Bromium®

Bromium Secure Platform

4.0 Update 2

Installation and Deployment Guide

Notices

Bromium Secure Platform 4.0 Update 2

09/25/2017

Preface

About This Guide

This guide describes how to manage the Bromium Secure Platform.

Audience

The intended audience for this document is IT professionals with an understanding of networking, databases, and systems management.

Conventions

This guide uses the following typographical conventions and icons:

Bold	Function or label in the interface
`Courier`	Code sample, command name, text string, file name
Note:	Important information

Finding Product Documentation

Bromium end-user documentation and white papers are available at https://my.bromium.com. Contact your Bromium sales representative for login credentials.

Getting Help

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

- Go to https://support.bromium.com. If you do not have an account, contact your Bromium Sales representative or Support.
- Email questions to support@bromium.com
- Call Bromium Customer Support at 1-800-518-0845
- Call your technical account representative directly

To provide more information about your issue, you can create an error report before opening a ticket with Bromium Support. Click  in the taskbar, select **Open Desktop Console**, click **Support > Send Report**, and confirm.

Feedback

To provide feedback on this documentation, you can send an email to documentation@bromium.com.

Contents

1 Predeployment Planning

This section describes requirements and guidelines to set up a new Bromium deployment.

Note: Ensure that system patches (such as Microsoft updates) are applied and tested before Bromium is deployed to endpoints and put into production environments.

Bromium Platform Requirements

Check that the systems on which you are installing the Bromium platform meet the following requirements:

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 RAM 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, 8.1, or 10 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) **Note:** 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) Microsoft Windows 10 Creators Update and earlier, 64-bit (Professional, Enterprise)

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. For more information, see the `Browser.IEMetro.EnableIEHelperHook` setting in Browser Settings.

- 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 3.5.1 (pre-installed with Windows 7)
- Microsoft .NET Framework 4.5 (pre-installed with Windows 8.1)
- 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 as needed:

- Local administrator privileges (if installing on specific machines for evaluation)
- Active Directory administrator privileges (if installing in the enterprise for production use)
- A Bromium license provided by your Bromium Sales or Customer Support representative, or use the built-in 21-day evaluation license
- To run Bromium in a virtualized environment using VMware, ESX 5.1 Update 1 or later is recommended

Supported Software

- Chromium versions 54, 55, 56, 58, 59, and 60 (32-bit versions), and version 60 64-bit
- Mozilla Firefox versions ESR 45 and 52 (32-bit versions)

  Note: If Firefox is already installed on endpoints and has not been launched previous 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.

  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.

- 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, x86 or x64:
  - 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 not supported.

- Microsoft Outlook 2010, 2013, and 2016
- Adobe Reader versions 9, 10, 11, DC Classic 2015, and DC Continuous 2015 and 2017
- 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 64-bit versions of Windows only

  Note: Virtualbox is not supported on endpoints running AMD processors

- Endpoints running virtualization-based security (VBS) is available in beta mode with the following configuration:
  - Windows 10 64-bit with virtualization-based security (VBS) and Hyper-V enabled
  - UEFI Secure Boot enabled
  - Intel vPro 4th generation Core (i3/i5/i7) and newer

Note: AMD processors are not supported in this release.

    - Trusted Platform Module (TPM) is recommended

Note: To use VBS, the **Lock Boot Order** setting must be disabled in the BIOS and the **Fast Startup** power option must be disabled.

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

Bromium software has been tested with the following third-party endpoint security product solutions in their standard configurations:

- 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

IMPORTANT: Ensure you create appropriate exclusions in the configuration of installed endpoint security products so that they do not interfere with or prevent the normal operation of isolation. Necessary actions may consist of excluding all Bromium processes and binaries from the third-party endpoint security product. The absence of exclusions may result in failed Bromium software initialization and slow or blocked browsing and opening of untrusted documents. For more information, see Third-party Product 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 (se-SV), all supported versions of Windows
- Italian (it-IT), Windows 10
- Brazilian Portuguese (pt-Br), Windows 10

Note: Isolation supports all Windows locales.

Monitoring Interval Setting

The `BEM.UpdateInterval` setting controls the frequency (in seconds) with which the endpoint communicates with the controller for regular updates (policy changes and so on.) It is recommended that this interval is set to `900` (seconds) to optimize CPU and network usage. You can add this setting in the controller in the policy Advanced tab.

Controller Requirements

Note: Before installing a new version of the controller, back up your current database.

Check that the systems on which you are installing the Bromium controller meet the following 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 HTTPS connections (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

Start the SQL Server Browser service if it is not already running on the SQL Server host. SQL

For IIS Server:

- The controller server must be the only HTTPS server running on the host system
- The controller server must be able to bind to both the HTTP port (80) and HTTPS port (443)

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) Microsoft .NET Framework 4.0
Storage Space	1 TB available space

File Sharing Requirements

A highly available network share with a minimum of 500 GB of free space should be provided as the controller uploads repository. This share can be hosted on a clustered Microsoft file server or a NAS device. The share must be accessible using Active Directory authentication from a domain trusted by the Controller server and it must use SMB 2.0 or higher as the protocol.

Identifying Trusted and Untrusted Resources

Bromium protects the sensitive trusted information and resources within your virtual perimeter from access by malicious exploits originating from websites and documents that users access from untrusted (risky) locations outside your perimeter. Web pages, downloads, and email attachments that originate from untrusted locations are executed within an isolated, disposable micro-VM.

Documents, attachments, web pages, and other information and resources originating from specified trusted locations execute in the native desktop and are not isolated. Additionally, access to the trusted data is blocked from untrusted websites and documents.

Define your trusted locations using one or more of the following methods during installation and initialization:

- Compile a list of AD/DNS domains comprising your intranet. Isolation blocks network access to these domains from untrusted web pages and documents. Websites located in these domains can be configured to be trusted and open on the system outside of isolation.
- Compile a list of IP address netblocks comprising your intranet. The IP address ranges entered for the netblocks should match and correspond to the list of AD/DNS domains. Isolation blocks network access to these netblocks from untrusted web pages and documents. Websites located at these IP address ranges can be configured to be trusted and open on the system without protection.
- Compile a list of DNS domains comprising your organization’s cloud and SaaS sites. Isolation blocks network access to these domains from untrusted web pages and documents, while still opening the cloud and SaaS sites in micro-VMs.

Evaluation Guidelines

Bromium recommends using physical machines to evaluate the software. Although isolation runs on hypervisors that support nested VT, it is not recommended to do so beyond performing technical evaluations. Unless isolation is running in a production environment, performance evaluations or conclusions about performance should not be drawn from Bromium products running in a nested VT evaluation environment.

Database and Network Usage Guidelines

Note: The following figures exclude data from threats. Changes in future versions of the Bromium platform may result in more or less information being stored, sent, and received than indicated in this topic.

Database Usage

Items that are factored into database usage include:

- Event data from endpoint to the controller server
- Configuration
- Policies
- State information per endpoint

Considering this information, the database is expected to grow by ~25,000 records per endpoint, per day when default settings are used. In addition to this figure, there is additional SQL overhead for indexes, logs, and so on that depends on your particular SQL deployment architecture.

Resource Usage

The following table lists the resources required by the Controller and SQL server based upon a given number of devices. Network traffic usage can be reduced by increasing the **Update Interval** setting in the policy Manageability tab page in the controller. Increase this interval to change how often Bromium checks devices for policy updates and remote commands. It is assumed that devices are configured with a 30-minute update interval.

Server	AVG IOPS / 10K Devices	Devices / 1 vCPU*	Devices / 1GB RAM**	Daily Trans Log per Device	Daily DB Growth per Device	BW per Device
Controller	25 IOPS	2,500	6,000	N/A	N/A	50 bps
SQL	50 IOPS	15,000	4,000	500 KB	5 KB	N/A

***** It is recommended that you configure SQL with four vCPUs and IIS with two vCPUs as a minimum, regardless of the number of devices.

****** 3 GB of additional RAM should always be added on top of the calculation to support the base OS and other services.

2 Installing Bromium Products Manually

You can install Bromium manually on each local system. Manual installation is ideal for evaluation and small-scale deployments, and does not require much setup time. Run the installer, provide some initial configuration information, and Bromium products are ready to use. You can install Bromium products using the installation wizard or in batch mode using the MSI from a command prompt.

Running the Installer

This topic describes how to run the Bromium installer (.msi) to manually install a single instance of the Bromium platform. Check that the target system is appropriately configured before running the installer.

Note: Do not install Bromium software from a USB drive. USB drives are untrusted by default and, when Bromium reaches the initialization stage, the installer will fail because it will no longer be able to read the installer data on the USB drive.

To install Bromium manually on a single local system:

1. Start the installer. Copy the installation file to the Windows system that will run the Bromium products.
2. Double-click the installation file.
3. In the setup wizard, click **Next**.
4. Accept the license agreement. Read the license agreement and select **I Agree**.
5. Click **Next**.
6. Enter or browse to the location in which you want to install the software. The default is `C:\Program Files\Bromium`
7. Enter the URL of the server on which you will run the controller. Click **Next**.
8. Click **Next** to begin platform installation.

   Bromium isolation and monitoring are installed.

   Note: If Microsoft Outlook is running, you are prompted to close it to continue with the installation.
9. To ensure isolation can operate correctly on the system, the installer checks that the system has a minimum set of resources before it installs Bromium software. Any issues are displayed in the Minimum Requirements window. If a check fails, correct the issue before proceeding.
10. Click **Finish** to complete installation and initialize isolation later in the Desktop Console. To initialize isolation immediately, click **Next** and then click **Next** again after initialization is complete.
11. To complete the installation, click **Close**.

Configuring Isolation with Oracle Virtualbox

To configure isolation with Oracle Virtualbox on systems running 64-bit versions of Windows, set the following msiexec parameter:
`GETCAPS=--no-strict-vbox-not-installed`

At run time, enter the following advanced settings in the controller:

- `IsolationOverrideDisabledChecks` using the value `vbox-not-installed`
- `LCM.TemplateInitOverrideDisabledChecks` using the value `vbox-not-installed`
- `XVM.CustomHypervisorArgs` using the value `hvmonoff=1`

After adding these settings, restart the machine.

Note: Virtualbox is not supported on endpoints running AMD processors

Configuring Isolation with McAfee DLP and Symantec DLP

To enable support for McAfee Endpoint version 9.3 and Symantec DLP version 14.0.1, add the following setting to your policy:

`Browser.DLPCheckMode = 1` (on) or `0` (off)

`Browser.DLPType = 1` (for McAfee DLP) or `0` (for Symantec DLP)

After you modify this setting, you must reinitialize isolation. To do this, use the **Reinitialize Isolation** remote command in the controller.

Installing Bromium Products Remotely

The **Install package** remote command in the Bromium controller allows you to install or upgrade the Bromium platform on multiple devices.

1. In the controller, open the **Devices** page (to run the remote command on individual devices) or the **Device Groups** page (to run a command on device groups) page.
2. Select the device(s) or device group(s) on which you want to run the command.
3. Click **Remote Management** and select **Install package**.
4. Enter the installation MSI location (and optionally the SHA-1 hash.)

   An HTTP/S server or a file share can host the MSI. file:// URLs cannot be used for local paths; they can be used only as equivalent of UNC paths, that is \\some-computer\share\file.msi can be written as file://some-computer/share/file.msi. The FQDN of the host (including its share) can be used.

   The SYSTEM account on the controller machine must have permission to access the fileshare in which the MSI package resides. The SYSTEM account (not the account of the logged in user) is used when the isolation client downloads the package from the network share.

5. Click **Send Command**. A confirmation message is displayed and the remote command is queued until the next time updates are obtained from the controller.

Troubleshooting Remote Installations

Expand the Devices menu and click **Remote Commands** to view a table of commands that have been issued. The Breakdown column displays a red bar to indicate any failed commands. Click the command to view more information about the failure.

Installing App Packs

When some third-party software such as Windows and Firefox are updated, App Packs are required to allow the updated applications to run in micro-VMs and to update the version of Chrome available for isolation (Chromium.) Your Bromium account representative will inform you when App Packs become available or you can check the Bromium Support site at https://support.bromium.com for updates. These .msi files can be deployed manually using SCCM, or using the **Install package** remote command in the controller (see Installing Bromium Products Remotely.)

Installation and Initialization Checks

Bromium checks that your system meets certain requirements before installing and initializing the software. The following table lists each check that Bromium performs and what happens to the installation or initialization process if the check does not pass:

- Fails - Installation or initialization does not finish
- Warns - Installation or initialization finishes but issues a warning that you must correct the condition
- N/A - The check is not performed or the result does not impact the process

If this check fails	Install	Initialization
Check if the CPU is an AMD CPU and if the CPU family is unsupported	Warns	N/A
Check if processor supports Virtualization Technology	Warns	Fails
Check if sufficient RAM is available	Warns	Fails
Check if sufficient disk space is available	Fails	Fails
Check if supported versions of Windows are running	Fails	N/A
Check if Windows 7 Service Pack 1 is installed	Fails	N/A
Check that Virtualbox is not installed	Warns	Fails
Check if VT is enabled in BIOS	Warns	Fails
Check if hardware supports Physical Address Extension	Warns	Fails
Check if Physical Address Extension enabled in BIOS	Warns	Fails
Check if NX is enabled in BIOS	Warns	Warns
Check if processor supports Extended Page Tables	Warns	Fails
Check if required applications are installed	Warns	N/A
Check if optional applications are installed	Warns	N/A
Check if supported applications are installed	N/A	N/A
Check if components required for Microsoft Office are installed	Warns	Fails
Check if Microsoft Office has been activated	Warns	Warns
Check the version of Microsoft Office installed	Warns	Warns
Check if Microsoft .Net 3.5 or 4.0 is installed	Warns	N/A
Checks for minimum number of CPU cores required (two)	Warns	N/A
Checks for VSS service to be running	Warns	Warns

If this check fails	Install	Initialization
Checks for MS Shadow Copy Provider service enabled	Warns	Warns
Checks if EMIE can be safely supported	Warns	N/A
Checks if Google Chrome Frame is installed	Warns	N/A
Checks if required Windows Updates are installed	Warns	Fails
Checks if required Windows languages are available	Warns	Fails
Checks for mismatch between kernelbase DLL and MUI files	Warns	Fails
Checks if 32-bit or 64-bit Windows is present	Fails	Fails

Initialization Overview

Initialization creates a *template* that includes particular settings specific to the user. Templates create a snapshot of applications that are protected by isolation to create a micro-VM. On shared systems where different users have different settings (for example DPI or language settings), multiple templates are created. The template becomes obsolete if one of the protected applications is upgraded to a newer version or other major configuration changes are made, because the older application in the template is still used to create the micro-VM.

Creating and Updating Master Templates

If isolation is preinstalled as part of a master image, it is important to perform an initialization prior to sealing and deploying the master image. When updates are applied to the master image, reinitialization may be required. It is important to ensure that the master image has a successful and complete initialization performed before it is deployed.

To create the initial master image or update an existing master image:

1. Use or create a "typical" user account with commonly used settings (group policy settings, policies, and so on.) This ensures that a template is created with the correct settings for your typical users. Log in to this account to create the master template.
2. Stop the Remote Management Service.
3. Close the `BrConsole.exe` process.
4. Remove the unique ID from the registry that identifies the installation within the controller. Delete the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Bromium\vSentry\State\BMS.ClientToken`

Some of these actions can be placed into scripts that can be run immediately prior to sealing and capturing the image. For example:

```
net stop "Bromium vSentry Remote Management Service"

taskkill /F /T /IM "BrConsole.exe"

reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Bromium\vSentry\State\BMS.ClientToken
```

Isolation Initializations

There are two types of initializations: critical and deferrable. A critical initialization means there is no usable template available and a new one is created immediately while the user is using the client device (unless otherwise configured in the advanced settings.) A deferrable initialization means there is a template, but it is not ideal (for example, if it has an outdated version of Flash.) In this case, a new template is created during idle-time, when the user is not at their machine, subject to the `LCM.DeferrableTemplateCreationPolicy` setting.

If you update any application supported by isolation, isolation must reinitialize or micro-VMs will continue to use the previous application version. Bromium monitors the changes in installed applications and automatically reinitializes if a change is detected.

Some common conditions that trigger reinitialization include:

- A logged in user starts reinitialization from the Desktop Console or command line
- A request for reinitialization from the controller
- Isolation detects that an installed application has been removed, added, or updated
- Changes to certain configuration parameters
- Microsoft Office becomes licensed or unlicensed
- Change of DPI
- Certain plug-ins
- Changes to Windows locale settings
- Installing or uninstalling Microsoft Office language packs
- Change of machine, system install, user default language
- Changes to Adobe Reader language settings

Using Sysprep With Isolation

Microsoft Sysprep works seamlessly with isolation; VM images prepared with Sysprep can be cloned as normal. Isolation system templates and user templates are still present after the Sysprep process, and can be reused when users log in after the machine on which Sysprep has been run is added back to the same domain.

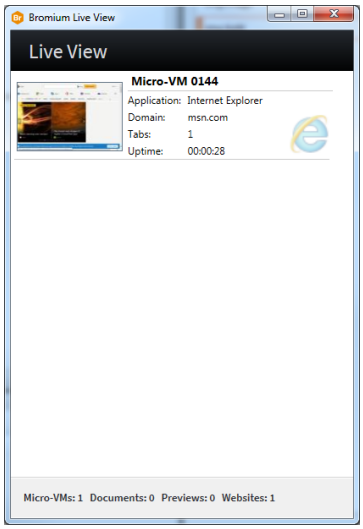
Verifying the Deployment

If installation or initialization fails, see Installation or Initialization Failures.

If installation and initialization finish without any problems, perform the following tests after initialization completes:

1. In the Start menu, click **Bromium Desktop Console** or in the taskbar, right-click  and select **Open Desktop Console**.
2. Click **Live View**. The **Bromium Live View** window is displayed.

   This window provides a view of the micro-VMs running on the system. Initially, this list will be empty.
3. Open an Internet Explorer browser window.
4. Verify that a new micro-VM is displayed in the Live View:

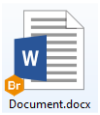


5. Navigate to one of the intranet sites that you configured during installation.

   Intranet sites are trusted and are opened on the host outside of isolation. A new micro-VM for a site will not be displayed in the Live View if the trusted site was configured properly.

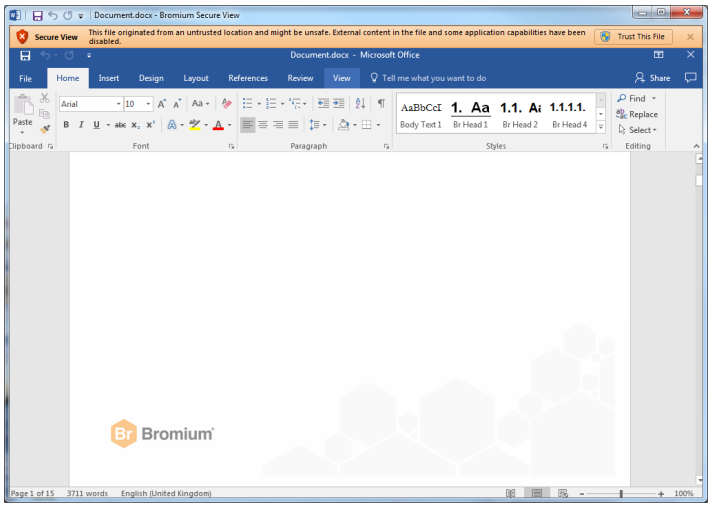
6. Download a Word document from the Internet and save it to the desktop.
7. Navigate to the folder that contains the document.

   The document will have a  icon on it to indicate that it is untrusted:

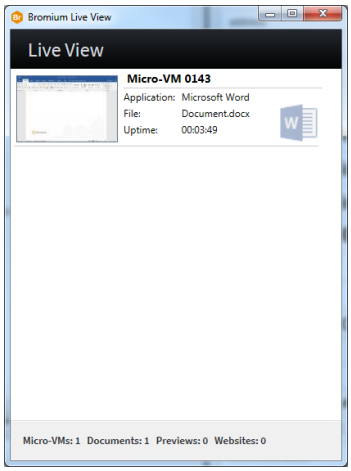


8. Double-click the document to open it.

   The document opens in Secure View:



9. Check Live View and verify that a micro-VM was created for the document:



Verifying Monitoring Installation

To verify that monitoring has been installed and is running:

1. Log in to the controller.
2. In the Policies page, click on or create a policy for your devices.
3. Enable monitoring on endpoints. In the Features tab, select **Host monitoring** then click **Save and Deploy**. Ensure the policy is applied to the applicable devices.
4. In the Settings page, click **Enable Endpoint Monitoring support**. This allows you to view monitoring information for endpoints in the controller.
5. Open the **Devices** page. Check that endpoints on which monitoring is installed are included in the devices table.

