Bromium®

Bromium Secure Platform

4.1 Update 8 GA

Installation and Deployment Guide

Notices

Bromium Secure Platform 4.1 Update 8 GA

11/08/2019

Bromium Secure Platform Installation and Deployment Guide

This guide describes how to install the Bromium Secure Platform and deploy Bromium products to endpoints.

Using This Guide

To install and deploy the Bromium Secure Platform, read the topics as follows:

1. Predeployment Planning and Deployment Guidelines and Recommendations to check hardware and software requirements and guidelines to set up a Bromium deployment.
2. For first time installations, read Installing Bromium Products Manually or Installing Bromium Products Remotely.
3. If you are upgrading from previous versions of the Bromium Secure Platform, read Upgrading, Repairing, and Uninstalling Bromium Products.
4. Install the Secure Browsing extension as outlined in Installing the Secure Browsing Extension.
5. Refer to Installing and Configuring the Bromium Controller to install the Bromium Controller.
6. Follow the information in Desktop Console Overview to configure or change settings in the Desktop Console.
7. Secure your endpoints using the Enabling Protection On Endpoints topics.

You can also refer to the one page Quick Start to get started with Bromium using recommended settings.

Additional Product Documentation

The Bromium Secure Platform documentation also includes:

- *Bromium Secure Platform Release Notes*

  A brief overview about what's new in each release, software and hardware requirements, and fixed issues.

- *Bromium Controller Online Help*

  A step-by-step guide to all functionality you can perform in the controller, including a summary report and dashboards to view your deployment at a glance, threat triage, device management, policy configuration, event logging, and other settings.

  The online help is launched from the Help icon  in the controller, or it can be viewed from the documentation portal on the Bromium Support site.

- *Bromium Secure Platform User Guide*

  Assistance for end users to provide information about Bromium protection, how to open isolated files and websites, and how to get help.

To view and download all product documentation, visit the Bromium documentation portal at: https://support.bromium.com/s/documentation.

Feedback

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

Contents

1 Deployment Guidelines and Recommendations

Defining Objectives

For a successful deployment, it is strongly recommended that you clearly define the specific business use cases and threat challenges you would like to solve with Bromium Secure Platform. Then, a deployment strategy and policy configuration can be defined.

The following are examples of some of the specific use cases that the Bromium Secure Platform can be used to solve:

- Protect against malicious email attachments sent through Outlook or Webmail containing ransomware
- Protect against spear phishing attacks that target browser or browser plug-in exploits
- Securely allow HR users to open PDF and Word documents downloaded from a job portal
- Reconfigure the proxy rules to allow Bromium protected browsing sessions to securely access uncategorized and previously blocked websites

When business objectives and goals are defined, the Bromium Secure Platform can be configured optimally to meet these objectives.

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.

Deploying Bromium in Phases

Due to the many capabilities of Bromium Secure Platform, it is not typically deployed in a “one size fits all” configuration. Based on the various needs of different business units and the defined business objectives, it is common to have different policies for specific user groups. Additionally, Bromium capabilities can be deployed in phases. As with any security product, Bromium does not recommend enabling all protection capabilities during initial rollout; it is recommended that you first define the minimum protection capabilities required to meet the initial business objectives and deploy that configuration first.

Once an initial configuration has been successfully and fully deployed, additional protection capabilities can then be evaluated and enabled in later phases.

For example:

- Phase 1 – spear phishing and email attachment protection
  - Internet Explorer isolation
  - Firefox and Chrome download and file protection
  - File protection for executables and scripts, Word documents, PDF documents, ZIP archives

- Phase 2 – full browser and file protection
  - All protections from phase 1 and the following:
    - Chrome and Firefox isolation
    - USB protection
    - File protection for Excel & PowerPoint files, images, and videos

In addition to enabling Bromium protection capabilities in well-defined phases that map to business objectives, it is often necessary to have different policies for different business units or groups. For example, the protection policy for IT users or developers could differ from the protection policy for HR users, which will often differ from the protection policy assigned to kiosk or conference room devices.

