed for the DNS configuration(s) to handle use cases where devices may move between being on the intranet and the internet.

Client Certificate Authentication at Proxy

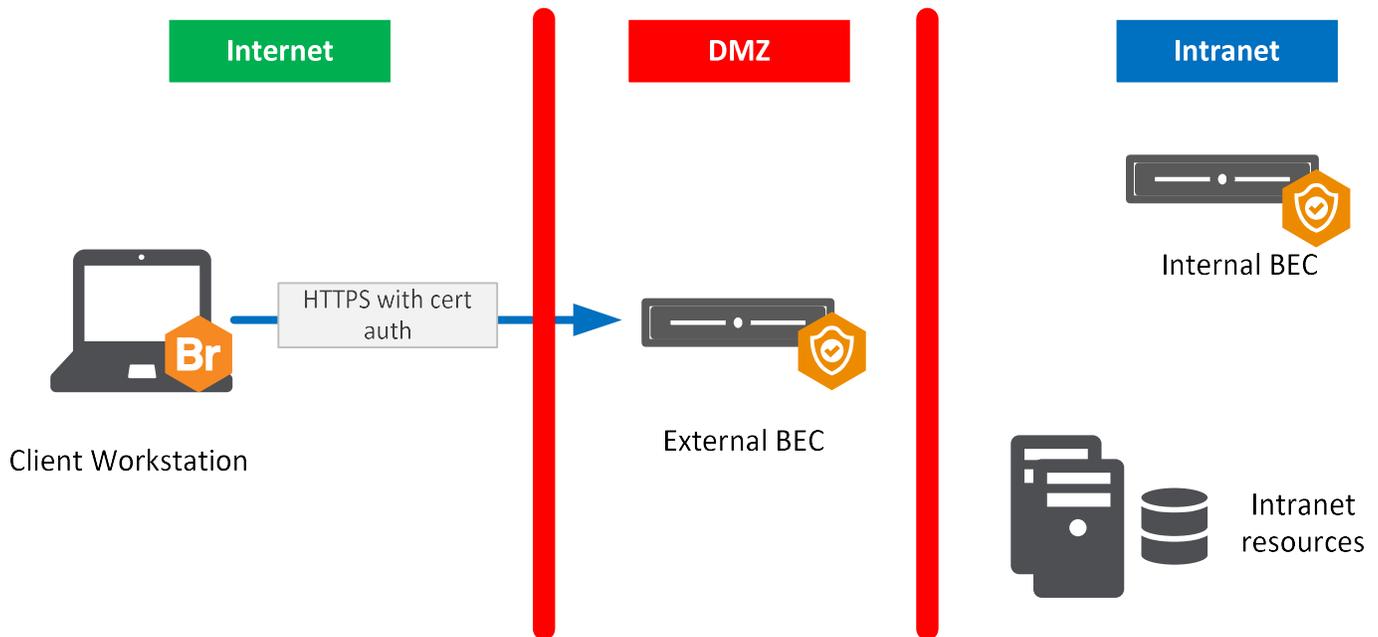
In this configuration, a proxy device (Citrix NetScaler, F5 BIG-IP, etc) is configured to require a client certificate before passing the connection back to the Bromium Controller servers. Typically, this proxy device is placed in the DMZ network for security purposes.



The configuration is typically considered the most secure as the only device that is located in the DMZ network is a dedicated network device. In addition, in this configuration, a device needs to successfully authenticate using its client certificate before accessing any of the Bromium Controller servers which are located on the internal network. This configuration is the Bromium recommended method for allow remote devices to connect without a VPN.

Client Certificate Authentication at Bromium Dashboard

In this configuration, a Bromium Controller(s) is placed in the DMZ network. IIS configurations are made to the Bromium dashboard to authenticate against a client certificate before allowing a network connection to be made. The Bromium Controller server located in the DMZ network is typically only used for devices connecting from the internet (or otherwise outside the internal network). A separate Bromium Controller would be used to handle internal connections. In addition, the Bromium server in the DMZ network will still need access to intranet resources such as its SQL database, network file shares, and Active Directory.



The primary benefit of this configuration is that it does not require an additional network device to proxy the connection and perform the client certificate authentication. In addition, the authentication against a client certificate occurs in the DMZ network ensuring that non authorized client devices do not gain access to intranet resources.

Additional information on how to implement and configure client certificate authentication for the Bromium Dashboard can be found in the *Bromium Secure Platform Deployment Guide*.