   The installation contains a default monitoring policy; monitoring can immediately start monitoring endpoints.

Missing Devices

If you do not see a particular device in the **Devices** page:

1. On the device, open an administrator command prompt.
2. Change directory to `C:\Program Files\Bromium`.

   This is the default location. If you installed Bromium in a different location, change to that directory.

3. Run the command `BrManage BMS.ServerUrl print`.
4. Check the returned response and confirm it is properly configured.
5. If you need to change the setting, run a command that specifies the controller server URL. For example:

   ```
   BrManage BMS.ServerUrl <controller URL>
   ```

6. To apply any changes, restart isolation.

Installation or Initialization Failures

If installation fails, check the installation log in `C:\ProgramData\Bromium\vSentryInstall.log`. This log file maintains a record of the installation and uninstall processes.

Due to a Windows installer issue, the versioned servers directory is not always removed on reboot after a failed installation. After a reboot, the directory can be removed manually.

If initialization fails, check the log at `C:\ProgramData\Bromium\vSentry\Logs\BrHostLog.log`. This log provides general information about the entire deployment. Check this log first if Bromium software fails any time during or after initialization. Additional logs may be needed, as directed by Bromium Customer Support.

3 Deploying Bromium Products Remotely

You can install Bromium products using a centralized software distribution system, such as Microsoft System Center Configuration Manager (SCCM) to deploy the software. Remote installation utilizes system management software products like SCCM, Active Directory Group Policy, and Altiris to install and configure Bromium products on multiple systems.

Remote Deployment Requirements

To deploy Bromium remotely, ensure you have the following requirements:

- Familiarity with and administrative access to AD and SCCM
- An AD deployment with target systems that are configured and network accessible
- The Windows 7 management station being used to configure Group Policy must have access to the Domain Controller and write permissions
- The installation package, which includes:
    - `BrHostDrvSup.exe` - provides drivers for the prechecker
    - `BrPreCheck.exe` - checks system readiness and checks for minimum required RAM on the system
    - `BrReporter.exe` - provides the generator that makes and uploads prechecker reports to Bromium
    - Installer package `.msi` - contains the software used for a clean install or to upgrade systems running previous versions
    - `vSentry_Bootstrap.xml` - contains a key named `BMS.ServerUrl` to identify the controller policy server to connect to and a key named `BMS.IgnoreInvalidServerCertificate` that allows the client to upload configuration and status information to the server in the event the server has an invalid SSL certificate during software installation or upgrade

Configuring the Bootstrap File

To use bootstrap file in the installation process, edit the bootstrap file to include the controller server URL during installation or upgrade so that the isolation clients can contact the controller server.

To configure the bootstrap policy:

1. Make a copy of the sample bootstrap file. The sample bootstrap `.xml` file is included in the Bromium installation package.
2. Open the bootstrap file in a text editor.
3. Set the XML parameter `BMS.ServerUrl`.Set the URL of the controller server. If the server has an SSL certificate installed, enter an HTTPS URL. If no certificate is installed on the server or the server does not have a properly signed certificate, enter an HTTP URL. Uncheck the required SSL flag for the controller website settings in IIS to enable access using HTTP. For example: `<key name="BMS.ServerUrl"><![CDATA[https://bec.corp.com]]></key>`
4. Set the parameter `BMS.IgnoreInvalidServerCertificate` to `1` to allow the client to upload configuration and status information to the server in the event the server has an invalid SSL certificate. For example:

   ```
   <key name="BMS.IgnoreInvalidServerCertificate"><![CDATA[1]]></key
   ```

   or
   Set this to `0` to disable the client from uploading configuration and status information to the server in the event the server has an invalid SSL certificate. For example:

   ```
   <key name="BMS.IgnoreInvalidServerCertificate"><![CDATA[0]]></key>
   ```

Specifying the Bootstrap Policy File Path

When specifying the bootstrap POLICIESXML file on the msiexec command line, it must be an absolute path.

For example, if the current working directory is c:\example:

```
msiexec /i installers\bromium_secure_platform.msi POLICIESXML=config\example.xml
```

it will install `c:\example\installers\bromium_secure_platform.msi` and read the config XML from `c:\example\config\`

Using SCCM to Deploy Bromium Products

Microsoft System Center Configuration Manager (SCCM) is a tool for managing a large number of systems remotely from a central system. You can use SCCM to install, upgrade, and uninstall Bromium software.

The method for configuring SCCM is the same if you are installing, upgrading, or uninstalling the software; the only variation is the strings you enter in the package program. For specific information about using SCCM, refer to the appropriate Microsoft documentation.

Note: Performing redundant pushes of the same package is not supported. Pushing (for example, installing) the same package multiple times disables Bromium products. To do this, use SCCM to uninstall and then reinstall Bromium software.

Before configuring SCCM:

- Open the AD console and verify that there is a valid OU for the target systems on which to install upgrade and uninstall the Bromium product
- Place the target systems in a domain that is visible to SCCM
- Copy the Bromium deployment file (`.msi`) to the network share that is used to distribute packages. An HTTP/S server or a file share can host the MSI file. :// URLs cannot be used for local paths; they can be used only as equivalents of UNC paths. For example, `\\my-computer\share\file.msi` can be written as `file://my-computer/share/file.msi`. The FQDN of the host (including its share) can be used.
- The SYSTEM account on the Bromium machine must have permission to access the fileshare where the MSI package resides. The system account (not the account of the logged in user) is used when the client downloads the package from the network share.

To create and deploy a package:

- Create a collection of client systems
- Create a software package
- Configure distribution points
- Configure the package program:
    - For example, to install or upgrade Bromium (specify the full path the policy file, including the volume name):

```
msiexec /i bromium_secure_platform.msi /qn SETTINGSFILE=\\myserver\myfolders\bootstrap.xml
SERVERURL=https://myserver.domain.com:8080 /forcerestart /L=\\myserver\myfolders\logfolder
```

  Include `/forcerestart` on the `msiexec` command line or, if users are logged in, `/promptrestart`. Additionally, ensure you include the `SERVERURL` setting. Otherwise, installation will fail.

  Note: If a network share is used to run `msiexec` or provide data to `msiexec` (such as the policy file specified by POLICIESXML), the network share must provide "Domain Computers" read access because `msiexec` and SCCM run in the SYSTEM context.

- Ensure you have 8 GB disk space
- Specify the client platform on which to run
- Configure the program to run whether or not a user is logged on
- Configure the program to run with administrative rights
- Configure an advertisement:
    - Allow users to run the program independently of assignments
    - Verify that the administrator for the collection has read, modify, delete, and distribute permissions

msiexec Command-line Switches and Parameters

The following table lists the supported `msiexec` command-line switches and parameters:

Parameter	Description
/forcerestart	This `msiexec` switch can be included to restart the system immediately after installing or uninstalling Bromium products
/i	Install Bromium software
/l [*opts*] *file*, /log *file*	All native `msiexec` logging switches and options are supported. Refer to the msiexec documentation for usage details. If installation or upgrade fails and more logging information is needed to debug the problem, try again and include the `msiexec` logging switches.
/qn	Set user interface level (`q`) to none (`n`) so that, from a user perspective, the operation runs silently without any user interaction. The /qn switch is recommended for remotely managed installation such as SCCM because the user does not need to be logged in. Bromium software installs without user interaction. Initialization starts immediately after installation, but Bromium products do not start until after a reboot.
/x	Delete the Bromium deployment
SERVERURL=*URL*	Set this for specifying the controller server URL with which the endpoint communicates. This setting is mandatory when using msiexec to install the Bromium platform. If this setting is not present, installation will fail. This parameter uploads error information that results from unmet requirements (such as insufficient RAM) during installation or upgrade to the controller server, and displays this information in client events. If this parameter is not set, client status information is not uploaded to the server until after the policy sets the server URL parameter. Status information is not reported to the controller server if this parameter is not set and installation fails before the policy can set the server URL. This parameter allows the controller to track the success or failure of Bromium deployments as they occur and is ideally suited for silent installations. Enter the HTTPS URL of a controller server with a valid signed certificate. If required, you can include a port number in the URL. Enter the server URL in the form `https://`*FQDN*`:`*nnnn*. For example, `https://bec0.bromium.net:8000`.
AllowInvalidServerCert = `yes/no`	For monitoring, set this to `yes` to allow the client to upload configuration and status information to the controller server in the event the server has an invalid SSL certificate. For example: `AllowInvalidServerCert=yes` Set this to `no` to disable the client from uploading configuration and status information to the controller server in the event the server has an invalid SSL certificate. For example: `AllowInvalidServerCert=no`

SERVERIGNORECERT= *yes/no*	For isolation, set this to `yes` to allow the client to upload configuration and status information to the controller server in the event the server has an invalid SSL certificate. For example:
	`SERVERIGNORECERT=yes`
	Set this to no to disable the client from uploading configuration and status information to the controller server in the event the server has an invalid SSL certificate. For example:
	`SERVERIGNORECERT=no`

cleanall=`yes`	Software artifacts are left behind after uninstalling Bromium products so that you can reinstall these products later and still retain most policy settings. Include this parameter on the `msiexec` command line when installing or uninstalling Bromium products to delete the associated directories in Program Files, ProgramData, AppData, and so on, delete both the system and user images, and Bromium state settings and configuration settings.

Parameter	Description
ENABLED=no	By default, isolation is installed as enabled. To change the behavior so that isolation is installed as disabled, add: `ENABLED=no`

POLICIESXML=*path*	The `POLICIESXML` parameter is used to specify the path to the bootstrap XML policy file with which to configure target systems during Bromium installation. You can specify the path to a file on a network share if the machine has appropriate read and write permissions. Enclose paths with spaces inside double quotes ("").
	The path can be absolute or relative. If the path is not absolute, it will be relative to the working directory when the MSI is launched.
	For example, if the current working directory is `c:\directory` and you run:
	`msiexec /i installers\bromium_secure_platform.msi POLICIESXML=config\directory.xml`
	it will install `c:\directory\installers\bromium_secure_platform.msi` and read the config XML from `c:\directory\config\directory.xml`.
	For example, if you run:
	`msiexec /i bromium_secure_platform.msi POLICIESXML=c:\config\directory.xml`
	it will pick up `c:\config\directory.xml`, regardless of what the current working directory is.
	When `POLICIESXML` is included on the `msiexec` command line, you are indicating that the local system will be managed by a policy server and the Desktop Console Settings windows that are normally displayed during manual installation will not be displayed because settings will be configured by the policy.
	For Bromium-managed clients, the policy file specified by `POLICIESXML` typically contains a few policy parameters to contact the controller server and downloading a complete policy. This parameter is not necessary if the policy is going to be managed through Active Directory/Group Policy. Alternately, you can import a policy using the BrManage utility.

POSTPONEINITUNTILREBOOTED=yes	By default, initialization automatically starts after a silent fresh install. To change the behavior so that initialization begins after a reboot, add: `POSTPONEINITUNTILREBOOTED=yes` This parameter has no effect on graphical installations.
Targetdir=vSentry install directory	This parameter is the Bromium default directory: `%ProgramFiles%\Bromium\vSentry\`

SCCM Remote Deployment Failures

The following is a partial list of the steps you can take to correct a failed remote deployment when using SCCM:

- Right-click the package and select **Update Distribution Points**
- Perform a client pull from the Configuration Manager Actions Console
- Navigate to the `C:\Windows\SysWOW64\CCM\Cache` folder on the client and delete the package folder. This removes previously run and failed advertisements for the package and allows you to rerun the advertisement.
- Disable and enable the advertisement if needed
- Before the advertisement has been successfully deployed, use the rerun advertisement option on the advertisement. This option is not displayed after the advertisement is deployed.
- If the previous actions fail, delete the advertisement and recreate it, wait for the package deployment message, and then perform a client pull

4 Upgrading, Repairing, and Uninstalling Bromium Products

These topics describe how to upgrade to newer versions or downgrade Bromium products, repair product installations, and uninstall Bromium products.

Upgrading Isolation and Monitoring

Use the installation file (`.msi`) to manually upgrade your product. Check that the target system is appropriately configured before running the installer.

Note: If you are running Bromium Endpoint Monitoring version 3.2 and earlier, it must be uninstalled before using the **Install Package** remote command to upgrade to version 4.0 GA and later.

To upgrade Bromium products manually on a single local system:

1. Copy the installation `.msi` to the system that you want to upgrade.
2. Double-click the `.msi`.
3. Click **Next** in the Upgrade Confirm dialog.
4. Click **Next**. The User Access Control (UAC) dialog opens. The User Access Control dialog box prompts you to perform the action with administrative privileges. If the UAC dialog is not displayed on the desktop, it is displayed in the taskbar. Click the icon to display the UAC dialog box. If you do not perform the upgrade as an administrative user, the User Account Control window displays the configured system administrators. Select an administrator and enter the password, then click **Yes**.

   The Upgrading window opens.
5. When the update is complete, click **Yes**.

   The User Access Control dialog box closes and installation begins. Installation progress is indicated in the status bar. If Microsoft Outlook is running when you install the Bromium platform, a dialog prompts you to quit Outlook and restart it.
6. Click **Finish**.
7. Restart the product. The new version will be used after the desktop is rebooted.

Database Changes After Upgrading

When you upgrade to Bromium version 4.0 Update 2 and later, Info severity alerts that have a corresponding higher severity alert are removed from the database. After upgrading, you may notice a decrease in your database size and a reduction in the number of threats listed in the controller. If event destinations have been configured, messages for these deleted alerts sent to syslog, email, or TAXII destinations may contain links to threats that no longer exist.

System Backup and Restore

There are no special requirements for backing up and restoring files on a Bromium-protected system. Backup and restore systems that run Bromium products just as you would other systems.

To back up the controller settings (including the secret key), copy the `settings.json` file located in the **ProgramData > Bromium > BMS** directory.

Uninstalling Bromium Products

To remove the Bromium installation:

1. Finish all network activity on the system, such as browsing and file downloads.
2. Open the Windows software removal utility.
3. Select the Bromium product you want to uninstall and then select **Uninstall**.

   The Programs and Features dialog box opens, prompting you to confirm the uninstall action.
4. Click **Yes**.

   The User Access Control dialog box opens, prompting you to perform the action as an administrative user.
5. Click **Yes**.
6. Click **Reboot**.

Some artifacts may remain on removable drives, network shares, and the local drive after disabling or uninstalling Bromium products. In each folder that contains untrusted files, there may be a hidden `~bromium` folder and files appended with `.bromium`. The `~bromium` folder contains meta files, one for each untrusted file. `.bromium` files contain metadata that identifies an untrusted file. It is recommended that you do not open, delete, move, or modify these files and folders if you intend to reinstall Bromium products. Leaving the files and folders maintains the provenance and state of untrusted files. If you enable or reinstall Bromium products without altering these files and folders, the file appendages and the `~bromium` folders will disappear again.

Repairing Installations

After using the Windows repair option, you must reboot the system immediately to ensure that isolation will run after the installation is repaired. If Bromium was installed remotely, you must deploy the same .msi to repair the installation remotely. To manually repair the installation, the .msi file must have the same name as the original file used for the installation.

Downgrading

To downgrade Bromium products, uninstall the newer version and install the previous version.

5 Installing and Configuring the Bromium Controller

The Bromium Controller provides centralized monitoring and management for Bromium software deployments in the enterprise. It consolidates diverse information from multiple, widely distributed systems into one central location to provide real-time monitoring, security status, and security analysis.

The controller creates and manages policies that are pulled by Bromium clients. It also monitors system and security software status such as client health, Bromium product version changes, connection times, and policy update times. Activity logs are generated and forwarded to the server at regular intervals. Ready access to timely information lets the administrator catch and analyze attacks quickly.

The controller also aggregates threat alerts from all endpoints, providing the SOC team with centralized and automated analysis of malware.

For information about adding controller servers to existing deployments, see Configuring Clustered Controllers.

Preparing the Server for Installation

Check that the systems on which you are installing the controller meet the following requirements and ensure all devices connected to the controller are offline. If you are running Bromium products prior to version 4.0, you must uninstall the controller before upgrading to version 4.0 or later.

For controller and general SQL database requirements, see Controller Requirements.

Checking IIS Authentication

Verify that IIS is configured to use Anonymous authentication. If it is not, refer the Windows documentation to configure IIS.

Install IIS

Verify that the Web Server (IIS) role is installed and that it has CGI enabled. For more information about enabling CGI on IIS, refer to the Microsoft documentation: https://technet.microsoft.com/en-us/library/cc753077(v=ws.10).aspx

Configuring an SQL Database and Database Administrator

Controller server data is stored and managed in an SQL Server database. The database is not included in the controller installation package. Ensure that you are logged on as an administrator when configuring the SQL database and database administrator. For specific information about configuring SQL, refer to the Microsoft documentation.

The database must be configured either locally on the server system or be remotely accessible. The database administrator must be configured as follows:

- Uses SQL Server authentication
- When creating the database in SQL Server, use a case insensitive collation for the new database
- Password policy not enforced

- Allocated to the public role
- Administers the database used for the controller
- Has access permissions to connect to the database engine and login
- Has all database role membership except db_denydatareader and db_denydatawriter

Note: If you are using SQL Server Express, by default it accepts Windows authentication mode only. Attempts to log in to the database, even with the authentication type set to SQL Authentication, can result in the following error:

```
Microsoft SQL Server Error 18456 Severity 14 State 1
```

To resolve this issue, open SQL Server Management Studio then navigate to the Server Properties to view the server authentication options. Enable **SQL Server and Windows Authentication mode** and restart SQL Server.

Ensure network access to databases on the database server is using the designated TCP port (1433 by default.) To configure the controller, enter the IP address of the SQL Server host and the assigned port number.

Installing the HTTPS Certificate

The installer detects installed certificates and allows you to choose a certificate to use. Install the server certificate as instructed by your enterprise, for example, by submitting a certificate request to your cryptographic service provider and adding the signed certificate to your system.

Note: For testing purposes, the controller server can be configured to run in HTTP mode. This is not recommended in a production deployment for security reasons.

Installing the Controller

To install the controller:

1. Copy the .msi installation file to the target server system and double-click the file.

   The installation wizard opens.

2. Click **Next**.

   The License Terms window is displayed.

3. If you agree with the terms of the license and want to continue installation, select **I agree**.
4. Click **Next**.
5. Enter or browse to the location in which to install the software. The default is: `C:\Program Files (x86)\Bromium\Controller`.
6. Click **Next**.
7. Click **Install**.

   Controller settings are displayed. The remaining installation steps are used to configure controller server operation.

Configuring the Controller

You configure settings for the controller in the **Application Settings** dialog during installation, or you can change any of these settings in this dialog at a later time in the Windows Start menu **> Bromium > Bromium Controller Settings**.

1. Configure the settings as follows:

- **Logging** - The **Detailed (for troubleshooting)** option performs detailed logging for Bromium Support to diagnose controller-related problems. Set this option to **Standard** during normal operation and to reduce disk space usage if it is an issue.
- **Secret Key** - A randomly generated string used by the controller for cryptographic signing. It should be set when the server is initially configured.

  Note: Do not share the secret key with anyone; this could introduce privilege escalation and remote code execution vulnerabilities. It is your responsibility to securely back up and store the secret key, which is located in the `settings.json` file in the **ProgramData > Bromium > BMS** directory.

- **Default Time Zone** - Select the time zone in which the controller server is located. Optional.
- **Allow Single Sign-On for Active Directory Accounts** - Provides a link to enter Active Directory credentials when users log in to the controller interface

  Note: To enable this option, Windows Authentication must be installed in IIS Feature Security and ensure the controller address is listed in the Intranet Zone in Internet Explorer.

2. Click **Next**.

   The **Server Settings** page is displayed.

3. Configure the settings as follows:

- **Protocol** - The protocol for server/device communication. Select either **HTTPS** or **HTTP**

  Note: HTTP is recommended in a test environment only. HTTP is insecure and should not be used in a production environment.

  If you switch protocols at a later time, change the protocol as appropriate for the controller and policy URLs in every policy. Before changing the **Protocol** setting, change the URLs in the policies. Otherwise, a protocol mismatch may orphan the Bromium clients.

- **Port** - Use the default port number or enter a port number. If you enter another port number, ensure you change the IIS Site Bindings on the server to match the port number you want to use and change the firewall rules accordingly.
- **HTTPS Certificate** - If HTTPS mode is enabled, select the certificate that the server should use. This must be a certificate that is already installed on the local machine. The HTTPS certificate becomes active when HTTPS is selected. If you need to generate a self-signed SSL certificate, click **Generate**.
- **Address** - Enter a URL that can be accessed externally (either the current server or another server used for load balancing or reverse proxy)
- **IIS local application pool user** - The built-in IIS application pool user
- **Service user** - The Active Directory user account that has access over IIS application pool. Enter the domain name, user name, and password for the account.
- **Test user** - If **Service user** is selected, click **Test user** to test the account to ensure that it has the privileges required for the server to function properly

4. Click **Next**.

   The **Database Settings** page is displayed.