Pilot Testing

Pilot testing is one of the most important elements of a successful deployment; therefore, proper selection of pilot users is paramount. Bromium recommends selecting typical, non-IT business users across all of the necessary business units and functions. VIPs and IT users may not be suitable for a pilot because they often perform unique workflows or use technologies that are more challenging to integrate with isolation, such as:

- Have local administrator rights
- Install and test beta software
- Change their locally installed software
- Use custom file system tools
- Install and run development environments
- Install and test many different web plug-ins
- Run custom scripts that interact with browsers and files
- Use many different USB drives for software installation and file transfer

A typical non-IT business user does not have local administrator rights and only uses a specific list of IT-approved applications and web plug-ins. Since the list of applications and configuration changes on business users' desktops is more static, there tends to be fewer conflicts deploying and managing software that controls web browsing and untrusted file access for business users. The varied and dynamic desktop configuration for an IT user is more difficult to define and support. This does not mean that Bromium should not be deployed to IT users, more time is required and it is common to encounter issues for IT users that do not occur for business users. It is recommended to select some IT users for the initial pilot; however, most pilot users should be business users.

Bromium recommends that an ongoing pilot or test group should always be in place. This could be the existing groups used for the initial pilots or a new group. The purpose of this group is to ensure that major changes and upgrades can continually be tested in a rapid and controlled environment before they are pushed out to the entire enterprise.

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.

Maintenance Tasks

Maintenance tasks ensure that a stable, well performing environment is sustained. The following maintenance tasks should be performed on a recurring basis:

- Database backup and grooming
- Policy and group maintenance
- Registered device maintenance
- Evaluation of new product features

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 Monitoring and Windows 10 Fall Creators Update

Support for Windows 10 Fall Creators Update was introduced in Bromium Secure Platform 4.0 Update 3 and will not work on earlier versions of Bromium. To upgrade to Windows 10 Fall Creators Update, you must upgrade to Bromium Secure Platform 4.0 Update 3 or later before updating Windows.

If you have already upgraded to Windows 10 Fall Creators Update, see https://support.bromium.com/s/article/Planned-Support-for-Microsoft-Windows-Fall-Creators-Edition for information about resolving this issue.

Running the Installer

This topic describes how to manually install the Bromium Secure Platform using the installation .msi. It is recommended that you read the Predeployment Planning topics to ensure your system meets the minimum requirements before proceeding.

Note: Do not install Bromium software on a USB drive. USB drives are untrusted by default and, when Bromium reaches the initialization stage, the installer will fail and will be unable to read the installer data on the USB drive.

To install Bromium manually on a single local system:

1. 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\vSentry`

   Note: Ensure that permissions on the installation location and directories (including the root of the drive) are limited to user accounts with local administrator or SYSTEM permissions.
7. Enter the URL of the server on which you will run the controller. If you do not know the URL, enter some placeholder text to continue. To add the URL after installation, use the `BrManage BMS.ServerUrl` command. For more information about using this command, see Configuring Isolation Clients to Report to the Controller.
8. Click **Next**.

9. Click **Next** to begin platform installation.

   Bromium Secure Platform is installed.

10. 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. For information about error messages, go to the Bromium Support site.

    Note: If you are running Windows 10 Fall Creators Update, an additional UAC dialog may be displayed during this step. If you are installing Bromium from an administrator command prompt or running the installer using an SCCM that does not require UAC prompts, this dialog will not be displayed.

11. Click **Finish**.

Next, enable browser protection for Chrome. Download and distribute the Bromium Secure Browser extension to your endpoints using the procedure in Running the Installer.

Installing the Secure Browsing Extension

The Bromium Secure Browsing extension provides protection for web browsing when Chrome is set as the default on endpoints. With this extension, when users click links to untrusted sites (for example, in an Outlook email), the site will open in an isolated Chrome tab running in a micro-VM. This extension can be downloaded then distributed across enterprises using Group Policies or PR Master, or users can download it directly from the Chrome store.

To download and enable the Secure Browsing extension:

1. Go to: https://chrome.google.com/webstore/detail/secure-browsing/fcbnoohifpjfjohaciofjaefgpdjmhcf
2. Ensure that **Allow access to file URLs** is enabled.

For information about distributing extensions, see the Chrome documentation at https://support.google.com/chrome/a/answer/188453?hl=en

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.)
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. 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.)