5. Configure the settings as follows:

- **Server Name** - Enter the location of the SQL Server instance, using the format `<servername>\<instance name>`. When the controller and SQL Server are installed on the same system, it is unlikely that TCP connections have been explicitly enabled for the SQL Server instance and, therefore, entering the system IP address may cause a connection failure. For this reason, if you want to install the controller on the same system as SQL Server, specify the hostname with a period (".").
- **Database Name** - Enter the database instance name. The database must exist and must be empty.
- **SQL Server User** - Enter the SQL Server user name with which to connect to the SQL Server instance. The user must have full administrative permissions to the database. The controller user must be able to modify the database and create and drop tables.
- **Password** - Enter the password for the controller administrator user.
- **Windows authentication against service user** - Check this option to enable Windows authentication for SQL log ins
- **Force protocol encryption** - Bromium recommends checking this option for production deployments
- **Test connection** - Click to test the SQL Server connection
- **Request new administrator user** - Check this option to add a new administrator

6. Click **Next**.

   The **Email Settings** page is displayed.

7. To use Email Destinations events in the Bromium Controller, configure the settings as follows:

- **Subject Prefix** - Enter text to use in the subject line of all emails sent by the management server
- **Appear From** - Enter the email addresses that you want to appear as the sender of all emails sent by the controller. Ideally this should be a valid email in case users accidentally reply to an automated email.
- SMTP Relay options:
  - **Host** - Specify the SMTP server to be used to send email. The user name and password boxes can be left blank if they are not required.
  - **Port** - Enter the outgoing SMTP port number for your email server. The default is 25.
  - **User** - Enter the SMTP email user account name used to send alert notification emails
  - **Password** - Enter the password for the user
  - **Security** - Select none, encrypted (STARTTLS), or verify encrypted (STARTTLS requiring a valid certificate)

Note: After you complete installation, ensure you add an email destination in the web console.

- **Test Connection** - Click to test the email connection

8. Click **Next**.

   The **File Storage Settings** page is displayed.

9. Configure the settings as follows:

- **Logs Directory** - Enter or browse to the folder that the server uses to output debug logs. The default is `C:\ProgramData\Bromium\BMS\logs`. If the `ProgramData` folder is hidden, change hidden file visibility in the Window folder options.

- **Uploads Directory** - Enter or browse to the parent folder where uploaded alerts, imported policies, and controller -generated policies are placed. This directory is where monitoring policies and policies are placed.

  Note: You are responsible for backing up both of these directories as well as the database. It is recommend that you back up both directories and the SQL Server database at the same time due to the database reference files within these directories.

10. Click **Next**. If a controller administrator does not exist when you save the settings, a dialog box opens so you can configure an administrative user.
11. Enter the name and password for the controller administrator.
12. Click **Next**. If an "IIS port already in use" error is displayed, click **No** to return to the controller settings wizard to change the server port.

    A message indicates successful configuration completion and restarts IIS.
13. Click **OK**.
14. Click **Finish**.
15. Verify the installation by logging in to the server. Enter the server URL in a web browser, then enter the administrator name and password. Click **Log In**.

Determining Remote Management

To determine if the local client is remotely managed by the controller:

1. Open the Desktop Console.
2. Click **Settings**.

   If the connection status in the Management tab indicates a controller URL or policy settings, the local client is remotely managed.

Changing Controller Configuration

You can change the controller configuration at any time using the settings interface that runs on the controller. The configuration categories are:

- Application Settings
- Server Settings
- Database Settings
- Email Settings
- File Storage Settings

These settings are described in Configuring the Controller.

To change the controller configuration:

1. Select **Start > All Programs > Bromium Enterprise Controller > Bromium Enterprise Controller Settings** or double-click `C:\Program Files (x86)\Bromium\Controller\bin\BrBMSSettings`

2. Configure the management interface as needed. If you want to change the secret key, see Changing Controller Configuration.
3. Click **Save** to confirm the changes.

   A dialog box indicates that the settings have been successfully saved and the IIS site has been successfully restarted.

   Note: If the server uses HTTPS and a different port number to the default (443), you must update the IIS Site Bindings on the server to match the port number in use. This must also be done if you save without making any changes.

4. Click **Close**.

Changing the Controller Secret Key

To change the secret key:

1. Open the Bromium Enterprise Controller Settings interface and select **Application Settings**.
2. Click **Change** next to the **Secret Key** field.
3. Click **Yes** to confirm.
4. Click **Generate** and click **Save** to save the new secret key.

Migrating to Controller Policy Management

Isolation can be installed and managed locally using the Desktop Console with the BrManage utility. Local management is suitable for malware analysis and one-off testing, however to ensure consistent policy application and client monitoring, Bromium recommends that you manage all isolated clients with the controller.

Migrating to controller management is simple and quick, requiring only a small XML policy file and permission to run the BrManage utility.

To migrate an isolated client from standalone mode to managed mode:

1. Obtain the controller URL. If you do not have a URL, see Installing and Configuring the Bromium Controller for information about configuring servers.
2. Run the following command from an administrator command prompt:

   ```
   BrManage management-server <your controller server URL, including HTTP or HTTPS>
   ```

3. Open the URL for the controller and check the **Devices** page to ensure that the client was added to the controller.

   By default, the device displays in the default group (Ungrouped) unless it is part of an automatic group such as an Active Directory OU or a group with membership rules. It fetches the policy configured for the appropriate group. Policies do not take effect until they have been downloaded and Bromium has been restarted.

4. Ensure that there is a policy configured for the default group.

If no policy is configured for the default group, you can manually move the device from the default group to a different group or you can set up a group with member rules to contain similar devices.

Configuring Isolation Clients to Report to the Controller

On each controller client, you must configure some policy settings so that the client knows where to push status and pull policy information.

Controller parameters tell the isolation client where to upload security data and how often. Without this information the isolation client is unable to register with the management server. These parameters are:

- `BMS.ServerUrl`
- `BMS.IgnoreInvalidServerCertificate`

Communication between the controller and device goes over HTTPS using the server SSL certificate to ensure a secure communication channel. The device then uploads status and downloads policy information on average at 15 minute intervals.

Data is pushed from each client to the controller. The controller does not use heartbeats to detect the presence of isolation clients or pull data from these clients. If the isolation client is improperly configured and tries to access the server using a non-existent URL or is retrieving policy files from an improper location, client information may be incomplete or missing from the controller.

The settings described above are set on each system during Bromium software installation. If the software is installed through SCCM or Altiris, this configuration is specified as an XML file.

If the software is installed manually, use command line parameters to configure these settings.

To configure BMS.ServerUrl:

1. On the controller client, start an administrator command prompt.
2. Change directory to `C:\Program Files\Bromium`.

   This is the default location; if you installed Bromium in a different location, navigate to that directory.
3. Run the command `BrManage BMS.ServerUrl print`.
4. Check the returned response and confirm it is properly configured.
5. If you need to change the setting, run a command that specifies the controller URL: `BrManage BMS.ServerUrl` *`<controller server URL>`*

Viewing Server History Logs

The history log generates an event in the `history.log` file when significant configuration changes occur in the controller. The `history.log` file is located in the logs directory. The default location is `C:\ProgramData\Bromium\BMS\logs`

The controller generates an event in the `history.log` file when users:

- Create, edit, or delete a:
  - Device
  - Device group, and when an endpoint is moved to/from a device group (show source/destination group)
  - Policy
  - User
  - User group
  - Role
  - AD connection
  - Syslog destination
  - Email destination
- Change their password
- Create a remote command
- Change the controller deployment configuration using the controller settings interface on the server
- Attempt an operation for which they do not have permission

The controller also generates an event in the `history.log` file if the controller is upgraded, uninstalled, or installed.

Upgrading the Controller

During the upgrade process, the SQL Server and IIS configuration and data are left intact. Controller data on the server is also left intact. After the upgrade, all agent logs, records, and tracking information are still displayed in the controller and accessible on the system.

Note: Before upgrading, ensure all devices connected to the controller are offline.

To upgrade the current deployment:

1. Check that you have a working installation to ensure that the Microsoft SQL Server database and IIS are operational and correctly configured. It is not necessary to perform other checks such as disk space, system, network, and so on as you have an existing working deployment and there should be little change in disk space consumption.
2. Check the version of the controller. Controllers version 3.2 and earlier must be uninstalled prior to installing the Bromium Platform 4.0 GA and later. For later versions of the controller, an in-place upgrade is performed. If you are running version 2.4.8 of the controller, you must upgrade to version 2.5 before upgrading to later versions.
3. Run the `setup.exe` file.

   The previous version of the controller is uninstalled.
4. Click through the setup and configuration windows to use the previous configuration settings. If the server (**Server Root** setting) does not use the default port 80, you must update the IIS Site Bindings on the server to match the port number in use.

   Settings are saved and the IIS site is restarted after the software installs.

   Note: Depending on the size of your database, migration may take up to an hour or more to complete. Do not cancel installation during this migration process.
5. Click **Finish**.

   The new software is installed.

Endpoint to Controller Communication: LAN

If your endpoint to controller communication goes through a proxy, read the following information to ensure communication between endpoints and the controller.

Endpoint services run at the system level. Because most proxies are configured at the user level (for example, Internet Explorer for browsing) they cannot be used by system-level services. The recommended approach is to open a firewall port or specify a rule for endpoints to communicate directly with the controller.

To use a proxy for these services, you can set machine-level proxy settings using the `netsh winhttp set proxy` command (http://technet.microsoft.com/en-gb/library/cc731131%28v=ws.10%29.aspx#BKMK_5) or enforcing it through Group Policy (http://msdn.microsoft.com/en-us/library/ms815135.aspx).

Endpoint to Controller Communication: Internet

Client certificates allow only customer-approved isolation devices to securely connect to the controller. This enables connections over the Internet to occur directly to the controller, without the need for a VPN to secure the connection. Devices without a valid client certificate will be halted from communicating to a controller instance.

Client certificates are used to limit access to the controller to endpoints that have been enrolled with a valid enterprise certificate, signed by a Certificate Authority (CA) of choice. The CA could be an internal enterprise CA or a public CA. Only endpoints with a valid client certificate, signed by the correct CA will be allowed to connect to the controller.

This mechanism allows devices to connect securely over the Internet to a controller instance on a corporate LAN. While HTTPS can be used to secure the communication protocol, any device that knows the HTTPS address of the controller can connect and try to

receive a configuration policy, regardless of its location, particularly if the HTTPS address of the controller is Internet-facing. Non Client-Cert HTTPS connections are recommended for LAN use only, with a VPN used for Internet connectivity.

The Client Certificate feature negates the need for an endpoint to use a VPN to securely connect to a controller for policy updates and reporting information.

Prerequisites

- A controller instance
- Endpoints with Client Certificates. Each endpoint that needs to communicate to the controller instance over the Internet requires a valid client certificate. This can be provisioned using existing Active Directory infrastructure (AD Cert Services) and Group Policy Objects (GPO) to deliver certificates to endpoints. Refer to your Active Directory administrator or security administrator for assistance.
- SSL Gateway, Reverse Proxy, LB and so on. The connection to the controller instance is validated by a device on the network perimeter that checks for certificates. This is a standard function of most network firewalls, Load Balancer, SSL Gateway, and Reverse Proxy. Your appliance must be configured to ask for the connection to the controller to check for the right CA certificate for the connection to be approved. You must select the CA that signed your client certificates.

Other Considerations

The controller address needs to be considered for internal and external endpoints. If you have devices that roam (such as laptops) and can be on the LAN and then be remote, your internal and external DNS will need to be configured correctly.

There are two options:

1. Both internal and external endpoints will use HTTPS and client certificates.

   This defends against rogue endpoints on the internal network as well as allowing access to certified endpoints across the Internet. In this case, all connections can be routed through your SSL Gateway/GSLB to secure your controller infrastructure.

2. Internal connections use HTTPS, external connections use HTTPS and client certificates.

   In this case, internal DNS should reflect the HTTPS IP of the controller server or cluster, but when external, that same HTTPS address should reflect the IP of the SSL gateway/GSLB.

Configuration

To complete configuration, ensure:

- Endpoints have the correct certificates and controller is installed and functioning
- The SSL gateway/LB and so on has been configured to check for a valid certificate (by selecting the correct CA for the connection)

Example connection from a non-enrolled (attacker) endpoint:

1. Endpoint attempts to connect to `https://bec.companyx.com`.
2. SSL gateway requests valid certificate for connection to pass and gives endpoint list of valid CA certs to use.
3. Endpoint unable to respond as no certificate signed by correct internal CA, or endpoint responds with non valid certificate.
4. Connection refused by gateway.

Example connection from enrolled endpoint with correct certificate:

1. Endpoint attempts to connect to `https://bec.companyx.com`.
2. SSL gateway requests valid certificate for connection to pass and gives endpoint list of valid CA certs to use.
3. Endpoint responds with valid cert, signed by internal CA.

4. Connection allowed through LB/SSL Gateway and so on.
5. Connection to the controller (or optional reverse proxy) made and endpoint downloads latest policy config and reports latest information to the controller.
6. Connection dropped by endpoint.

Troubleshooting

Certificate Troubleshooting

The Bromium endpoint automatically detects that the controller requires client certificates. If there is a certificate in the endpoint's machine store (with a private key accessible in SYSTEM/BrRemoteMgmtSvc for isolation or SYSTEM/BemAgent for monitoring), the Bromium software will automatically use that to authenticate the connection with the controller.

To test that the endpoint can communicate with the controller, open the Desktop Console and select **Update Policy** in the Management tab. If the update occurs without error (and the connection status is shown as **Connected**), it has communicated to the controller server successfully.

If the endpoint does not automatically detect a client certificate (or detect that a certificate is required), the configuration parameter `BMS.UseClientCertIssuer` (for isolation) or `BEM.ClientCertIssuer` (for monitoring) can be used to specify the certificate issuer DN. Bromium software will use this to search the machine's certificate store for a certificate issued by this DN. The Bromium software will then use this certificate for all controller communication, whether or not the server requires client certificates.

Note: If you set the `BMS.UseClientCertIssuer` or `BEM.ClientCertIssuer` parameters through policy, it should be added to the policy before requiring client certificates on the server. After client certificates are enabled on the server, any misconfigured clients will be unable to pull policy.

Connection Troubleshooting

The `BrHostLog.log` under Bromium's Program Data directory should contain information about connection attempts to controller. It is recommended that the log level be set to **Debug** (through Policy or the Desktop Console) before troubleshooting connection issues. Logs regarding client certificates are located in the Windows Application Event Log.

When the Bromium software is choosing which certificate to send to the controller, messages are displayed. For example:

```
2015-08-28 13:30:56.094+01:00[56:23.821] P23444T16360
BrRemoteMgmtSvc BrRMLUploadThread.cpp<499>:CreateRequest(): Using
client cert CN=PF00WRFW-UKL.bromium.net
```

If the Bromium software is unable to use the required certificate, it may be because the SYSTEM user does not have access to the certificates private key. In this case, alter the permissions on the private key using mmc.exe and try again.

Uninstalling the Controller

An uninstall removes the software and the IIS settings for the controller. Configurations, logs, uploaded files and databases in the *drive*`:\ProgramData\Bromium\BMS` folder are left intact. This prevents data loss, and allows you to install a newer version of the controller using the same data.

To uninstall the controller, either:

- Select **Start > All Programs > Bromium Controller > Uninstall Bromium Controller** and click **Yes** when prompted to continue with the uninstall, or
- Go to **Control Panel > Programs and Features** and double-click **Bromium Controller** to uninstall

Troubleshooting Controller Issues

If you encounter problems running the controller, check the logs in the default location `C:\ProgramData\Bromium\BMS\logs`. These logs are also helpful if you contact Bromium Support for assistance with any issues. You can also search for issues on the Bromium Support site: https://support.bromium.com

Device Missing from Devices Page

If you do not see a particular device in the **Devices** page, follow these steps:

1. On the device, open an administrator command prompt.
2. Change directory to the `C:\Program Files\Bromium\vSentry\servers` directory.

   This is the default location. If you installed Bromium in a different location, change to that directory.
3. Run the command `BrManage BMS.ServerUrl print`
4. Check the returned response and confirm it is properly configured.
5. If you need to change the setting, run a command that specifies the management server URL. For example:

   ```
   BrManage BMS.ServerUrl https://admin.myserver.net:8000
   ```
6. If you changed the setting, restart isolation to apply the change.

Remote Deployment Failures

The following is a partial list of the steps you can take to correct a failed remote deployment:

- Right-click the package and select `Update Distribution Points`
- Perform a client pull from the Configuration Manager Actions Console
- Go to the `C:\Windows\SysWOW64\CCM\Cache` folder on the client and delete the package folder. This removes already-run and failed advertisements for the package and facilitates re-running the advertisement.
- Disable and enable the advertisement if needed
- There is a re-run advertisement option present on the advertisement, but only before the advertisement has been successfully deployed. This option is no longer displayed after the advertisement is deployed.
- If the previous actions fail, delete the advertisement and re-create it, wait for the package deployment message, and then perform a client pull

Bromium Error Codes

When Bromium issues an alert for an error, warning, or information, it is also sends the alert to the controller. For descriptions of and possible actions needed for Bromium error codes, refer to the "Actionable Error Codes" article on the Bromium Support site: https://support.bromium.com

6 Using Bromium Secure Monitoring

Bromium Secure Monitoring detects suspicious behavior on endpoints, enables you to search and view a detailed analysis of file hashes, provides file quarantine to prevent malicious files from being accessed by users, and allows you to configure custom monitoring rules in the Bromium Controller.

Enabling Monitoring

To enable Bromium Secure Monitoring, select a policy in the Policies page. In the Features tab, enable **Host monitoring** in the Monitoring options. Click **Save and Deploy** to apply this change to devices using this policy. To display monitoring information (such as monitoring threat information) in the controller, in the Settings page select **Enable Endpoint Monitoring Support**.

When the monitoring is enabled, the Dashboard page in the controller displays alert graphs for threats detected by monitoring. Additionally, potentially malicious files on host machines detected by monitoring are indexed. If **Indexing for search** is enabled in the policy, you can search for MD5, SHA-1, or SHA256 hashes using the **Hash Search** field.

Using File Quarantine

The **Blacklist support** option in the policy allows you to quarantine files to prevent them from being accessed and executed on endpoints. Quarantined files are still visible on endpoints and will contain a Bromium icon, but cannot be trusted, attached to emails, or opened when double-clicked or accessed by third-party software. If you delete a quarantined file and then restore it on the endpoint, it will remain quarantined, even if the file name or location changes.

Click **Add File to Blacklist** in the Threat Summary page or the File analysis page to quarantine the file. After the hash is quarantined, any files detected (current files or incoming) with matching content will be quarantined immediately. When you quarantine a file, you still need to repair any damage done by the malware. Quarantining prevents future files with the same hash from being executed, but does not reverse any actions executed by the malicious file.

Removing Files From Quarantine

On the **Blacklisted Files** page, select a file and click **Remove from Blacklist**. This prevents future instances of the file hash from being accessed or executed. To completely remove the file from quarantine, send the **Unquarantine file** remote command to the applicable devices. Additionally, if you uninstall Bromium products, files remain quarantined until you reinstall the Bromium platform and send the remote command to the devices.

Using Quarantine Without Isolation

You can use quarantine without running isolation (that is, website browsers and files are opened outside of Bromium isolation) by adding the `vSentry.QuarantineOnly` advanced setting with a value of `1` to the policy.

Note: When selecting files to quarantine, ensure you are selecting the correct file. For example, check that you are not quarantining a file that is required for Windows to boot.

Using Monitoring Rules

If enabled, Bromium can monitor for malicious or unexpected activity on the host which might be indicators of compromise. These behaviors are contained in a *base rules file* (.brf) and are supplied by Bromium. The base rules file is not mandatory and monitoring will detect potentially malicious events without it; however base rules provide additional filtering to help avoid false positive alerts.

These base rules can be imported and then viewed in the controller in the **Base Rules** tab in the **Monitoring Rules** page. To import the .brf, select **Import Base Rules** file in the **Rules Actions** list. To view the file, click on it in the Base Rules table.

Select the base rules file to display the Rule Information page. This page allows you to rename the file, apply it to device groups, and enable or disable the file. The Monitors area displays behavior (such as changes to the file registry or modifications to Internet Explorer settings) that triggers high severity alerts in the Dashboard and Threats pages.

Bromium provides new .brf files with each update to the Bromium platform. You can download the .brf with the software update from https://my.bromium.com/ .

Custom Rules

Optionally, you can also add custom rules to monitor for extra behaviors that you consider to be malicious.

Custom monitoring rules can be used to monitor additional processes or behaviors on endpoints. Additionally, you can exclude applications from monitoring to help avoid false positive alerts. Using rule layering, custom rules are applied on top of the base rules.

Note: Custom rules are carried over after upgrading Bromium products and do not need to be reconfigured.