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 Bromium Isolation 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 "BrRmService"
```

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

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

If you are using Persona Management, create a scheduled task that starts on Windows. Open elevated command prompt and run the following command:

```
schtasks.exe /create /tn "Reset BMS.ClientToken" /tr "c:\windows\System32\reg.exe delete
HKLM\Software\Bromium\vSentry\state /v BMS.ClientToken /f" /sc ONSTART /ru SYSTEM
```

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 software version.) 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.

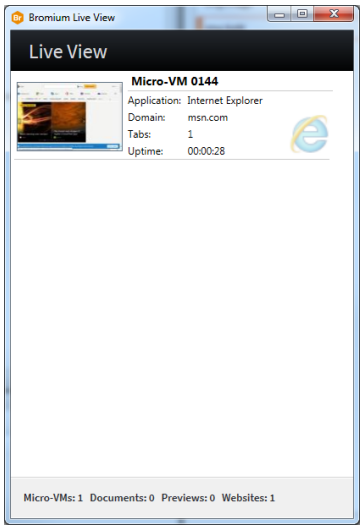
Verifying the Deployment

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:

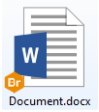


5. Navigate to one of the intranet sites that you configured during installation.

   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 intranet site was configured properly.

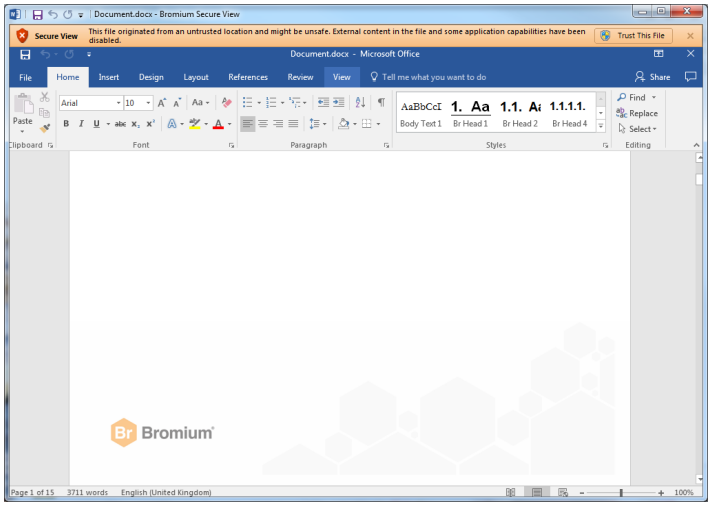
6. Download a Word document from the Internet and save it to the desktop.
7. Navigate to the folder that contains the document.

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

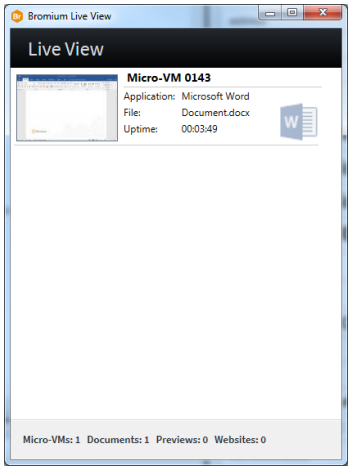


8. Double-click the document to open it.

   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 using `cd %BRS%`.

   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, the problem can be diagnosed using an installer log file. You can generate this file using the msiexec `/l` command line argument. For example: `msiexec /i bromium_secure_platform.msi /l*v install.log`. This creates a verbose installer log file called `install.log` in the current directory and makes a copy in the `c:\ProgramData\Bromium` folder which contains the date and time in the file name. For more information about using msiexec, see msiexec Command-line Switches and Parameters.

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.

For more information about other error messages displayed when installation fails, see the Bromium Support site.

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
    - `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 POLICIESXML=\\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 products
/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	Uninstall Bromium products

Parameter	Description
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	For monitoring, set this to `1` 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=1` Set this to `0` 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=0`

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

Parameter	Description
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=`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

Upgrades can be performed in the same manner as installation, using existing enterprise software deployment platform such as SCCM. Additionally, once Bromium has been installed on an endpoint and is connected to the controller, the controller can be used to deploy upgrades to endpoints. This capability can be useful for upgrading specific endpoints used to pilot new releases.

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 machine. The new version will be used after the desktop is rebooted.

To upgrade Bromium products remotely from the controller:

1. In the controller interface, navigate to the Devices page and check the box next to the devices on which you want to run the upgrade, or select the top checkbox to select all devices.

2. Select **Install Package** from the **Remote Management** drop-down list.
3. Enter the location (URL or path) of the MSI file.
4. Click **Send Command**.

   A confirmation message is displayed. An endpoint runs its queued remote commands the next time it checks for updates from the management server. A command remains queued until it is run on the device. You can cancel commands if they are still queued.

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. 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 or Windows 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. To configure these settings, see Changing Controller Configuration for details.

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

  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 > Bromium 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 the Controller Secret Key.
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>`

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.

Older events are removed from `history.log` when it exceeds 5MB. Backups of previous logs can be configured using the audit_log_backup_count setting in the in `settings.json file`. This is set to 5 by default.

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 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 this option is selected 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. You can use the asterisk (*) wildcard anywhere in the domain, for example `*//*.abc.*.domain.com`.
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 **Remove sensitive data from logs** policy setting can be used to exclude proxies, URLs, and so on from log data.