Managing Alert Volumes

High volumes of alerts can be triggered if monitoring policies are not configured carefully or if, for example, an update causes existing software to behave differently and trigger alerts. If the controller receives a high volume of alerts, scalability issues may occur.

Use the following guidelines to help avoid this issue:

- When you add new rules or monitor new applications, carefully consider if there are situations in which they could cause a high volume of alerts. For example, if malware executes using PowerShell, it is not recommended that you add powershell.exe to your monitoring policy. PowerShell is frequently used with legitimate applications and adding it to a monitoring policy would cause numerous false positive alerts.
- If you change monitoring policies, consider rolling them out to a small group of endpoints first and watch for unwanted alerts over the next few days. After this time, roll the changes out more widely.
- Edit a policy and in the **Advanced** tab, add one of the following settings to help prevent excessive threats:
    - `bem.alertsmaxfilebacklogcount`: sets the maximum number of alert files that can exist on an endpoint. If monitoring produces more alerts than the specified limit, it ceases to create further alerts until new rules are deployed, and a management action is displayed in the controller. The default value is 1000.
    - `bem.circlealertslimit`: sets the maximum number of individual events to include in an alert. The default value is 300.

Additionally, you can create custom monitoring rules to exclude specific applications from monitoring.

Adding Exclusions to Suppress False Positive Alerts

If alerts are being triggered for events that you do not want to include in monitoring, you can do one of the following:

- Create a custom rule using the **Monitor** option. To this rule, add the application that is triggering the alert and apply the registry or file path to the application. These applications will continue to be monitored; however, alerts will no longer be produced. Use this method if the false positive is the result of a registry or file read or write process that is specific to a particular registry or file location.
- Create a custom rule using the **Don't Monitor** option to exclude an entire application from monitoring. This may be necessary if an application is producing false positive alerts in different ways.

Settings for Monitoring Endpoints

If a group for monitoring only exists, you can create a policy and assign it to that group. If this group does not exist, it is recommended that you create a group for monitoring agents to allow monitoring-specific configurations to be applied through policy to that group.

To add monitoring settings, create a new policy in the Policies page and apply it to an existing or new monitoring group. The following advanced settings are available:

Setting	Description
`BEM.AlertsMaxFileBacklogCount`	Sets the maximum number of alert files that can exist on an endpoint. If monitoring produces more alerts than the specified limit, it ceases to create further alerts until new rules are deployed, and a management action is displayed in the controller. The default value is 1000.
`BEM.CircleAlertsLimit`	Sets the maximum number of individual events to include in an alert. The default value is 300.
`BEM.CloudCheckEnabled`	Controls whether or not monitoring connects to the Bromium Threat Cloud to provide real time threat data analysis. The settings available are: `0` - Do not connect to Thread Cloud `1` - Connect to Threat Cloud (default)
`BEM.LogLevel`	This setting controls the type of log that is created: `0` - Error `1` - Warning `2` - Info (default) `3` - Trace `4` – Debug
`BEM.MaxLogSize`	Controls maximum log file size in MB that can be uploaded to the controller server. The default is 50.

Setting	Description
`BEM.MinimumUpdateInterval`	The frequency (in seconds) with which the endpoint communicates with the controller for important updates (status update and threats updates.) The default is 60 seconds.
`BEM.Search.ScanScheduling`	The initial file system scan occurs during idle time when users are not using their machines in order to avoid disruption; however, users may not be away long enough for this scan to complete. If the scan does not complete within a given number of days, it will then start to occur in the foreground with a greater risk of user disruption. This setting controls how many days before the scan switches from idle time to the foreground. The default is 10 days. You can change the setting to any number of days or one of the following: `0` = always scan in the foreground `-1` = always scan during idle time
`BEM.UpdateInterval`	The frequency (in seconds) with which the endpoint communicates with the controller for regular updates (policy changes and so on.) It is recommended that this interval is set to `900` (seconds) to optimize CPU and network usage. The default is 120 seconds.

7 Desktop Console Overview

The Desktop Console is a user-facing graphical interface for viewing and configuring (if enabled) isolation information on the local system. The Status page is the first place to check the following information:

- Health status, when isolation was started, and whether or not isolation is running
- Initialization status and when isolation was last initialized
- Security status and the number of web pages and documents that have been opened safely in a micro-VM
- Policy status and controller URL (if isolation is managed by the Bromium Controller)

Pages and options that are displayed in the Desktop Console are dependent on whether or not the endpoint is using a policy, and if a policy has been applied to the device, options displayed depend on what has been enabled in the policy.

If permitted in the policy or if no policy has been applied, you can click **Restart** or **Disable** in the Desktop Console or from the taskbar to restart or disable isolation.

Click **Edit** to set or change the license. Enter the license key and click **Apply** to apply the Bromium license to the endpoint.

You can open the Desktop Console by navigating to **Start > All Programs > Bromium > Bromium Desktop Console** or click the Bromium icon in the taskbar and select **Open Desktop Console**.

Before you proceed, plan your configuration strategy. Anticipate the configuration that may be required to provide web access to trusted sites. In the case of a single sign-on (SSO) environment, websites that make use of SSO tools must be added to the list of trusted sites so that the user credentials are passed to the native browser. For example, environments using a SaaS CRM application that relies on an SSO tool to pass AD credentials to automatically log in users to other websites must include the system hosting the SSO tool to the list of trusted sites for auto-login to work.

Checking Initialization Status

To check the initialization status, hover the mouse over or click the Bromium icon in the taskbar. If a "May need attention" message is displayed in the tooltip or the pop-up menu, isolation may require initialization. Alternatively, select **Open Desktop Console** from the menu. The Health section indicates if initialization is required.

Configuring Settings

The **Settings** page contains Management information such as connection status and policy information, and a Settings tab to configure network isolation settings.

In the Management tab, you can click **Update Policy** after you save any policy changes in the controller. Policy changes are visible in the Desktop Console either after the policy is updated manually or when it is checked automatically (every two minutes, by default.) This interval can be configured in the policy Manageability tab in the controller.

If the Settings tab displays a message stating that the settings are managed by policy, the endpoint is managed by a controller policy and you cannot change the configuration locally. Otherwise, by default, the Trusted Sites options are displayed in the Settings tab.

If **Allow network isolation** is enabled in the policy, the Intranet, Cloud/Saas, Trusted, Associated, and Advanced tabs are displayed.

Changing Intranet Settings

Use the network isolation settings to change the configuration of the Active Directory/DNS domains and blocks of IP addresses that comprise your organization's intranet.

To change intranet settings:

1. Open the Desktop Console.
2. Click **Settings**.
3. Click the **Settings** tab. If the "Settings are managed by your administrator" message is displayed, click **Edit**.
4. If the User Access Control dialog box is displayed, click **Yes**.
5. Click **Intranet**.
6. Click **Add Intranet Site**.

   The Add Intranet Site window is displayed.
7. Enter an AD/DNS domain name for your intranet using the format `*.intranetdomain.com` or enter a netblock, ensuring the IP address includes a subnet mask in the form *IP* / *mask bits*. The IP address ranges entered for the netblocks must match and correspond to the list of AD/DNS domains. Isolation will block network connectivity to this domain/netblock from untrusted web pages and documents.
8. Click **OK**.
9. Add further intranet domain or netblocks as required. To modify or delete an existing entry, select the entry in the list and click either **Edit** or **Remove**.
10. To include the sites specified in the Windows **Internet Options > Security >** Local intranet list with the list of trusted intranet sites, enable the **Include sites from Internet Explorer intranet security zone** option.

Changing Cloud/SaaS Settings

To limit access to specific cloud/SaaS sites:

1. Open the Desktop Console.
2. Click **Settings**.
3. Click the **Settings** tab. If the "Settings are managed by your administrator" message is displayed, click **Edit**.
4. Click **Cloud/SaaS**.
5. Click **Add Cloud/SaaS Site**.

   The Add Cloud/SaaS Site window opens.
6. Enter a DNS domain. Start the DNS domain with the asterisk (*) wildcard.
7. Click **OK**.
8. Add more domains as needed. To modify or delete an existing entry, select the entry in the list and click either **Edit** or **Remove**.

Changing Trusted Sites Settings

Trusted Internet sites run on the native desktop, unlike untrusted Internet sites that run isolated in a micro-VM. By default, downloaded executable files are marked untrusted and cannot be run on the native desktop. This is to protect the local system from potential attacks.

To configure trusted Internet sites:

1. Open the Desktop Console.
2. Click **Settings**.
3. Click the **Settings** tab. If the "Settings are managed by your administrator" message is displayed, click **Edit**.
4. Click **Add Trusted Site**.

   The Add Trusted Site window is displayed.

5. Enter a DNS domain. Start the DNS domain with the asterisk (*) wildcard.
6. Click **OK**.
7. Add further Internet domains as required. To modify or delete an existing entry, select the entry in the scroll-list and click either **Edit** or **Remove**.
8. To include the sites specified in the Windows **Internet Options > Security > Trusted sites** list with the list of trusted sites, enable the **Trust sites in Internet Explorer trusted zone** option.

Changing Associated Sites Settings

By default, isolation co-locates linked websites that interact with each other in the same micro-VM if they pass a security check. You can change these settings if required.

To change associated sites settings:

1. Open the Desktop Console.
2. Click **Settings**.
3. Click the **Settings** tab. If the "Settings are managed by your administrator" message is displayed, click **Edit**.
4. Click **Associated Sites**.
5. Use the slide control to choose a setting:

- **Strict**: All sites are mutually isolated
- **Restricted**: Sites that explicitly trust each other are isolated together
- **Unrestricted**: Associated sites are isolated together

Changing Cookie Management

In the Advanced tab, cookie management can be relaxed to permit greater end user control, but with less security.

To configure cookie management:

1. Open the Desktop Console.
2. Click **Settings**.
3. Click the **Settings** tab. If the "Settings are managed by your administrator" message is displayed, click **Edit**.
4. Click **Advanced**.

5. Change the following options as required:

- Enable the **Enable Persistent Cookies** option to set the types of cookies in other domains that can download to micro-VMs. The default allows cookie downloads from all domains.
- Use the web page cookies options to determine the cookies that can be downloaded to micro-VMs from domains other than the top-level domain (TLD) for the current web page:
    - **No cookies from other domains.**
    - **Only persistent cookies from other domains (recommended).**
    - **All cookies from other domains.**

Viewing Security Alerts

The **Security Alerts** page displays the number and severity of any threats that have been detected on the endpoint, the time the threat was detected, severity, the type of threat (such as a PDF file or Internet Explorer site), and the response and action taken by isolation.

Sending Isolation Error Reports

The error reporting function compiles system and related information for debugging the local Bromium deployment and uploads it to Bromium. In conformance with the privacy policy presented in the license agreement, certain information will be transmitted to Bromium for use in troubleshooting submitted errors. The `Log.RemoveSensitiveInformation` policy setting can be used to exclude proxies, URLs, and so on from log data. For more information about this setting, see Manageability Settings.

To generate an error report:

1. Open the Desktop Console.
2. Click **Support**.
3. Click **Send Report**.
4. Click **Yes** to confirm.

After the report is sent, you can create a corresponding support ticket. Alternatively, click **Save Report** to save the report locally and, for example, send it as an email attachment to Support.

Setting the Isolation Log Level

Logs are a useful tool for monitoring isolation performance and behavior. Log level determines the types and amount of information collected. Select a level that is appropriate for the type of data you want to track. Log levels are:

- Debug
- Trace
- Event
- Warning

Debug is the lowest setting. Warning is the highest setting. The lower the setting the larger the amount of data collected. In general, the Event or Warning level is sufficient for day-to-day tracking. In the event isolation is not performing as expected, then the Trace or Debug level may be necessary. The default is Event.

If your deployment is experiencing problems and you intend to send an error report to Bromium, set the log level to Debug, and allow the issue to continue for a short period before you click **Send Report**. This gives the system an opportunity to generate the detailed data necessary for debugging issues.

To set the log level:

1. Open the Desktop Console.
2. Click **Support**.
3. Select a log level from the **Log Level** list.

You may ask users to clear their log files before reproducing an issue to reduce file size and to ensure the log only contains symptoms relevant to the issue. To do this, click **Clear Log Files** then send or save the report.

Viewing Hardware and Software Details

The Software and Hardware tab displays version and physical information for software and hardware running on the endpoint that is relevant to isolation. These details can be used to help diagnose issues on endpoints running isolation.

Opening Live View

To view the micro-VMs running on the system, click the Bromium icon in the taskbar and select **Open Live View** or click **Live View** in the Desktop Console. This window displays applications (web sites, files, Office documents, PDFs, and so on) that are currently running and protected by isolation.

A Using BrManage to Configure Policies

It is recommended that you manage Bromium-protected clients with the controller to obtain the following advantages:

- Clients download a policy during isolation installation and at set intervals afterward
- Policy changes automatically propagate to the isolation clients that are configured to use that policy

If you choose not to use the controller to manage policies, isolation provides a BrManage utility to configure policies locally. You can also use BrManage to perform administrative actions such as restarting isolation and importing a policy or exporting the isolation deployment configuration to a structured policy file to the location: `C:\Program Files\Bromium\vSentry\servers`

You can run BrManage in an administrator command prompt or using a batch file. Changes made by BrManage are superceded when centralized policy management through the controller is applied.

Note: Policy changes made with BrManage may not be applied when a policy is being managed by the controller or group policy. If you notice configuration changes made with BrManage are not being applied, and controller policy management is enabled, restore control to the local system with the command `BrManage management-server del`.

BrManage Syntax

BrManage syntax depends on the task you want to perform:

- Enter a string value for BrManage parameters with two states (off and on) or that require a string value such as a domain name or MIME type
- Enter a numeric value for BrManage parameters with multiple levels. For example, a valid value for `Browser.CookiesNonTLDAccessMode` can be 0 (do not share cookies), 1 (share only persistent cookies), or 2 (share both session and persistent cookies.)

For parameters with multiple values, such as `Browser.CloudSaaSSites` and `Browser.TrustedSites`, run the BrManage command once for each value that you want to add or delete. Enclose multi-word string values in double quotes (").

For examples, see Commonly Used BrManage Commands.

BrManage Commands

Commands	Description
BrManage *param action value*	Sets most policy parameters. For example, `BrManage Browser.TrustedSites add 216.139.0.95/8.` and `BrManage BMS.ServerUrl https://bec.bro.net:8000`
BrManage config set --name=*param* --value=*value*	Sets other policy parameters that are not set with the previous command. For example, `BrManage config set --name=MimeHandler.Winword.EscapeOut --value=1`
BrManage config get --name=*param*	Displays the current value of most policy parameters. For example, `BrManage config get --name=MimeHandler.Custom0.FileTypes`
BrManage config add-to-list --name=*param* --value=*value*	Adds file extensions to a list of MIME file-types. For example, `BrManage config add-to-list --name=MimeHandler.Winword.FileTypes --value=.wrd`
BrManage config remove-from-list --name=*param* --value=*value*	Removes file extensions from a list of MIME file-types. For example, `BrManage config remove-from-list --name=MimeHandler.Winword.FileTypes --value=.wrd`
BrManage config dump	Outputs most policy settings and their values
BrManage	Lists all supported BrManage parameters and options. Parameters comprise a simple name and a long name. For example: `management-server | BMS.ServerUrl [address|print]` The simple name in this example is `management-server` and the long name is `BMS.ServerUrl`. You can specify either name on the BrManage command line; however, only the long name is recognized within a policy and only the long name is used to configure policies in the Group Policy Management Console.

BrManage Settings

The long name is listed first, followed by its simple name.

Controller Settings

Setting	Description
BMS.ServerUrl management-server	Specifies the URL that the isolation client uses to contact the controller. This must be an HTTPS URL with a valid signed certificate. If required, you can include a port number in the URL. Use the form: `https://servername:nnnn` `print` - Display the current value. If you want to restore control to the local system, enter: `BrManage management-server`

Manageability Settings

Setting	Description
`vSentry.AllowConsole`	Controls whether or not the Bromium icon is displayed in the System Tray menu and the Desktop Console shortcut is displayed in the Windows Start menu. `0` - Do not show `1` - Show (default)
`vSentry.AllowStatusMonitor`	Controls whether or not users can access Live View from the Desktop Console. `0` - Do not show `1` - Show (default)
`vSentry.DesktopConsoleShowChangeSettingsPage`	Controls whether or not to display the **Settings** tab in the Desktop Console. When disabled, system users cannot change these configuration settings. `0` - Disable the Settings tab (default) `1` - Enable the Settings tab `print` - Display the current value
`vSentry.ProductLicenseKeys license-keys`	Use the following settings for Bromium license keys: `add <key ID>` - Add a key `del <key ID>` - Delete a key `info` - Display the timestamp, lifespan in days, serial number, and key for every key `print` - List every key

Setting	Description
`vSentry.QuarantineOnly`	You can use quarantine without running isolation (that is, website browsers are opened outside of Bromium isolation.) This mode still blocks access to untrusted malicious files; however websites open natively on the host and files are not protected by isolation. To enable this feature, add the `vSentry.QuarantineOnly` advanced setting with one of the following values: `0` - Isolation is enabled. If isolation is not supported on the device, an error is displayed in the Desktop Console. `1` - Isolation is disabled and is in "quarantine only" mode. If isolation is not supported in the device, an error is reported to the controller. `2` - Isolation will enter full protection mode if supported by the device. Otherwise, it will be in quarantine only mode. (Default.) **Note:** When selecting files to quarantine, ensure you are selecting the correct file. For example, check that you are not quarantining a file that is required for Windows to boot.
`vSentry.SystemInitialization init-system`	Initializes or reinitializes the Bromium system image after performing system-level configuration and software changes. The user image is also automatically reinitialized. `request` - Prompt to reinitialize the deployment `create` - Reinitialize the deployment immediately on receipt of this setting `status` - Display the initialization status of the local deployment `cancel` - Cancel reinitialization
`GuestSystemCrashDumpMode`	Sets the system crash dump type. Run the following command: `BrManage config set --name= GuestSystemCrashDumpMode --value=value` where `value` is one of the following: `0` - Debugging information is not written to a file `1` - Complete crash dump is written to a file `2` - Kernel memory dump is written to a file (default) `3` - Small memory dump is written to a file
`LCM.TemplateExclude`	You can exclude certain (bad) system files from the micro-VM to avoid long or failed initializations. To exclude a file from initialization, run the following command: `BrManage config set-list --name=LCM.TemplateExclude \Windows\System32\[file name]` After enabling this setting, subsequent initializations exclude the specified file.

Setting	Description
`Log.RemoveSensitiveInformation clean-logs`	Controls whether or not to restrict information that is logged during operation. For example, when enabled, Bromium does not save a record of URLs that were browsed, which can make debugging and error investigation more difficult. `0` - Include sensitive data in log files, all pertinent data is logged (default) `1` - Exclude sensitive data from log files `print` - Display the current value
`Mimehandler.Default.SecureRibbonText`	Use this setting to customize or brand the secure toolbar text. To change the default secure toolbar text, set the following parameter:] `Mimehandler.Default.SecureRibbonText = [your custom text]` The parameter supports up to 5200 characters in upper or lower case, numbers, or special characters.

`Mimehandler.Default.TrustFile`	Controls content checking when trusting files. Available choices are:
	`0` - No content check
	`1` - Content check (basic.) Deny trusting if contents do not match extension.
	`3` - Content check (advanced.) When enabled, file extensions are checked. Bromium takes action based on what is set in the configuration for that extension (such as administrator privileges required, allow trust, deny trust, and so on.)
	If no handling for the extension is found in configurations, check content. There are two possible outcomes:
	• If content is malicious (consult a third pre-populated, extendable list of malicious content types), deny trust
	• If content is not malicious, either:
	  • For known content types, take action based on what is set in the configuration for that content type (show UAC, allow/deny trust, and so on)
	  • For unknown content, block trusting or allow trusting based on a third configuration

Setting	Description
`Reporting.Enabled error-reporting`	When enabled, this setting displays **Send Error Report** in the Desktop Console. `0` - The option is not displayed `1` - Display the option `print` - Display the current value

`XVM.CustomProxyConfig`	Configures a custom web proxy (different to the proxy configured in Internet Explorer settings) for web traffic originating from Bromium. Must be used with `XVM.CustomProxyNTLMCreds`.
	This configuration contains the proxy configurations in one of the following formats:
	• PAC URL - This must start with http:// https:// or file://
	Example:
	`http://example.com/my-pac.pac`
	• PROXY string
	Example:
	`PROXY my-proxy.domain.com:3128; PROXY 10.10.20.6:8080`

`XVM.CustomProxyNTLMCreds`	Configures a custom web proxy (different to the proxy configured in Internet Explorer settings) for web traffic originating from Bromium. Must be used with `XVM.CustomProxyConfig`.
	This configuration contains NTLM credentials for authenticating with proxy and uses the format: `DOMAIN:USERNAME:NTLM_HASH`
	Example:
	`BROMIUM:John.Smith:`
	`757D2D46EC36CF52D99B665C57415962`
	To generate the NTLM hash:
	On the server running the controller, run the following commands:
	`Execute c:\Program Files (x86)`
	`\Bromium\BMS\python\python`
	Then:
	`import binascii, hashlib`
	`print binascii.hexlify( hashlib.new('md4',`
	`"mypassword".encode('utf-16le')).digest() )`
	The returned value can then be used for the NTLM hash in the `XVM.CustomProxyNTLMCreds` setting.

Browser Settings

Setting	Description
Trusted website options	
Adblock for Internet Explorer	The following settings can be used to control Internet Explorer tracking protection (Adblock): `Browser.IEAdBlock` Controls whether or not Internet Explorer tracking protection is enabled. The default is on. `Browser.IEAdBlockListLocation` Allows you to specify a tracking protection list (TPL) file to use when Adblock for Internet Explorer is enabled. You can also use the `Browser.IEAdBlockListUpdateInterval` setting to set the interval (in days, 1 - 9999) between checking for and downloading updated TPL files. The default for this setting is 7. `Browser.IEAdBlockAddresses` The list of domains on which Internet Explorer tracking protection is enabled. The default value `*.*` enables tracking protection for all sites. `Browser.IEAllowUnblockAds` Allows users to enable or disable ad blocking for individual web sites using the context menu. The default setting is on.

Intranet Trust	For endpoints on intranets, trusted sites accessed using IP address can be configured to open on desktops. To do this, use the following settings:
	`Browser.TrustIntranetNetblocks = 1`
	`Containment.EnableIntranetDetection = 1`
	`Containment.ForceAppearOnIntranet = 0`

Setting	Description

Temporary Trust	Temporary Trust allows users to override the trust level of a web site for a single session in isolated Internet Explorer, Chromium, or Firefox browsers. It is activated when users right-click on an untrusted web page and select the **Temporary Trust** option from the context menu.
	To enable this feature, apply the following settings to the policy:
	`Browser.TemporaryTrust.Mode`
	`0` = Feature disabled (default)
	`1` = Request mode; user types reason and submits request for trust
	`2` = User can trust sites but must first enter a reason
	`3` = User can trust sites without entering a reason
	`Browser.TemporaryTrust.RequireUAC`
	`ON` = Require UAC prompt before trusting (default)
	`Browser.TemporaryTrust.PromptText`
	Custom text is shown when users temporarily trust a site. The default is blank, in which case an internationalized default is used.
	`Browser.TemporaryTrust.RequestPromptText`
	Custom text is shown when users request trust for a site The default is blank, in which case internationalized default is used.
	`Browser.TemporaryTrust.BlockedSites`
	List of sites for which the temporary trust workflow is blocked.

`Browser.AllowClientCertAuthFromAllVMs`	Controls support for websites requiring certificate-based authentication. Must be used with `Browser.EnableClientCertAuth`. `0` - Off `1` - On (default) By default, when turned on, certificate-based authentication is allowed only for sites listed as intranet and SaaS.

`Browser.BlockDownloads`	You can configure isolation to block downloads from all websites in Internet Explorer and allow downloads from specific addresses. By default, downloads are allowed (0) from all websites. To block downloads, use the following setting:
	`Browser.BlockDownloads = 1`
	To allow downloads from a specific address, use the setting:
	`Browser.BlockedDownloadAddresses = <address>`
	Separate multiple addresses with commas.
	Users are prompted with a message if a download is attempted from a blocked website.

Setting	Description
`Browser.CheckDefaultBrowser` `check-default`	Isolation opens untrusted web pages using the default browser. If you have multiple web browsers on a system, such as both Firefox and Internet Explorer, configure a supported browser as the default browser to ensure that websites open securely in a supported browser or prompt the user to select the browser. `0` - Skip this check and use the current default browser `1` - Set the default browser to Internet Explorer `2` - Prompt the user to select a browser `print` - Display the current value
`Browser.Chrome`	`0`- Disable protection for Chrome `-1`- Auto detect and enable protection for Chrome on endpoints that have Chrome installed Isolation must be reinitialized after enabling this setting.
`Browser.ChromeExtensionsBlackList`	Controls which Chrome extensions to blacklist. Ensure that `Browser.ChromeExtensionsEnabled=1`. To blacklist extensions, set the following: `Browser.ChromeExtensionsBlackList=<extension ID>` To view extension IDs: 1. Open a Chrome browser. 2. Go to chrome://extensions/ 3. Check the **Developer Mode** box. The ID is listed in the extension details.
`Browser.ChromeExtensionsEnabled`	`0` - Chrome extensions are off `1` - Chrome extensions are on

`Browser.ChromeExtensionsWhiteList`	Controls which Chrome extensions to whitelist. Ensure that `Browser.ChromeExtensionsEnabled=1`.
	To whitelist all extensions, set the following:
	`Browser.ChromeExtensionsWhiteList=*`
	To whitelist specific extensions, set the following:
	`Browser.ChromeExtensionsWhiteList=extension IDs to whitelist`
	To get an extension ID, follow the steps described in the `Browser.ChromeExtensionsBlacklist` description.

Setting	Description
`Browser.ChromeShouldAskWhereToDownloadByDefault`	Determines whether or not you need to specify a location for individual file downloads in Chrome. Use one of the following values: `0` - off `1` - on This setting is on by default.
`Browser.CloudSaaSSites` `cloudsaas-sites`	Specifies corporate cloud /SaaS sites that you want to protect. These websites still open in micro-VMs, but they are invisible to other micro-VMs that are not in this list. Add sites using domain wildcard notation, for example: `*://*.domain.com` `add *://*.domain.com` - Add a DNS name `del *://*.domain.com` - Delete a DNS name `print` - Display the current value
`Browser.CookiesNonTLDAccessMode` `browser-nontld-cookies`	Controls access to cookies of a specific website from a different website. For example, if you browse to abc.com, it can request cookies set by xyz.com. While this is normal browser functionality, it can have security implications. `0` - No cookies from other domains may be accessed by the current website `1` - Persistent cookies from other domains may be accessed but access is blocked to session cookies, which usually contain sensitive information. (Recommended.) `2` - All cookies from other domains may be accessed by the current website `print` - Display the current value
`Browser.EnableClientCertAuth`	Controls support for websites requiring certificate-based authentication. Must be used with `Browser.AllowClientCertAuthFromAllVMs`. `0` - Off `1` - On (default) By default, when turned on, certificate-based authentication is allowed only for sites listed as intranet and SaaS.
`Browser.IE`	`0`- Disable protection for Internet Explorer `1`- Auto detect and enable protection for Internet Explorer on endpoints that have Internet Explorer installed **Note:** Isolation must be reinitialized after enabling Internet Explorer protection.
`Browser.IEAllowUnblockFlash`	Allows you to enable Flash on domains present in `Browser.IEFlashBlockAddresses` and then disable it again from the context menu. The options available are: `1` - Off. Flash is not available in the context menu `0` and the domain is present in `Browser.IEFlashBlockAddresses` - Users can right-click to enable Flash and are permitted to disable Flash

Setting	Description
`Browser.IEEnablePhishingFilter`	By default, SmartScreen is off. To enable it, use the following setting: `Browser.IEEnablePhishingFilter = 1`
`Browser.IEMetro.EnableIEHelperHooks`	On Windows 8.1, isolation does not protect web browsing sessions open in the Metro version of Internet Explorer. Isolation can be configured to either block browsing in Metro Internet Explorer or to allow native browsing in Metro Internet Explorer (default behavior.) The desktop Internet Explorer will be protected in the same way as Windows 7. To change the behavior, use the following configuration: `0` - Allow native browsing in Metro Internet Explorer (default) `1` - Block browsing in Metro Internet Explorer
`Browser.IE.UsePersistentCache`	Controls persistent caching in Internet Explorer. `0` - Disabled (default) `1` - Enabled

`Browser.IntranetSites`
`intranet-sites`
	Specifies a list of intranet DNS or network zones for your enterprise. Untrusted web pages and documents opened in micro-VMs will not have network access to the intranet. Do not remove the default localhost entry.
	Bromium recommends entering both the DNS zone and Netblocks for the intranet because both are required to isolate the intranet from micro-VMs running untrusted content.
	Add sites using domain wildcard notation, for example:
	`*.domain.com`
	`1.2.3.0/2`
	`print` - Display the current value.

`Browser.LinkedTabPlacementMode` `browser-linked-tab-placement-mode`	Controls how associated sites are isolated so you can maximize user privacy without breaking cross-site dependencies. `0` - Unrestricted: associated sites are isolated together. `1` - Restricted: sites that explicitly trust each other are isolated together. `2` - Strict: all sites are mutually isolated. `print` - Display the current value.
`Browser.TrustedSites` `trusted-sites`	Specifies which websites open natively without isolation. Bromium pre-populates this list with the sites Microsoft uses to deliver software updates. Use this list to allow applications, such as screen sharing software, native access to systems in order to run plugins, and so on. Add sites using domain wildcard notation, for example: `*://*.domain.com` `add *://*.domain.com` - Add a DNS name `del *://*.domain.com` - Delete a DNS name `print` - Display the current value

Setting	Description
`Browser.TrustIntranetSites` `trust-intranet-sites`	Controls whether or not to mark sites listed in the Trusted Corporate/Intranet Sites list as trusted, thereby disabling isolation for these sites and opening them natively. This permits these sites to deliver custom ActiveX plugins and other code requiring native access to Bromium endpoints. `0` - Trust only the intranet sites specified in the configuration `1` - Trust websites located on the Intranet, as specified in `Browser.IntranetSites` `print` - Display the current value
`Browser.TrustSitesInIETrustedZone` `trust-ie-sites`	Controls whether to include the sites specified in Internet Explorer Trusted Sites and Intranet sites in the list of trusted sites. Web contents and downloads from trusted sites run on the main Windows desktop and are unprotected by isolation. `0` - Do not allow sites listed in Internet Explorer Intranet and Trusted Zones to be opened without isolation `1` - Allow sites listed in Internet Explorer Intranet and Trusted Zones be opened natively without isolation `print` - Display the current value

Setting	Description
`Containment.Enabled`	The network containment setting controls whether or not network isolation is used, and the if the Intranet, Cloud\SaaS, Associated Sites, and the Advanced tabs are displayed in the Desktop Console. The network containment setting is off by default for standalone installs. `1`- On `0`- Off (default)

Isolate Networks By Port Number	If network isolation is enabled, you can block access to port numbers for Internet, intranet, and Saas sites.
	To block ports, set `Containment.Enabled` to `1` (on), then:
	Internet:
	`Containment.PortBlocking.Internet.Ports = [port number]`
	Intranet:
	`Containment.PortBlocking.Intranet.Ports = [port number]`
	SaaS:
	`Containment.PortBlocking.SAAS.Ports = [port number]`
	To allow access to blocked ports:
	Internet:
	Set `Containment.PortBlocking.Internet.IsWhitelist = true`
	Add `Containment.PortBlocking.Internet.Ports = [blocked port number]`
	Intranet:
	Set `Containment.PortBlocking.Intranet.IsWhitelist = true`
	then add `Containment.PortBlocking.Intranet.Ports = [blocked site]`
	SaaS:
	Set `Containment.PortBlocking.SAAS.IsWhitelist = true`
	then add `Containment.PortBlocking.SAAS.Ports = [blocked site]`

Document and File Protection Settings

Setting	Description
Threat checking for embedded documents	You can enable isolation to check for threats in embedded Microsoft Office documents, for example, if a Microsoft Word file contains an embedded Word file containing malicious content. To enable this feature, add the `MimeHandler.Default.BackgroundLavaCheck`, `Untrusted.BGLavaCheckOfficeEmbeddedObjects`, `Untrusted.Editing.Enabled`, and `Untrusted.OfficeMacrosEnabled` advanced settings with a value of `1`.
`GuestPrintingMode`	Allows you to disable printing and to specify the behavior when printing is disabled. To use this feature, set `GuestPrintingMode` to one of the following values: `0`: Printing disabled `1`: Bromium secure printing (default) If you disable printing (`0`), set `GuestPrintingDisabledConfig` with one of the following values: `0` - No printers are displayed in the print dialog `1` - "Functionality is not available" message is displayed `2` - Printers are visible and the **Print** button is available, and the "Functionality is not available" message is displayed `3` - Printers are visible and the **Print** button is available, no additional dialog is displayed
`MimeHandler.Acrobat.EscapeOut`	Controls whether or not to mark PDF documents as untrusted, which will open inside micro-VMs. If this option is not selected, documents will be auto trusted. `0` - Auto trust PDF documents `1` - Mark PDF documents as untrusted `print` - Display the current value

Setting	Description
`MimeHandler.AcrobatPro.InstalledOnHost`	Controls whether or not to enable protection for PDFs opened in Adobe Acrobat Pro. By default, Acrobat Professional protection is turned on. `0` - Disable Acrobat Pro protection sets the following behavior: • When both Acrobat and Adobe Reader are installed on the desktop, isolation protects PDF documents by opening them in Adobe Reader • When only Adobe Reader is installed, isolation protects PDF documents by opening them in Adobe Reader • When only Acrobat is installed, isolation does not have protection for PDF documents `-1` - Auto detect (default) sets the following behavior: • When both Acrobat and Adobe Reader are installed on the desktop, isolation protects PDF documents by opening them in Acrobat • When only Adobe Reader is installed, isolation protects PDF documents by opening them in Adobe Reader • When only Acrobat is installed, isolation protects PDF documents by opening them in Acrobat
`MimeHandler.Winword.EscapeOut`	Controls whether or not to mark Microsoft Word documents as untrusted, which will open inside micro-VMs. If this option is not selected, these documents will be auto trusted. `0` - Auto trust Word documents `1` - Mark Word documents as untrusted `print` - Display the current value
`MimeHandler.Excel.EscapeOut`	Controls whether or not to mark Microsoft Excel documents as untrusted, which will open inside micro-VMs. If this option is not selected, these documents will be auto trusted. `0` - Auto trust Excel PDF documents `1` - Mark Excel documents as untrusted `print` - Display the current value
`MimeHandler.PowerPnt.EscapeOut`	Controls whether or not to mark Microsoft PowerPoint documents as untrusted, which will open inside micro-VMs. If this option is not selected, these documents will be auto trusted. `0` - Auto trust PowerPoint documents `1` - Mark PowerPoint documents as untrusted `print` - Display the current value

Setting	Description
`MimeHandler.Other.EscapeOut`	Controls whether or not to auto trust files that cannot be opened inside micro-VMs. `0` - Auto trust files that cannot open in micro-VMs `1` - Mark files that cannot open in micro-VMs as untrusted `print` - Display the current value
`MimeHandler.Executable.BackgroundLavaCheck`	Controls whether or not a background threat check is automatically run on an EXE file when **Trust and Open** is used on the file. If the EXE file is found to be malicious, the file is prevented from being marked as trusted. `0` - Do not run background threat check on EXEs when **Trust and Open** is used (default) `1` - Run background threat check on EXEs when **Trust and Open** is used. Execution of EXEs remain blocked. Attempting to trust an EXE displays a progress bar while the EXE is analyzed in a micro-VM in the background. The result is either to allow trusting or to deny trusting with an alert to the end user if the executable is found malicious. The result is cached so if the user attempts to trust the same malicious EXE again, trusting is denied without having to analyze the EXE again in the micro-VM.
`MimeHandler.Executable.Open`	Turn this setting on to enable SOC mode. `0` - Execution of EXEs is blocked. The **Trust and Open** dialog is displayed when the EXE is double-clicked. (default.) `1` - Double-clicked executables open in the executable analyzer window. Ensure that `Lava.executablevmvisible = 1` (default is 1) to display the analyzer window.

`TrustFiles`	Use this setting to trust a specific file or files, using the following syntax:
	`TrustFiles --path="<file path>"`
	where `<file path>` is the location of the document. For example : `TrustFiles --path="C:\USERS\BRUSER\DOCUMENTS\IMPORTANT.DOCX"`
	To trust all untrusted files in a directory, enter the folder name. For example:
	`BrManage TrustFiles --path="C:\Users\BrUser\MyDirectory`

`Untrust-File`	Use this setting to mark a file as untrusted, using the following syntax: `untrust-file --path="<file path>"` where `<file path>` is the location of the document. For example : `untrust-file --path="C:\USERS\BRUSER\DOCUMENTS\IMPORTANT.DOCX"`
`Untrusted.ClipboardPolicy allow-cut-paste`	Controls how isolation constrains cut and paste access to and from documents or web pages in micro-VMs. `0` - Allow clipboard access initiated by the user, but block automated access `1` - Allow all clipboard access `2` - Deny all clipboard access `print` - Display the current value

Setting	Description
`Untrusted.Editing.Enabled`	Controls whether or not untrusted documents can be edited. If this option is disabled, users need to trust an Office document to be able to edit it. `0` - Do not allow editing of untrusted documents. Documents will open in Protected View. `1` - Allow editing of untrusted documents
`Untrusted.Enabled`	Controls whether or not isolation detects untrusted files on the system. You must log out and log in again for the change to take effect. `0` - Do not detect untrusted files. Untrusted files will open Office documents (such as Word, PowerPoint, and Excel) in "protected view". The user can click **Enable Editing** to reopen the document. `1` - Detect untrusted files `print` - Display the current value
`Untrusted.NetworkPassthrough`	Controls whether or not to enable pass-through mode for untrusted network shares. When enabled, isolation treats network shares as pass-through. A pass-through network share has no support for untrusted files. Any file (trusted or untrusted) that is saved on a pass-through network share is treated as trusted. `0` - Disable pass through mode `1` - Enable pass through mode
`Untrusted.OfficeMacrosEnabled`	Controls whether or not to enable macro support in Microsoft Office documents. `0` - Disable Office macros. Macros cannot run and the macro tool is not accessible in untrusted Office documents. `1` - Enable Office macros `print` - Display the current value The default is 1.
`Untrusted.TrustDrivePermissionsRequired` `trust-drive-perm`	Controls whether or not users can mark drives trusted and what authentication is required. `0` - Trusting drives is not permitted `1` - Allowed with administrative privileges `2` - All users are permitted to trust drives `print` - Display the current value

Setting	Description

`Untrusted.TrustedSMTPDomains`	Controls whether or not isolation automatically trusts email attachments from specified SMTP domains.
	
	Once configured, if you send a trusted attachment, it remains trusted for the receiver. If an untrusted attachment is sent, it remains untrusted for the receiver. Email attachment trust is retained only if the email originated from a Bromium-protected endpoint.
	
	This functionality has the following requirements:
	
	• Outlook is configured with a Microsoft Exchange Server connection
	• Outlook is not configured with a POP/IMAP server connection
	
	You can whitelist the following:
	
	• a domain,
	for example: `abc.com`
	• a specific sender,
	for example: `john@abc.com`
	• all child domains within a parent domain,
	for example: `*.ParentDomain.com`
	
	Entries must be in a comma-separated list.
	