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.

7 Enabling Protection On Endpoints

With Bromium protection enabled, malicious files and websites open in a micro-VM - any malware that might be present is isolated from the host and cannot execute. When the micro-VM is closed, the malware is discarded along with it. This protection and threat monitoring is set on devices using *policies*: a group of settings that are enabled and fine tuned in the Bromium Controller.

Bromium polices contain preconfigured settings that can be applied to multiple (or all) devices. The four read-only policies are provided with the Bromium Secure Platform, and are indicated by a  next to the policy name in the controller interface. These policies allow you to quickly enable endpoint protection that is relevant to your environment and users, without having to configure settings individually.

- **Recommended Protection Settings**: use this policy as a base policy on all of your endpoints in conjunction with the other three Bromium policies.
- **Attachment Protection**: email attachments in Outlook and webmail are isolated in a micro-VM. These attachments include executable files, Microsoft Office documents, and (if Adobe Reader or Adobe Acrobat are installed) PDFs. For a complete list of supported file types and prerequisites, see "Supported Software" in the Bromium Platform Requirements topic.
- **Link Protection:** links contained in emails messages and attachments, shared links in supported chat clients (Skype, Skype for Business, HipChat, and Slack), and any other opened links are opened in an isolated browser tab.
- **Download Protection**: files downloaded and/or opened from websites are opened in a micro-VM. This includes files accessed through malicious web sites and URL redirects.

To enable the Bromium polices on your endpoints:

1. Navigate to the Bromium Controller site.
2. Add the four preconfigured polices to your devices. In the Device Groups page, select a device group. If you have not grouped your devices, you can select **(Ungrouped)** in the table.
3. Click **Add Policy**. From the drop-down list, select a Bromium policy to apply to the device group. The Bromium policies are indicated by a  next to the policy name in the list.
4. Click **Add Policy** again and add the next three Bromium policies to the group.

   Polices are set to **On** by default.
5. Click **Save Group** to save your changes and return to the Device Groups page.

   The devices will connect to the controller to receive the new policies.

To customize these settings (for example, to add sites to the trusted websites list), create *delta policies*. Delta policies inherit settings from existing policies on your endpoints and specify settings that differ. This allows you to customize features for specific endpoints or groups of endpoints.

For more information about using the controller interface to configure policies, refer to the Bromium Controller Online Help.

8 Using Monitoring

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 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, for example on endpoints or servers that do not meet the technical requirements of Isolation (such as VT support). In order to stop machines running quarantine only causing isolation errors on the Controller, you can set the advanced setting of `vSentry.QuarantineOnly` to a value of `1` to the a delta policy targeted at just those quarantine only machines. If you set this on a general policy, it will disable isolation on all machines and this may be undesirable.

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 can 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 add custom rules to monitor for extra behaviors that you consider to be malicious. Custom monitoring rules can also be used to exclude applications from monitoring to help avoid high volumes of alerts and false positive events. Using rule layering, custom rules are applied on top of the base rules.

Custom rules should have both an application(s) specified and a corresponding trigger event(s). Configuring both an application and trigger event ensures that the intended behavior occurs. If a trigger event is not specified, it can cause unintended effects. For example, an application will be monitored but will have no triggering events if they are not present in the base rules. As a result, unexpected alert behavior may occur.

You can use wild card logic for the trigger conditions. For instance, a wild card can be used to specify the path for a process launch: for application `ABC`, this would be entered as `*\ABC.exe`. Wild cards can also be used for registry and file triggers.

For steps to create custom rules in the Bromium Controller, see the Creating Monitoring Rules topic in the online help at: https://documentation.bromium.com.

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.

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.

Custom Rule Limitations

Custom rules have the following limitations:

- Custom rules cannot suppress monitoring of all unsigned applications
- The monitoring policy for a base application such as Chrome cannot be copied to a new application, such as Opera. For new applications, a new custom rule needs to be created for the monitoring of the application.