	You can also choose to trust internal emails received from a non-Bromium-protected endpoint. To do so, specify the sender's SMTP email domain in the `Untrusted.TrustedSMTPDomains` setting, and set the following configuration to `On`:
	
	`Untrusted.OutlookAttachmentSecurityLevel = 4 (On)`
	`Untrusted.OutlookAttachmentSecurityLevel = 2 (Off)`

`Untrusted.WhiteListedContextMenuItems`	Extends the context menu with added text. For example: `brmanage config add-to-list --name=Untrusted.WhiteListedContextMenuItems --value="Scan with Microsoft Essentials..."` Log off and then log on for the change to take effect.
`Untrusted.DenyAccessToMaliciousFile`	Blocks particular file operations (trust, open, copy and paste, access by third-party software) when isolation detects that the file is malicious. `0` - Off `1` - On

User Interaction Settings

Setting	Description
`LCM.DeferrableTemplateCreationPolicy`	Isolation must reinitialize itself when certain desktop configurations change, for example, a change in the version of Java, Flash, or PDF. Use this configuration to choose the reinitialization behavior when the need to do so is detected. `0` - Immediately. Initialization occurs as soon as a new system update is detected, even if a user is logged in to the system. `1` - Only Manual. Initialization never starts automatically. The controller server is alerted that an initialization is required and you must explicitly start initialization using a remote command or the Desktop Console. `2` - User is logged out. Initialization starts if the user is logged off. `3` - Device is locked or user is logged out. Initialization starts if the device is locked or if the user is logged off. `4` - On system idle. Initialization automatically occurs when a user is not using the system. This includes states in which the device is locked, the user is logged off, or when the system has been idle. This is the default and recommended setting.
`Untrusted.ShowUntrustedFileIcons` `untrusted-icons`	Controls whether or not to mark untrusted files and drives with a Bromium logo to visually indicate that they are different from other files. `0` - Exclude the logo `1` - Include the logo `print` - Display the current value
`Untrusted.WarnUserOnAttemptToTrustFile` `trust-file-warning`	Controls whether or not isolation warns users when trusting any untrusted file. `off` - Do not warn `on` - Warn `print` - Display the current value
`UserInteraction.DisabledReminderInterval`	Controls the system tray reminder that can be configured to appear when isolation is disabled. `0` - Off any non-zero value - The interval (in minutes) at which the reminder appears Log off and then log on for the change to take effect

Setting	Description
`UserInteraction.UILevel`	Controls the display of pop ups and system tray icon messages on client systems. The Bromium system icon functionality is preserved. Pop ups are displayed in the bottom right of the screen. Balloon messages are displayed from the Bromium tray icon. Available values: `1` - No pop ups. No balloon messages. `2` - Critical pop ups. All balloon messages. `3` - Critical/major pop ups. All balloon messages. `4` - Critical/major/minor pop ups. All balloon messages. `5` - Same as 4 (default) Critical pop ups are shown for: • Initialization failed • Initialization blocked • License expired Major pop ups are not currently used. Minor pop ups are shown for license expiring.
`UserInteraction.ShowFeatures`	Controls whether or not the Features tab is displayed in the Desktop Console: `1` - Show `0` - Hide (default)
`UserInteraction.ShowTrayIcon`	Controls whether or not the Bromium system tray icon is displayed in the system tray and the Bromium shortcut is displayed in the Windows Start menu. `0` - Hide `1` - Show (default)
`vSentry.AllowDisableFromConsole` `disable-allowed`	Controls whether or not users can turn off isolation in the user interface. `0` - Prevent the user from disabling isolation `1` - Allow the user to disable isolation `print` - Display the current value
`vSentry.AllowUntrustedAccessDuringInitialization` `init-browsing`	`0` - Prevent Internet browsing and the opening of untrusted documents during initialization. `1` - Allow Internet browsing and the opening of untrusted documents during initialization. Systems are not protected during this time. (Default.) `print` - Display the current value.

Threat Rules

Setting	Description
`Lava.ExecutableVMVisible`	Controls whether or not to show the executable analyzer window. If SOC mode is on and this configuration is off, executable analysis results (suspicious, malicious, and so on) is displayed after the timeout. `0` - Do not show the executable analyzer window `1` - Show the executable analyzer window (default)
`Lava.HideExectuableAlerts`	Controls whether or not the .exe analyzer prompts for threat results. By default, prompts are hidden. The analyzer continues to generate threat alerts if an .exe file is found malicious, suspicious, or unknown. `0` - Receive result prompts `1` - Hide result prompts if the .exe analyzer does not find anything malicious, suspicious, or unknown
`Lava.RulesFiles`	Allows you to distribute custom rules to endpoints running isolation through the device policy. To use this setting, enter the path of the XML file containing your rules as the value for `Lava.RulesFiles`. For example: `Lava.RulesFiles = c:\Program Files\Bromium\CustomRules\rules.xml` Restart isolation to change this configuration.

Exporting and Importing Isolation Configurations Locally

You can use the BrManage utility to export the configuration of an isolation deployment to a structured policy file.

Exported policy files can be copied to individual Bromium deployments or a network share. They are located in `C:\Program Files\Bromium\vSentry\servers`.

Policy configuration files loaded locally (using `BrManage settings import` or the MSI installation switch `policiesxml= "c:\bootstrap_policy.xml"`) configure local settings only and do not change policy configurations if already set.

The policy configurations, if set, are owned by the controller server. If any local changes are made, they are overwritten by next policy update from the controller server. This also includes the removal of a group policy in the controller.

The following commands are available for importing or exporting settings:

Command	Description
`settings export --file`	Outputs the local configuration to a policy file in XML format. To output the file to the current directory, specify the file name only. To output the file to a local disk or network share, specify the full path, using the Uniform Naming Convention (UNC), and the file name. Syntax: `BrManage settings export --file=`*`filename`*`.xml`
`settings import --file`	Imports a policy from a local disk or a network share. Specify the full path and file name using the Uniform Naming Convention (UNC.) Syntax: `BrManage settings import --file=`*`filename`*`.xml`

Command	Description
`settings import --url`	Imports a policy from the controller server specified by the `url` argument. Syntax: `BrManage settings import --url=http[s]://server/filename.xml`
`settings clear`	Removes all configuration and policy information. Syntax: `BrManage settings clear`
`BrRemoteManagement --update-status-and-policy`	Imports the policy from the configured controller server immediately. This is an ideal way to quickly verify configuration changes made to a remote policy. Syntax: `BrRemoteManagement --update-status-and-policy`

Commonly Used BrManage Commands

This topic provides examples of commonly used BrManage commands. Browse to the Bromium install directory by using the `%brs%` environment variable.

Description	Command
Stop isolation	`# BrManage vSentry stop`
Start isolation	`# BrManage vSentry start`
Disable isolation	`# BrManage vSentry disable`
Re-enable isolation	`# BrManage vSentry enable`
Display Bromium license	`# BrManage vSentry.ProductLicenseKeys info`
Set the controller server URL	`# BrManage management-server http://your.company.server` Replace `http://your.company.server` with the controller server URL, including HTTP or HTTPS.

Allow Users to Copy and Paste Clipboard Contents	`# BrManage Untrusted.ClipboardPolicy print`
	`0`
	`# BrManage Untrusted.ClipboardPolicy 1`
	Restart isolation for the changes to take effect.
	`# BrManage Untrusted.ClipboardPolicy print`
	`1`
	`# BrManage vSentry start`

Add IP address to the trusted Internet sites list	`# BrManage Browser.TrustedSites add 216.139.0.95/8`
	Restart isolation-protected application(s) for the changes to take effect.
	`# BrManage Browser.TrustedSites print`
	`*.bromium.com`
	`216.139.0.95/8`

Enable Chrome protection	`# BrManage config set --name=browser.chrome --value=-1` Reinitialize isolation to enable Chrome protection.

Description	Command

Disable the untrusted documents functionality	`# BrManage Untrusted.Enabled off`
	Log out and log in again for the changes to take effect.
	Use the print command to verify the status of the untrusted functionality:
	`# BrManage Untrusted.Enabled print off`

Re-enable the untrusted documents functionality	`# BrManage Untrusted.Enabled on`
	Log out and log in again for the changes to take effect.
	Use the print command to verify the status of the untrusted functionality:
	`# BrManage Untrusted.Enabled print on`

Quarantine malicious files	`# BrManage config set --name=Untrusted.DenyAccessToMaliciousFile --value=1` Log out and log in again for the changes to take effect.

B Bromium Prechecker

There are a number of dependencies that must be addressed in order to successfully install Bromium products on a target system. Some software packages must be present, some system parameters need to be set, and the system itself must have a certain architecture. System architecture and software packages are checked during initial Bromium software installation. This level of verification should be sufficient for most installations. If problems arise, a more detailed checker is provided and can be run to pinpoint unsupported architecture and software. You can use the BrPreCheck utility to verify target systems before installing Bromium software. BrPreCheck is used to verify the suitability of a system to host and run Bromium products.

Running the Prechecker

You can run the BrPreCheck utility either manually in a command prompt on each target system or as an SCCM program to check multiple systems. Run BrPreCheck as an administrative user.

Because of system complexity and interdependencies, you may need to run BrPreCheck iteratively before the target systems pass all checks.

The BrPreCheck utility is included in the software installation package. It can be copied manually and run locally on select systems or copied and run remotely using SCCM.

BrPreCheck relies on special Bromium drivers to test part of the system and upon another executable to generate a report. If the Bromium platform is not already installed, you must include the `BrHostDrvSup.exe` and `BrReporter.exe` files in the same folder as the `BrPreCheck.exe` file. If it is not present while running BrPreCheck, BrPreCheck cannot perform Vt-x and extended page tables (EPT) checks.

An example BrPreCheck command line is:

```
BrPreCheck.exe -o=C:\User\IT\vSentry\bin
               -j=PrecheckJSON.json
```

BrPreCheck creates two files: a summary of the checks performed and a detailed log of each check performed. The default output names are *hostname*`-summary.txt` and *hostname*`.log`, respectively. Check the summary file first after running BrPreCheck. If errors are reported in the summary file, check the log file for more detailed information to determine the cause of the error. If you are unable to correct an error condition, run BrPreCheck again and enter `y` when prompted to upload status file to Bromium (or include `-u=1` on the command line.) Note the Upload ID number and call Bromium Customer Support for assistance.

The BrPreCheck command arguments are as follows:

Argument	Description
-c	Verbose mode. This argument displays BrPreCheck progress on the terminal screen as each check is being performed. By default, progress is not displayed. The summary file is the output of the `-c` and `-i` arguments.
-h	Displays BrPreCheck online help.
-i	Verbose mode. This argument displays on the terminal screen system information, such as the CPU type and speed and the versions of the software to be virtualized. By default, this information is not displayed. The summary file is the output of the `-c` and `-i` arguments.

Argument	Description

-j=*file*	Specifies the JSON (JavaScript Object Notation) file that determines the individual tests to perform. When the -j option is not included on the command line, an internal JSON file is used that performs each test using the default values. When the -j option is entered on the command line, include an edited JSON file in which only test values are changed. Each test must be present in the file, even those you want to skip. Change the value to skip or run a specific test. The default JSON *str*:*num* pairs are:
	`{`
	`"BrPreCheck.VT": 0,`
	`"BrPreCheck.Applications": 1,`
	`"BrPreCheck.OSVersion": 2,`
	`"BrPreCheck.WindowsLicenceKey": 0,`
	`"BrPreCheck.VSSService": 1,`
	`"BrPreCheck.VSSOperation": 2,`
	`"BrPreCheck.UserProfileWriteAccess": 0,`
	`"BrPreCheck.RegistryReadAccess": 1,`
	`"BrPreCheck.ProcessPermissionLevel": 2,`
	`"BrPreCheck.IPC": 0,`
	`"BrPreCheck.BrServiceConnectivity": 2,`
	`"BrPreCheck.HostServerConnectivity": 0,`
	`"BrPreCheck.IEBHOLoaded": 1,`
	`"BrPreCheck.OutlookExtensionLoaded": 2,`
	`"BrPreCheck.ShellExtensionLoaded": 0,`
	`"Applications": {`
	`"Adobe Reader": 0,`
	`"Silverlight": 1,`
	`"Flash": 2,`
	`"Internet Explorer": 0,`
	`"Java": 1,`
	`"Office": 2`
	`}`
	`}`
	where
	0 = skip the test
	1 = perform the test but a pass status is not required
	2 = perform the test and a pass status is required

-o=*file*	Specifies the path or the path and base name for the output files. Enter the full path using Uniform Naming Convention (UNC) notation. If the path does not exist, and the user has write permission to the specified folder hierarchy, the path will be created and the output files will be written to it. If the user does not have write permission, the output files will be placed in the `%TEMP%` folder (usually, `C:\Users\`*user*`\AppData\Local\Temp`). If the -o argument is not included, the output files are written to the local folder. The output files are *basename*`-summary.txt` and *basename*. If a base name is not specified, the host name is used instead.
-u=*int*	Specifies the action to take when prompted to "upload status file to Bromium (y/n)?" *int* may be `0` (prompt user), `1` (yes), or `2` (no). The default is `0`. Include this argument and set it to `1` or `2` when running BrPreCheck remotely; otherwise BrPreCheck will appear to hang as it waits for someone on the target system to respond to the prompt.
-s	Output to standard log location instead of file

The checks performed by BrPreCheck are not normally displayed on the terminal screen. To see the BrPreCheck results, check the output files.

The BrPreCheck session report can be uploaded to Bromium for analysis.

Run BrPreCheck in a command prompt because, when executed through an Windows Explorer window (that is, double-clicked), the window that is open during the course of the test is closed immediately after the utility completes.

When running BrPreCheck remotely, you can copy the output file back to the server in a manner you prefer. For example, you can configure SCCM to copy and run the BrPreCheck utility in **New Program Wizard/General/Command line** and copy the output file by running a `.bat` file in **New Program Wizard/General/After running**.

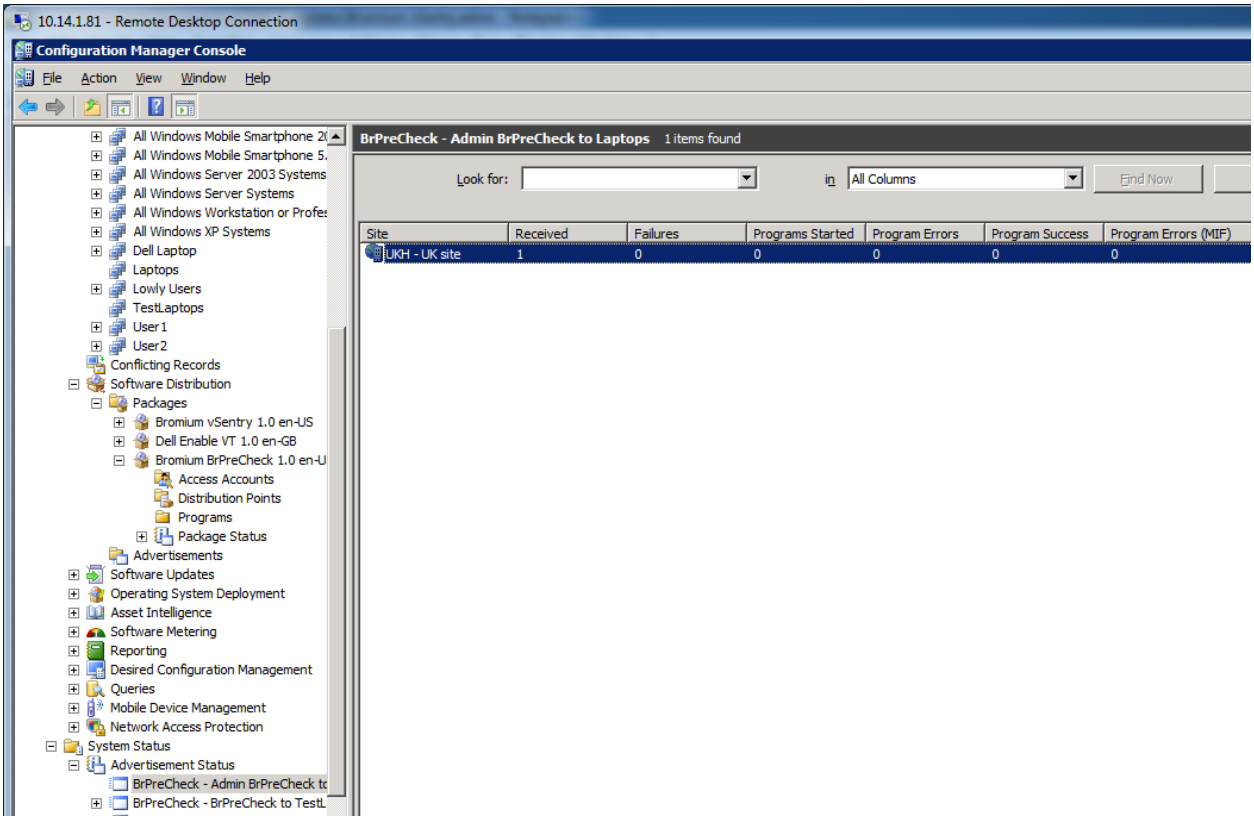
The output file includes details to assist debugging in the event a check fails. Analyzing BrPreCheck Output shows an excerpt of the output log file and provides some tips for debugging a failed check.

Remotely Monitoring BrPreCheck

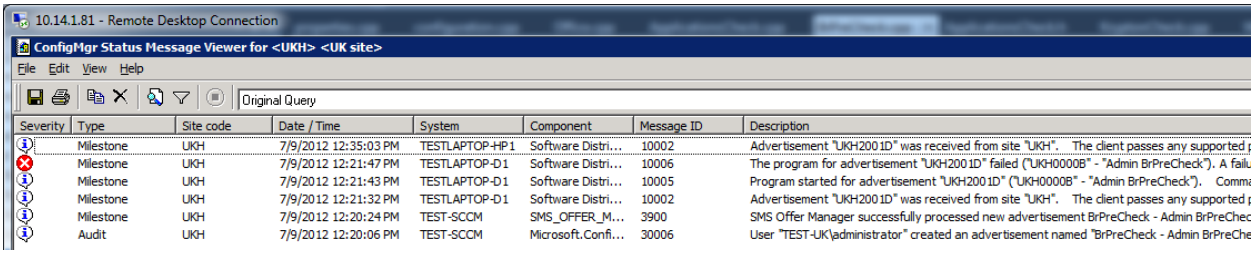
When using SCCM to run BrPreCheck on a collection of client systems, you can check BrPreCheck status for each client under SCCM **Advertisement Status** as BrPreCheck runs on the respective systems.

To check BrPreCheck endpoint status, right-click the site name and select the desired view from **Show Messages**.

For example:



Displaying the BrPreCheck advertisement



Displaying BrPreCheck advertisement status

In this example, a red X in the **Severity** column indicates that an error has occurred on a client system. BrPreCheck returns -1 when a test fails and 0 when it passes. The text for the failed example also indicates that an error occurred and displays the error message “A failure exit code of -1 was returned.” in the **Description** column.

Analyze the BrPreCheck output file to determine the cause of the failure.

Analyzing BrPreCheck Output

You can check the following categories:

Check	Description
BrService Connectivity Check	Verifies service connections
CPU Features Check	Verifies that the target system's CPU has the required features to support Bromium and that they are enabled: VT-x, EPT, PAE, NX/ND. If a target system has the required feature but it is not enabled, enable it or remove the system from the OU. Check the system documentation for information about checking and setting the features.
Device Drivers Check	Verifies device drivers
Explorer Shell Extension Loaded Check	Checks Windows Explorer
Host Server Connectivity Check	Checks the host:server connection
IE BHO Loaded Check	Verifies that Internet Explorer can support isolation
IE Version Check	Verifies the Internet Explorer version
Check if Microsoft Office has been activated	Checks that Microsoft Office is activated
Check if the VBA component is installed as required for Microsoft Office	Checks that Microsoft Office and VBA are installed
OS Activation Check	Verifies that the current Windows operating system is activated
OS Version Check	Verifies Windows 7 is running
Process Permission Level Check	Verifies that Bromium has the right permission level
Registry Read Access Check	Verifies that Bromium can write to the registry
Supported Language available	Verifies the language installed is supported by isolation
Untrusted Support Check	Verifies that isolation can support untrusted documents

Check	Description
User Profile Write Access Check	Verifies that the system's administrative user profile has write permission to the file system. If this check fails, verify that the user is part of the administrators group. This check is enabled by setting the `BrPreCheck.UserProfileWriteAccess` JSON string.
VSS Service Enabled Check	Verifies that the Volume Shadow Copy service is running on the system. This check is enabled by setting the `BrPreCheck.VSSService` JSON string.
VSS Shadow Operation Check	Verifies that the administrative user can perform VSS operations. This check is enabled by setting the `BrPreCheck.VSSOperation` JSON string.
Windows License Key Check	This check is enabled by setting the `BrPreCheck.WindowsLicenceKey` JSON string.

C Isolation for VDI

Isolation can run “nested” in a Windows 7, Windows 8, or Windows 10 64-bit or 32-bit virtual machine on VMware ESXi 5.1.0 or later.

Functionality is identical to isolation running on physical machines; however, performance characteristics may differ. When running isolation in a nested environment, you are also dependent on the security of the underlying third-party hypervisor.

VDI System Recommendations

Isolation uses virtualization to isolate untrusted tasks; hardware-assisted virtualization capabilities must be available and passed to the VDI guest VMs by the hypervisor. This is typically referred to as *nested virtualization*.

In this release, only VMware vSphere supports nested virtualization. Additionally, isolation only supports nested virtualization when running on modern Intel CPUs with VT-x and EPT enabled in the BIOS. Guest VDI VMs must have the following hardware configuration as a minimum:

Component	Description
vSphere	ESX version 5.5 update 2 or later
CPU	Intel Xeon Processor or later with VT-x and EPT enabled in the BIOS
VM Guest Hardware	Version 10 or later
Guest CPU Configuration	Enable Hardware virtualization Enable Hardware CPU and MMU
Guest vCPU Configuration	Two virtual CPUs minimum
Guest Memory Configuration	Minimum: 4 GB RAM Recommended: 5 GB RAM
Isolation	Version 3.2 Update 3 or later is supported; however version 4.0 is recommended

Note: It is recommended that you add the following setting to the config file in the `etc/vmware` directory on all servers running ESX 5.5 or later on Intel Xeon Processors or later:

```
monitor_control.disable_gphys_abit = "TRUE"
```

Setting Up the VDI Environment

Isolation has optional configuration parameters that can be tuned to adjust performance. Since isolation running in VDI requires separate configuration policies, it is recommended that a separate policy is created on the controller and applied to the VDI machines. Additionally, a separate policy may be needed based on whether or not the VDI images are pooled non-persistent VMs or dedicated persistent VMs.

Recommended controller settings for pooled and persistent VDI:

- Unless required temporarily for troubleshooting, ensure that the **Logging Level** in the Manageability tab is set to no higher than **Event** to minimize the IOPS generated for logging purposes
- Advanced policy recommendation: the `LCM.uVMCPUCount = 1` setting reduces the virtual CPU count within the micro-VM to one. This reduces host CPU usage and improves overall session response.

Recommended settings for pooled VDI set in the policy:

- Since pooled VDI is based on a master image and reset at reboot, it should never reinitialize. Set the **Initialization Behavior on System Updates** in the User Interaction tab to **Manual**.
- Advanced policy recommendations:
  - `UserInteraction.UILevel = 1`: this setting eliminates the pop up messages on the system tray icon. Often these messages offer to reinitialize or other options not applicable to non-persistent VDI. Full functionality of the icon and the desktop console is unaffected.
  - `LCM.CriticalTemplateCreationPolicy = 1` and `LCM.DeferrableTemplateCreationPolicy = 1` : these settings prevents automatic reinitialization since this is not required as the master image contains the initialized template

The following provisioning methods are supported:

- Citrix XenDesktop:
  - Machine creation services
  - Provisioning services
  - Sysprep and standalone VM creation
- VMware Horizon View version 7:
  - Full clones
  - Linked clones
  - Instant clones
  - Sysprep and standalone VM creation

Creating and Updating Master Templates

If isolation is preinstalled as part of a master image, it is important to perform an initialization prior to sealing and deploying the master image. When updates are applied to the master image, a reinitialization may be required. It is important to ensure that the master image has a successful and complete initialization performed before it is deployed.

Additionally, when deploying isolation as part of a master image in pooled VDI or preloading isolation into a master image that is used to create persistent images, remove the unique ID from the registry that identifies the installation within the controller. When creating the initial master image or updating an existing master image, the following steps must be performed after the image has been initialized and immediately prior to sealing or capturing the image:

1. Use or create a "typical" user account with commonly used settings (group policy settings, policies, and so on.) This ensures that a template is created with the correct settings for your typical users. Log in to this account to create the master template.
2. Stop the Remote Management Service.
3. Close the BrConsole.exe process.

4. Delete the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Bromium\vSentry\State\BMS.ClientToken`
5. Set `Browser.Sync.ZoneSettings` to `off`.

These actions can be placed into script that can be run immediately prior to sealing and capturing the image. For example:

```
net stop "Bromium vSentry Remote Management Service"

taskkill /F /T /IM "BrConsole.exe"

reg delete "HKLM\SOFTWARE\Bromium\vSentry\State" /v "BMS.ClientToken" /f /reg:64
```

Configuring Profile Technologies

Many VDI implementations use third-party profile technologies to save user settings between sessions, and is often used for VDI implementations that use pooled non-persistent desktops. These technologies copy files from a user's profile location at log off to a central file server and back to their session again when they log on.

When users download files marked as untrusted by isolation to their profile, metadata is tagged to flag that the file should continue to be untrusted and opened inside a Bromium micro-VM. It is critical that this metadata be preserved when the profile technology saves the file back to the central file server. This is required so that untrusted files are not inadvertently marked as trusted when a user logs onto a new VDI session.

To allow the profile tool to be able to see the metadata so that it can be preserved on the central server, the processes of the profile technology must be added in the controller. In the Policies page Advanced tab, add the setting `Untrusted.PassthroughProcesses` with one of the following values:

- `UserProfileManager.exe`: Citrix user profile manager
- `VMWVphelper.exe` and `VMWVvpsvc.exe`: view persona management

Note: A crash may occur on micro-VMs using View Persona Management with linked clones when a user without a locally cached profile logs in to a linked clone running isolation. To resolve this issue, set the VMware View Persona Management policy **Cleanup CLFS Files** using GPO for any systems using View Persona Management by loading the `ViewPM.adm template`.

Persisting Bromium Chrome Settings

The browser settings for Chrome are typically located in the user profile directory under `AppData\Local\Google\Chrome\User Data`. For Bromium-protected Chrome, these settings are stored under `AppData\Local\Bromium\vSentry\BrChromium\User Data`.

By default, Microsoft Roaming Profiles and some third-party profile tools do not synchronize these directory locations across sessions. If non-persistent VDI desktops are being used, files must be synchronized during the log on and log off process for personal Chrome settings for users to persist. Typically, the following Chrome settings should be persisted across sessions of non-persistent VDI:

- Bookmarks
- History
- Chrome Extensions

To preserve these settings without synchronizing unnecessary data, the following files and folders should be synchronized:

- Directories:

```
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Databases

AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Extensions

AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Extension State

AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Local Extension Settings

AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Extension Rules
```

```
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Local Storage
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Managed Extension Settings
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Web Applications
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Storage
```

- Files:

```
AppData\Local\Bromium\vSentry\BrChromium\User Data\First Run
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Bookmarks
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Bookmarks.bak
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Cookies
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Favicons
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\History
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Login Data
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Preferences
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Secure Preferences
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Shortcuts
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Top Sites
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Web Data
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Visited Links
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Extension Cookies
AppData\Local\Bromium\vSentry\BrChromium\User Data\Default\Google Profile
AppData\Local\Bromium\vSentry\BrChromium\User Data\Local State
```

Directory Exclusions

Isolation stores settings for each user locally in the user profile under the following directories:

- `AppData\Local\Bromium\vSentry`
- `AppData\LocalLow\Bromium\vSentry`

The majority of these files should not be synchronized as part of a user's profile. By default, Microsoft roaming profiles will not synchronize files from `AppData\Local` or `AppData\LocalLow`; however, many third-party profile solutions synchronize these local AppData folders. Add exclusion rules to any third-party profile technology to exclude these directories from synchronizing as part of the user profile.

If Chrome protection is enabled, files and subdirectories under `AppData\Local\Bromium\vSentry\BrChromium\User Data` should be synchronized. It is advisable to add an exclusion rule for `AppData\Local\Bromium\vSentry` and then add a specific inclusion rule for the specific BrChromium files. Inclusion rules typically take precedence over exclusion rules.

Tuning VDI for Maximum Performance

To ensure that users have a good experience and the resources needed to run isolation, it is important that you implement many of the tuning parameters on the VDI system. Refer to the following optimization guides and tools for details on optimizing Windows images for VDI:

- Citrix Windows 7 Optimization Guide:

  http://support.citrix.com/article/CTX127050

- VMware OS Optimization Tool:

  https://labs.vmware.com/flings/vmware-os-optimization-tool

- VMware Horizon with View Optimization Guide for Windows 7 and Windows 8:

  https://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf

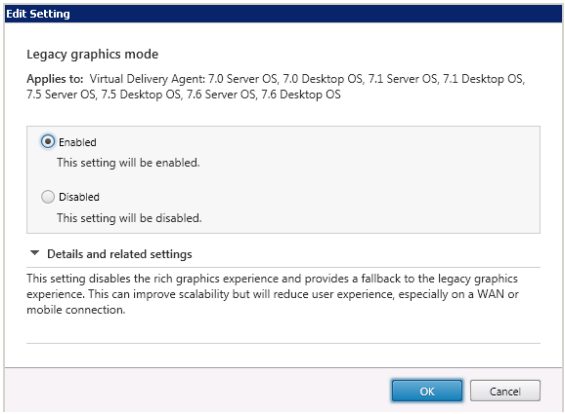
Citrix ICA/HDX Protocol Policy

The Citrix ICA/HDX protocol has several different graphics modes, some of which can be CPU intensive on the server and designed for use cases where uses are running high definition video or graphically intense applications. If users do not spend the majority of their time in these types of applications, it is recommended that you use the traditional Thinwire ICA protocol with Adaptive Display. Since CPU resources in VDI are often a limiting factor in performance and scalability, it is recommend the H.264 codec be disabled.

Refer to Citrix's recommendations around their HDX Flash Redirection technology: http://www.citrix.com/products/xendesktop/support/hdx-flash-redirection-security-information.html.

Windows 7 VDI

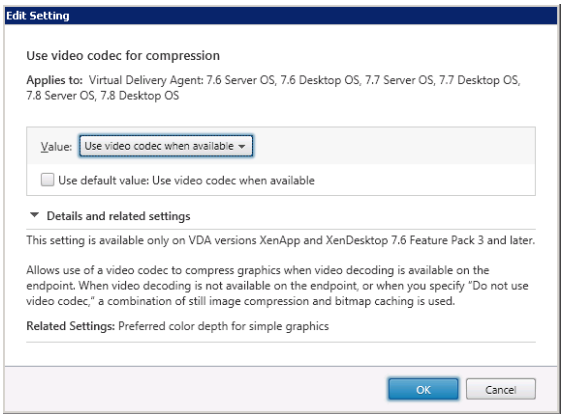
The following Citrix policy should be set to enable the more CPU efficient codec for Windows 7. Set the graphics policy on XenDesktop 7.0 and later as follows:



Windows 8.1 or 10 VDI

If you are running Windows 8.1 or Windows 10 VDI sessions hosted on Citrix XenDesktop, it is recommended to use XenDesktop 7.6 Feature Pack 3 or later. For users that do not spend the majority of their time running highly graphical applications, it is also recommended to disable the H.264 rendering and leverage the new Thinwire Plus protocol.

Set the graphics policy on XenDesktop 7.6 Feature Pack 3 and later as follows:



Limiting HTML and Flash Advertisements

Web browsing can be one of the most resource-intensive applications hosted in a VDI environment. Often it is not the actual web content that users view that causes high resource usage, but excessive Flash and HTML5 advertisements.

There are several ways that desktop resource usage can be improved by limiting unnecessary advertisements on VDI systems. Bromium recommends that you implement one of the following methods:

• Block unwanted ad sites at the Proxy/Network perimeter

• Implement Adblock or Adblock Plus

• Implement a custom HOSTS file in the master VDI image such as MVPS HOSTS: http://winhelp2002.mvps.org/hosts.htm

Sizing and Scalability Considerations

Each VDI environment is unique; to truly understand the scalability impact of enabling isolation on VDI, conduct a detailed analysis and a pilot or by simulate a real production workload with a tool such as LoginVSI. The following guidelines can be used for general planning purposes as long as the VDI tuning recommendations in Setting Up the VDI Environment have been implemented and isolation version 3.1 or later is used.

CPU Considerations

Running isolation fully optimized on VDI will increase overall host CPU usage on average between 10 - 30%. If isolation is being implemented on a VDI system already in production, Bromium recommends that the average CPU usage during peak business hours for each physical vSphere host be reviewed. If average CPU usage on a host is at or below 65% during peak business hours, the host should have enough CPU resources to enable isolation with affecting VM density from a CPU perspective. On VDI systems where each VDI VM is given two vCPUs, you can run VDI with isolation enabled at a density of up to five VMs per physical core.

Memory Considerations

Running isolation on VDI increases physical memory consumption within the guest VM on average between 600 – 1200 MB RAM. Isolation requires that the guest VM have a minimum of 4GB RAM. In most instances it is often advised to avoid over committing memory on isolation hosts. However, the transparent page sharing feature of vSphere can save memory and hosts can be safely overcommitted without going into a swap state if the overcommit ratio is kept to less than 10% total host memory. For example, assuming that a physical host has 384 GB RAM, then the total memory allocated to booted VMs could be as high as 422 GB RAM before the host would risk entering a swap state.

D High Availability

High availability is achieved by adding additional machines to your controller deployment to create a server cluster. A clustered environment requires the following additional components:

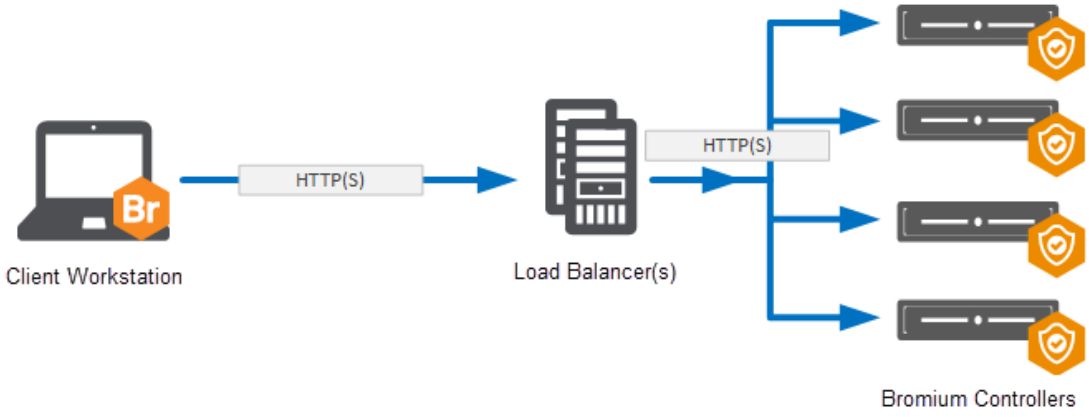
- Two or more machines to run controller instances
- Load balancing software (installed on its own machine) or physical load balancer or round-robin DNS for routing work to machines in the cluster
- Configuration of controller machines to communicate with the load balancer

A clustered controller environment has the following benefits:

- High availability
- Disaster recovery
- No single point of failure
- Stateless
- Increased endpoint count support (100,000+ per cluster)

Architecture

The following diagram depicts the high level architecture of hardware load balanced Bromium Controller servers. This diagram shows a single client connected to a load balanced address which then gets routed to one of the load balanced controller servers. This diagram does not take into account the various SSL load balancing modes that can be used or how the DNS aliases, certificates, or load balancers should be configured. These topics are discussed in further detail later in this chapter.



Using Load Balancing

There are primarily two reasons to load balance controller servers: scalability and high availability. Although a single controller server can scale to support 10,000+ devices, there are many environments that necessitate larger scales that require multiple controller servers to support all endpoints. In addition, if a single controller server can support a large number of clients, this is not necessarily the recommended configuration. The other reason to load balance controller servers is for high availability. This ensures that if a single (or in some cases multiple) controller servers fail, the remaining controller servers are able to handle the client connections. Although the controller servers can be load balanced through legacy methods such as DNS round robin, this chapter tells you how to configure hardware load balancing for the controller servers. Hardware load balancing provides numerous benefits over legacy DNS round robin including faster failover times, more reliable health checking, and the ability to easily move servers in and out of service.

The architecture of isolation means that the clients can function as normal in the event that the controller is unavailable. A store-and-forward architecture on the client ensures that any stored events or threat reports are uploaded once the controller becomes available again. High availability is therefore optional, however it is desirable if businesses want to maintain real time visibility and the ability to make changes to endpoint policies

Select and Set Up a Load Balancer

Choose a load balancing solution that best meets the enterprise's needs and follow the vendor's installation and configuration steps. The load balancer must be capable of acting as an SSL endpoint and support returning HTTP redirections.

Guidelines for load balancers:

- Configure an IP address for the load balancer
- Load balance traffic across controller servers
- Act as an SSL endpoint for port 443 and load balance traffic on that port across controller servers
- The load balancer should perform frequent health check HTTP GET requests to a specific URL and take servers temporarily out of rotation if it receives an HTTP status 503 response

Encryption and Load Balancing Modes

There are four main SSL encryption options when using a hardware load balancer:

- **SSL Bridge**: SSL bridge is a form of load balancing in which the back end controller and IIS servers own the SSL connection and a server certificate is applied to them. The hardware load balancer does not handle any of the encryption and only load balances traffic between the web servers.

  This configuration allows for end-to-end encryption without applying a significant load to the hardware load balancer. In addition, this configuration can be easier to implement as it does not require any certificates to be managed by the hardware device.

- **SSL Offload**: In SSL offload load balancing, the SSL connection is owned by the hardware load balancer. In this scenario, the client connects to the hardware load balancer over SSL and then the connection between the load balancer and the controller servers are unencrypted.

  This configuration drastically reduces the load on the controller servers by removing the SSL encryption from the servers, which can be a resource-intensive process. This then allows increased scalability on the controller servers.

- **SSL to SSL**: SSL to SSL load balancing SSL connection is owned by both the hardware load balancer and the controller servers. In this scenario, a client connects to the hardware load balancer over SSL and then the hardware load balancer creates a new SSL connection to the controller servers.

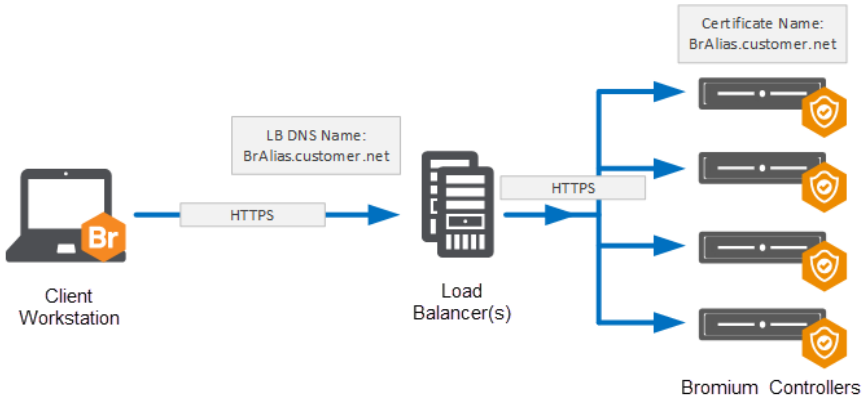
  The main benefits of this configuration is that it allows for end to end encryption while reducing the load on the controller servers versus the SSL offload method. This reduced load occurs because the hardware load balancer is able to aggregate multiple SSL sessions to the controller servers which reduces the number of individual sessions that are managed by the controller servers.

- **No SSL**: In this scenario, there is no SSL connection of any kind. The client connects to the load balancer unencrypted and the load balancer connects to the controller server unencrypted. The primary benefit to this configuration is ease of configuration for testing and lab environments.

Based on the encryption and load balancing mode chosen, a corresponding DNS alias and certificate architecture then needs to be implemented. The following diagrams show how the certificates and DNS aliases should be configured for each mode.

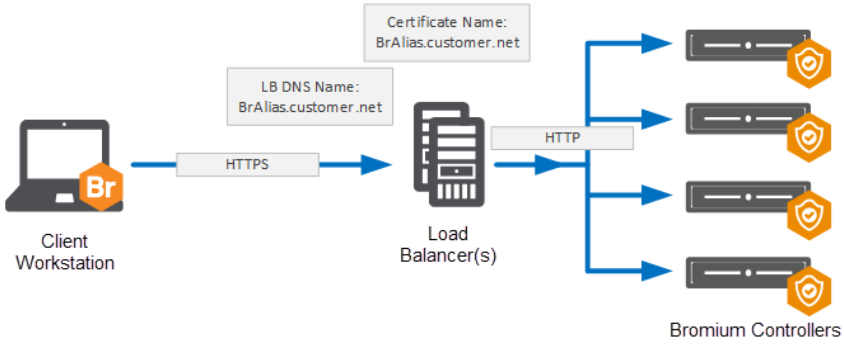
SSL Bridge

For the SSL bridge configuration, a DNS alias is created for the load balanced IP address and a certificate is created to match the FQDN of the DNS alias. This certificate is applied to each of the controller servers. The client workstation is then configured to connect to the same DNS alias.



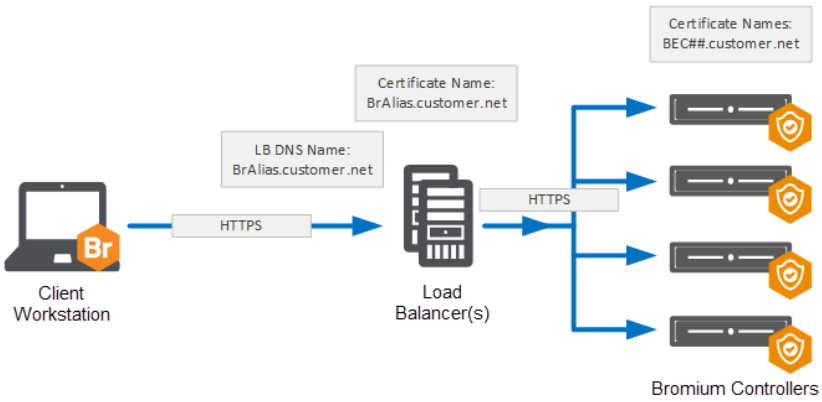
SSL Offload

For the SSL offload configuration, a DNS alias is created for the load balanced IP address and a certificate is created to match the FQDN of the DNS alias. This certificate is then applied to the load balanced IP address on the hardware load balancer.



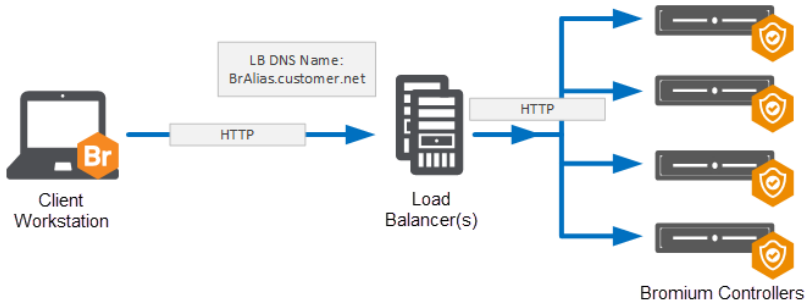
SSL to SSL

For the SSL to SSL configuration, a DNS alias is created for the load balanced IP address and certificate is created to match the FQDN of the DNS alias. This certificate is applied to the load balanced IP address on the hardware load balancer. In addition, one or more separate certificates are created and applied to the controller servers. The load balancer is then configured to communicate over SSL to each of the controller servers.



No SSL

For the No SSL configuration, a DNS alias is created for the load balanced IP address. No certificates need to be created for this configuration because there is no SSL encryption.



Load Balancing Configurations

When configuring a load balanced server, three primary configurations need to be made. First, configure the Load Balancing Monitor or health probe that will be used to determine if the backend server is considered available or not. The second configuration is the Persistence which determines how the load balancer ensures that a single client connection continues to communicate to the same server over the life of the connection. The third is the Load Balancing Method which determines which backend server a new client connection gets routed to.

Recommended Configurations

The following table contains recommended configurations for load balancing a controller server with an explanation for each configuration:

Configuration Type	Recommendation	Description
Load Balancing Monitor	HTTP Request: GET [server] /static/test.json Response Code: 200	The test.json file exists on all controller servers. This HTTP request will attempt to GET this test file. If it successfully retrieves this file, it will get a 200 response code. This will ensure that both IIS is up and running as well as the controller having been installed on the server.
Persistence	Options: Source IP (All load balancing modes) SSL Session (SSL Offload / SSL to SSL) No Persistence	Source IP is a simple configuration which works well for all load balancing modes. This persistence method works well in flat networks that do not use any type of NAT between client devices and the controller servers. SSL Session can be used if the hardware load balancer is performing SSL. This persistence method should be used if NAT is being used between client devices and the controller servers
Load Balancing Method	Least Connection	This connection method ensures that the client connections are evenly spread across all available controller servers. In general, the client connections are short-lived connections, so the load should get evenly spread across all servers.

E Third-party Product Exclusions

Overview

The following information discusses general guidelines for creating exclusions for third-party endpoint security products so that they do not interfere with or prevent the normal operation of isolation. Necessary actions may consist of excluding all isolation 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 isolation initialization and slow or blocked browsing and opening of untrusted documents.

To stop third-party products from interfering with isolation, certain exclusions need to be created on the system so that isolation processes and binaries are whitelisted. In particular, rules should be created that whitelist the following isolation directories or files on the system:

Directories Exclusions

```
%userprofile%\AppData\LocalLow\Bromium

%userprofile%\AppData\Local\Bromium

%programfiles%\Bromium

%programdata%\Bromium
```

File Exclusions

```
BrConsole.exe

BrDesktopConsole.exe

BrDownloadManager.exe

BrExeScanner.exe

BrHostDrvSup.exe

BrHostSvr.exe

BrInstaller.exe

BrInstallerPopup.exe

BrLauncher.exe

BrLogMgr.exe

BrManage.exe

BrNav.exe

BrPreCheck.exe

BrProgressDialog.exe

BrRemoteManagement.exe
```

```
BrRemoteMgmtSvc.exe
BrReporter.exe
BrSecurityAlertInspector.exe
BrService.exe
BrStatusMonitor.exe
BrWinFile.exe
chrome.exe
dpinst.exe
getcaps.exe
HostPcapDump.exe
Br-hostconfig.exe
Br-init-a.exe
Br-init-c.exe
Br-init-l.exe
Br-init-m.exe
Br-init-n.exe
Br-init-o.exe
Br-init-w.exe
Br-uxendm.exe
uxenctl.exe
uxenctx.exe
```

Symantec Endpoint Protection

Symantec Endpoint Protection can be configured to block the execution of unknown process on the system, resulting in the br-uxendm.exe process not getting launched when trying to browse untrusted sites or open untrusted documents. Policy exceptions should be created in SEP to either exclude all isolation binaries from the AV scan or exclude all isolation folders from the AV scan. For more information, see http://www.symantec.com/docs/HOWTO80920

1. Log in to the SEPM and click **Policies**.
2. Under **View Policies**, click **Centralized Exceptions**.
3. Under **Tasks**, click **Add a Centralized Exception policy**. This creates and opens a new Centralized Exceptions Policy.
4. In the left pane, click **Centralized Exceptions**.
5. Click **Add**, hover the mouse over **Windows Exceptions**to display the menu and select **Folder**.
6. Check **include subfolders**.
7. Under **Specify the type of scan that excludes this folder**, select **All**.
8. You must whitelist four directories. You can add an `%appdata%` variable using one of the built in prefixes `COMMON_APPDATA`

Note: Do not use the built in `%PROGRAMFILES%` prefix, as this always defaults to the 32-bit directory due to the fact that the client is a 32-bit application. Include the explicit program files path.

SEP can be configured to output logs in one of the following locations:

```
C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.1101.401.105\Data\Logs
```

or

```
C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint
Protection\12.1.1101.401.105\Data\Logs
```

You can also go to the View Logs tab in the SEP client UI.

McAfee Virus Scan / HIPS

HIPS logs can be found here: https://kc.mcafee.com/corporate/index?page=content&id=KB72869

McAfee Host Intrusion Prevention injects into the running process on the system and can significantly degrade the performance of isolation. The following article describes how to exclude directories from McAfee AV scan: https://kc.mcafee.com/corporate/index?page=content&id=KB50998

Either turn off Process Spoofing (uncheck block) or exclude br-uxendm.exe from the process spoofing check. This is done under the Access Protection policy in ePO, then Anti-Virus Standard Protection. Select Prevent Windows Process Spoofing and add the exclusion. Add `br-uxendm.exe` separated by a comma and not by a semicolon.

In some cases, excluding the four Bromium standard directories may not work. This may be true particularly if the administrator has increased the sensitivity level of McAfee scan analyzer to medium-high (the default is low-medium.) In this case, create exclusions for each of the Bromium processes listed in File Exclusions.

Digital Guardian

To avoid performance issues with Digital Guardian and isolation, configure the Digital Guardian resource file `(PFF = process flag file)` to whitelist all Bromium processes.

1. In the Digital Guardian management console (DGMC), create a dynamic group called “Bromium” (for example) and add the test system/s to that dynamic group.
2. Update their current master PFF file and include the below listed Bromium processes to it.
3. Apply the updated PFF file to the dynamic group created in step 1.
4. Once the Digital Guardian Agent communicates with DGMC, verify on the test system that updated PFF file included all Bromium processes. The Digital Guardian configuration file `prcsflgs.dat` is in the `C:\Program Files\DGAgent\` folder.

Note: If the Digital Guardian agent is running in stealth and/or tamper mode, you need to terminate the Digital Guardian agent to grant access to this file.

Next, you may need to rewrite some Digital Guardian rules for network operations-related tasks if they implemented with Digital Guardian, for example, network transfer upload or download (NTU/NTD.) In this case, collect the information for these rules and contact Bromium Support.

Process flags used to whitelist Bromium processes:

```
Br-hostconfig.e,NI+NC+ND+NR+SK+TR

Br-init-a.exe,NI+NC+ND+NR+SK+TR

Br-init-b.exe,NI+NC+ND+NR+SK+TR

Br-init-c.exe,NI+NC+ND+NR+SK+TR

Br-init-l.exe,NI+NC+ND+NR+SK+TR

Br-init-m.exe,NI+NC+ND+NR+SK+TR

Br-init-n.exe,NI+NC+ND+NR+SK+TR

Br-init-p.exe,NI+NC+ND+NR+SK+TR
```

```
Br-init-w.exe,NI+NC+ND+NR+SK+TR
Br-uxendm.exe,NI+NC+ND+NR+SK+TR
kdd.exe,NI+NC+ND+NR+SK+TR
uxenctl.exe,NI+NC+ND+NR+SK+TR
uxendm.exe,NI+NC+ND+NR+SK+TR
vhd-util.exe,NI+NC+ND+NR+SK+TR
xenctx.exe,NI+NC+ND+NR+SK+TR
BrConsole.exe,NI+NC+ND+NR+SK+TR
BrDesktopConsol,NI+NC+ND+NR+SK+TR
BrDownloadManag,NI+NC+ND+NR+SK+TR
BrHostDrvSup.ex,NI+NC+ND+NR+SK+TR
BrHostSvr.exe,NI+NC+ND+NR+SK+TR
BrIEHelper.exe,NI+NC+ND+NR+SK+TR
BrIEHelper64.ex,NI+NC+ND+NR+SK+TR
BrInstaller.exe,NI+NC+ND+NR+SK+TR
BrInstallerPopu,NI+NC+ND+NR+SK+TR
BrLauncher.exe,NI+NC+ND+NR+SK+TR
BrLogMgr.exe,NI+NC+ND+NR+SK+TR
BrManage.exe,NI+NC+ND+NR+SK+TR
BrNav.exe,NI+NC+ND+NR+SK+TR
BrPolicy.exe,NI+NC+ND+NR+SK+TR
BrPreCheck.exe,NI+NC+ND+NR+SK+TR
BrProgressDialo,NI+NC+ND+NR+SK+TR
BrRemoteManagem,NI+NC+ND+NR+SK+TR
BrRemoteMgmtSvc,NI+NC+ND+NR+SK+TR
BrReporter.exe,NI+NC+ND+NR+SK+TR
BrSecurityAlert,NI+NC+ND+NR+SK+TR
BrService.exe,NI+NC+ND+NR+SK+TR
BrStatusMonitor,NI+NC+ND+NR+SK+TR
BrWinFile.exe,NI+NC+ND+NR+SK+TR
getcaps.exe,NI+NC+ND+NR+SK+TR
BrDeprivilege.e,NI+NC+ND+NR+SK+TR
Autonomyhelper3,NI+NC+ND+NR+SK+TR
BrDeprivilege.e,NI+NC+ND+NR+SK+TR
BrExeScanner.ex,NI+NC+ND+NR+SK+TR
dpinst.exe,NI+NC+ND+NR+SK+TR
HostPcapDump.ex,NI+NC+ND+NR+SK+TR
```

You can verify the exclusions list in Digital Guardian configuration file `prcsflgs.dat` in the `C:\Program Files\DGAgent\` folder.

Digital Guardian Agent can be configured for stealth and tamper mode. If the performance issue continues even with exclusions done as described above, perform the following steps:

1. Terminate Digital Guardian.
2. Disable all Digital Guardian drivers if performance issues continue, even after terminating Digital Guardian.

BeyondTrust PowerBroker

PowerBroker for Windows allows privilege management by removing or enforcing administrative privileges from users, maintaining application access control, or simply logging privileged activities.

The following exclusions must be added to the PowerBroker product:

`c:\Program Files\Bromium\vSentry`

`c:\ProgramData\Bromium\vSentry`

There are also certain exception rules that can be configured in PowerBroker in which any user request may get elevated and files that invoke a UAC prompt cannot be trusted.

To fix this issue, remove UAC from the trust file function using the **File types requiring administrative privilege to trust** documents policy option in the controller.

Citrix Receiver Internet Explorer Plug-in

The Citrix Receiver plug-in causes a lengthy delay when new uVMs are launched in the browser. Once the original delay has occurred, continuous browsing of that TLD appears normal. With each new TLD, the delay is repeated.

To resolve this issue, disable (or uninstall) the Internet Explorer plug-in in the **Internet options >manage Add-ons** window.

Trend Micro OfficeScan

Exclusions for the Bromium directories and VolumeShadowCopy files can be applied to Trend Micro to improve initialization times and general machine performance. To do this:

1. Log in to the OfficeScan management console:

    - For OfficeScan 10.6 and earlier:

    Click **Networked Computers > Client Management**, then select the server or workgroup on which the backup is located.

    - For OfficeScan 11.0:

    Click **Agents > Agent Management** and select the server or workgroup in which the backup is located.

    - For OfficeScan 10.6 and earlier:

    Click **Settings > Scan Settings > Real-time Scan Settings**.

    - For OfficeScan 11.0:

    Right-click the server or workgroup and click **Settings > Scan Settings > Real-time Scan Settings**.

2. On the Target tab in the **Scan Exclusion List (Directories)** area, enter `C:\Program Files\Bromium|C:\ProgramData\Bromium|C:\Users\*\AppData\LocalLow\Bromium|C:\Users\*\AppData\Local\Bromium` then click **Add**.
3. Click **Apply to All Clients** to save the changes.

Confirm these exclusions are in place on the endpoint by checking the following registry entry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration`

When both Dell Credant Data Protection and Trend Micro OfficeScan Client software are installed and running, users may experience hang or system unresponsiveness. This issue occurs when TrendMicro Scan Engine scanning threads are intercepted by Credant's CMGShCEF.sys driver and vice versa, creating excessive scan threads for the system.

1. In the OfficeScan Server, open the `PCCSRV\ofcscan.ini` file and add the following lines in the `[Global Setting]` section:

```
[Global Setting]

RegCount=2

Reg1.Description=VSAPI CFI Flag

Reg1.Key=!CRYPT!84037165B03F2E61D3212DF0527D84E8D56F1B04DE3093DD8464D3D7B7DAD3655E4A6
B732387EC7A53F5397320C19AAD0FF52CDD44D4D77B58B2B730BA6EFB93C2B4B017734!20BD3D21041E62
5215008B3EDC4EB4F18451774653F

Reg1.Value=1

Reg2.Description=VSAPI SecI Flag

Reg2.Key=!CRYPT!840FEA4427D119052DE12DF0527D84E8D56F1B04DE3093DD8464D3D7B7DAD3655E4A6
B732387EC7A53F5397320C19AAD0FF52CDD44D4D77B58B2B730BA6EFB93C2B4B017B30!20CD3D21041E62
52150E2BFE035151A93815E17006C

Reg2.Value=5
```

2. Log in to the OfficeScan web console and go to the **Networked Computers > Global Client Settings** tab. Click **Save** to deploy settings to OfficeScan clients.
3. Connect to one of the OfficeScan client computers and enure that the following registry entries are created:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TmFilter\Parameters]

"CFI"=dword:00000001

"SecI"=dword:00000005
```

4. Reboot the system and verify the result.

Additionally, you can exclude Dell's working directories and file extension in the OfficeScan Realtime Scan Settings:

```
[Folder Exclusion]

C:\Program Files\Dell

C:\Windows\CSC\v2.0.6\namespace

[File Exclusion]

*.CEF
```

Dell Data Protection

Dell Data Protection is a third-party disk encryption product that may experience faulty behavior with hardlinks. To avoid this, exclude the `ProgramData\Bromium\vSentry` folder from encrypted folder lists. Check `C:\ProgramData\CREDANT\CMGShield.log` to verify that the isolation folders are excluded.

To ensure that Credent is installed in the system, create a list of installed and device drivers on the system by running `BrPrecheck.exe`. The list is created in the `output log` file and flags any conflicting system drivers (such as Credant Encryption) found on the system.

Avecto Privilege Guard

Avecto Privilege Guard may cause errors with Internet Explorer and Chrome. To avoid this, locate or create a multi-string value named `HookExclusions` in the following reg keys:

`Win7 32bit - HKEY_LOCAL_MACHINE\SOFTWARE\Avecto\Privilege Guard Client`

`Win7 64bit - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avecto\Privilege Guard Client`

For the value, add the Bromium directories (`C:\Program Files\Bromium` and `c:\ProgramData\Bromium`) separated by a semicolon.

Also, configure the isolation policy so that UAC (administrator permissions) do not become an issue:

- Allow trusting files by non-administrators
- Allow disable by non-administrators

To create exclusions for Avecto using GPO:

1. In the Avecto Privilege Guard MMC snap-in, navigate to **Computer Configuration > Policies**.
2. Right-click **Privilege Guard Settings** and select **Advanced Agent Settings**.
3. Select **64-bit Agent Values** from the **Edit** drop-down menu.
4. Click **Add Value** and name it `HookExclusions`.
5. Select **Multi-String** in the Type column.
6. Click in the Value Data column. In the **Value Data** field, add the Bromium paths (`c:\Program Files\Bromium` and `C:\ProgramData\Bromium`)

Note: Separate the paths with a carriage return, not a comma or semicolon.

Device Lock

Device Lock is a DLP product that has been known to have issues with various security products, specifically, initialization failures. To avoid this, whitelist the following Bromium processes in Device Lock:

`BrConsole.exe`

`BrDesktopConsole.exe`

`BrDownloadManager.exe`

`BrExeScanner.exe`

`BrHostDrvSup.exe`

`BrHostSvr.exe`

`BrInstaller.exe`

`BrInstallerPopup.exe`

`BrLauncher.exe`

`BrLogMgr.exe`

`BrManage.exe`

`BrNav.exe`

`BrPreCheck.exe`

`BrProgressDialog.exe`

`BrRemoteManagement.exe`

```
BrRemoteMgmtSvc.exe
BrReporter.exe
BrSecurityAlertInspector.exe
BrService.exe
BrStatusMonitor.exe
BrWinFile.exe
chrome.exe
dpinst.exe
getcaps.exe
HostPcapDump.exe
Br-hostconfig.exe
Br-init-a.exe
Br-init-c.exe
Br-init-l.exe
Br-init-m.exe
Br-init-n.exe
Br-init-o.exe
Br-init-w.exe
Br-uxendm.exe
uxenctl.exe
uxenctx.exe
uxendm.exe
```

For more information, contact DLP Support.

AppSense

AppSense Application Manager and AppSense Performance Manager operate on a low-level file basis that sometimes brings them into conflict with some reactive antivirus products. In certain situations this can cause a deadlock to occur, resulting in process requests that cannot be completed. You may need to configure some exclusions, both within the AV and within Application Manager/Performance Manager, dependent on the choice of AV that is in use.

Symantec Endpoint Protection

Add the following exclusions to Performance Manager for Symantec, under **Global Resources > Memory Optimizer > Excluded Components**:

```
%ProgramFiles(x86)%\Symantec\*
%ProgramFiles%\Symantec\*
```

In addition, add the following paths to Symantec's exclusion list for Performance Manager:

```
%ProgramFiles(x86)%\AppSense\Performance Manager\*
%ProgramFiles%\AppSense\Performance Manager\*
```

as well as the Bromium directory exclusions listed in Directories Exclusions.

McAfee

The following files need to be added to the McAfee exclusion list:

`amagent.exe`

`amminifilter.sys`

`amfilterdriver.sys`

`pmagent.exe`

`pmoptimizer.sys`

`pmusermem.sys`

as well as the Bromium file exclusions.

Additionally, all relevant McAfee processes and drivers should be added to the following area of the Performance Manager console: **Resources Setup > Options > Excluded Application > Share Factor Exclusions**. Ensure you are using McAfee VirusScan Enterprise 8.7; update to Patch Level 5 or higher to avoid a potential conflict with AppSense agents.

Trend Micro

To avoid issues with Trend Micro, exclude the following processes from scanning by Trend:

`amagent.exe`

`AmAgentAssist.exe`

and add the following value to the Registry key:

`HKLM\SOFTWARE\AppSense Technologies\Application Manager\DriverParameters`

Value: `ExProcessNames`

Type: `REG_SZ`

Data: `TMBMSRV.exe` (and the files listed in File Exclusions.)

Note: This key contains the names of any processes you want to exclude from Application Manager. You can add other processes, as long as they are in a space-delimited format. If you are using Application Manager as a primary anti-malware mechanism, it is recommended that you configure an AppSense Environment Manager Self-Healing Action for this key to protect it.

Sophos

Sophos requires the following processes to be added to the `HKLM\SOFTWARE\AppSense Technologies\Application Manager\DriverParameters` registry key:

`SavMain.exe`

`SavProgress.exe`

`SavService.exe`

`ALMon.exe`

`ALsvc.exe`

`ALUpdate.exe`

`RouterNT.exe`

`sav32cli.exe`

`wscclient.exe`

Kaspersky Antivirus

Add all of the AppSense agents and notify processes to the exclusion list in the Kaspersky software and add `%ProgramFiles%\AppSense` and the Bromium directory to the exclusion list. Add the agents to the trusted applications list.

Using EM Policy, create a computer startup registry action to exclude the Kaspersky processes from AM:

`HKLM\SOFTWARE\AppSense Technologies\Application Manager\DriverParameters`

Value: `ExProcessNames`

Type: `REG_SZ`

Data: `avp.exe klnagent.exe` (and the files listed in File Exclusions.)

Bit9

Whitelist the following directories:

%userprofile%\AppData\LocalLow\Bromium

%userprofile%\AppData\Local\Bromium

%programfiles%\Bromium

%programdata%\Bromium