A Quick Start

Use this topic as a quick reference to install the Bromium Secure Platform and enable recommended security settings on your endpoints. For complex environments that require customized protection settings, refer to the relevant policy topics in the *Bromium Controller Online Help* for more information.

To deploy Bromium using the recommended settings:

1. Install the Bromium Secure Platform. For first time installations, read Installing Bromium Products Manually or Installing Bromium Products Remotely. If you are upgrading from previous versions of the Bromium Secure Platform, read Upgrading, Repairing, and Uninstalling Bromium Products.
2. Install the Bromium Controller. For more information, see Installing and Configuring the Bromium Controller.
3. Navigate to your Bromium Controller site.
4. Enable security settings on your endpoints. On the Device Groups page, select an existing device group or create a new one. To apply policies to devices that are not in device groups, select **(Ungrouped)** in the Device Groups table.
5. For new groups, enter a name in the **Name** field.
6. In the Applied policies area, click **Add Policy**.
7. Select **Recommended Protection Settings** from the drop-down list, then click **Add Policy** again.
8. Continue adding the **Attachment Protection**, **Link Protection**, and **Download Protection** policies.
9. Click **Save Group**.

   The Bromium policies are now enabled on the selected device groups. For more information about the Bromium preconfigured policies, see Enabling Protection On Endpoints.

10. Add a delta policy. In the Policies page, click **Add Policy** and select **Create Delta Policy**. Enter a name for the new policy.
11. In the Web Browsing tab, set the **Trusted website** option to **On**. In the field, enter the domain address or CIDR notation of the website(s) that will open without isolation protection.
12. In the Manageability tab, set the **Product license keys** option to **On**. Enter the license key in the field.
13. Click **Save** to save your changes.
14. In the Device Groups page, select the required group. Click **Add Policy** and select the new delta policy from the drop-down list.
15. Click **Save Group**.

For information about using secure web browsing and working with files that are protected by Bromium, refer your end users to the *Bromium Secure Platform User Guide* at https://support.bromium.com/s/documentation. A direct link to the guide can be provided or you can print and save individual topics that are relevant to your policy settings.

B Isolation for VDI

Isolation can run “nested” in a machine running all supported versions of Windows on VMware ESX 5.5 Update 2 or later (ESX 6.0 is recommended) or Citrix Hypervisor 7.3.

Note: The Japanese language version of Windows 8.1 is not supported.

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 VMWare	VMware, ESX 5.5 Update 2 or later. ESX 6.0 is recommended
ESX VM Guest Hardware	Version 10 or later
ESX Guest CPU Configuration	Enable Hardware virtualization Enable Hardware CPU and MMU
Citrix Hypervisor	7.3 or later
CPU	Intel Xeon Processor or later with VT-x and EPT enabled in the BIOS
Guest vCPU Configuration	Two virtual CPUs minimum
Guest Memory Configuration	Minimum: 4 GB RAM Recommended: 5 GB RAM
Bromium Secure Platform Version	For ESX: version 3.2 Update 3 or later is supported; however version 4.0 and later is recommended For Citrix Hypervisor: version 4.0 Update 4 or later

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; however, this may decrease responsiveness for tasks that are running in isolation.

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 prevent automatic reinitialization since this is not required as the master image contains the initialized template

The following provisioning methods are supported:

- Citrix Virtual Desktops:
  - 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

It is recommended that isolation is preinstalled as part of a master image; however, 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) and access to the display(s) for target users. This ensures that a template is created with the correct settings for your typical users.

2. If required, you can tell isolation what screen resolution to target by setting `XVM.TemplateScreenWidth` and `XVM.TemplateScreenHeight` to the required resolution. If there is more than one resolution, use the maximum value.
3. If you are running Bromium Secure Platform version 4.0 Update 3 or later, set `LCM.TemplateRespectUserMaxResolution` to `0`.
4. Log in to the account created in step 1 to create the master template.
5. Stop the Bromium Isolation Remote Management Service. If applicable, also stop the Bromium Endpoint Monitoring Agent Service for monitoring.
6. Close the BrConsole.exe process.
7. Delete the following registry value: `HKEY_LOCAL_MACHINE\SOFTWARE\Bromium\vSentry\State\BMS.ClientToken` If it exists for monitoring, also delete the value `HKLM\SOFTWARE\Bromium\BEM\Agent\v1\state\Token`
8. 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 "BrRmService"

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

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

For example, for monitoring:

```
net stop "Bromium Endpoint Monitoring Agent Service"

reg delete "HKLM\SOFTWARE\Bromium\BEM\Agent\v1\State" /v "Token" /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
- `VMWVvphelper.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`.

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.

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
```

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

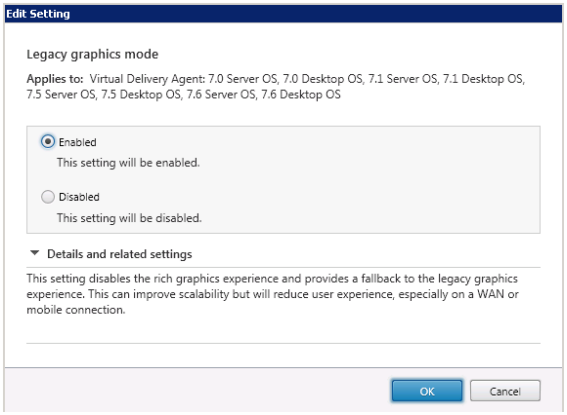
Citrix ICA/HDX Protocol Policy

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 Citrix Virtual Desktops 7.0 and later as follows:

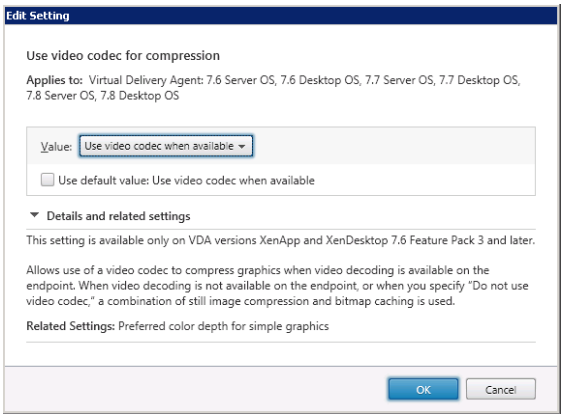


Windows 8.1 or 10 VDI

If you are running Windows 8.1 or Windows 10 VDI sessions hosted on Citrix Citrix Virtual Desktops, it is recommended to use Virtual Desktops 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 Virtual Desktops 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.

C 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:

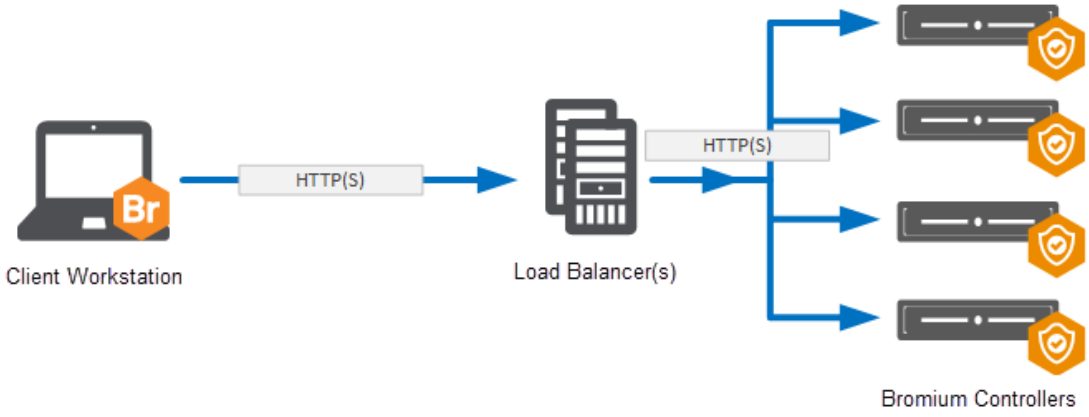
- Two or more machines to run controller instances
- Load balancing software (installed on its own machine) or physical load balancer or round-robin DNS for routing work to machines in the cluster
- Configuration of controller machines to communicate with the load balancer

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.

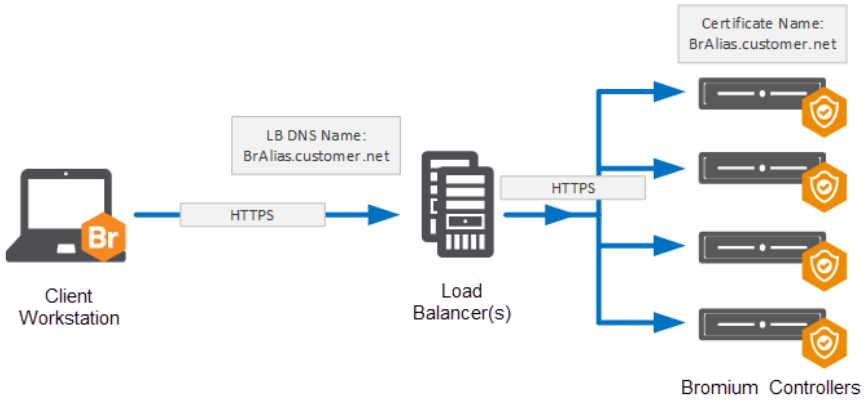
  The main benefits of this configuration is that it allows for end to end encryption while reducing the load on the controller servers versus the SSL offload method. This reduced load occurs because the hardware load balancer is able to aggregate multiple SSL sessions to the controller servers which reduces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

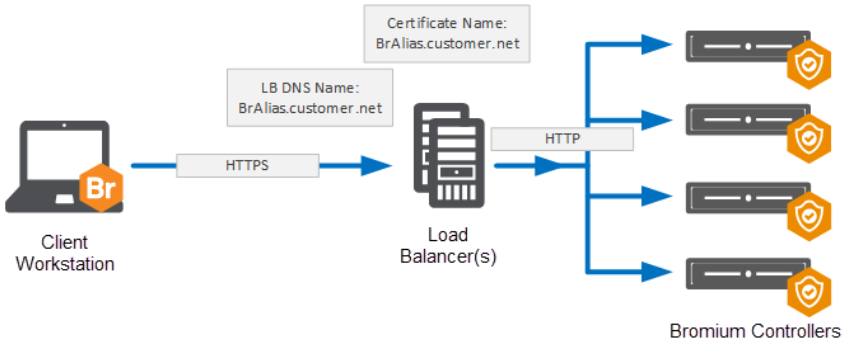
SSL Bridge

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.



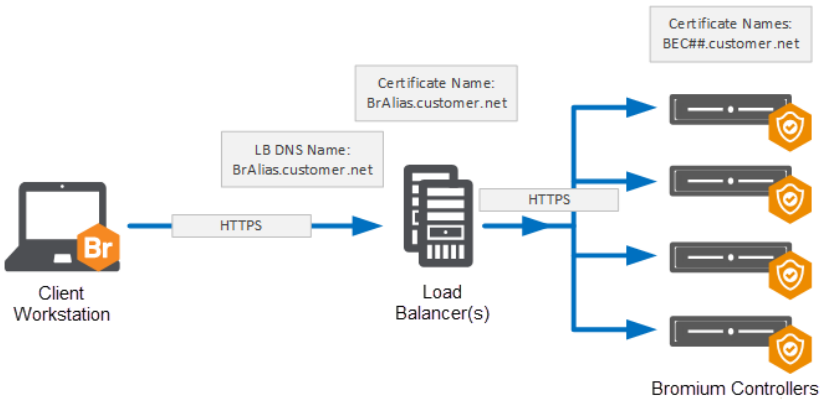
SSL Offload

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.



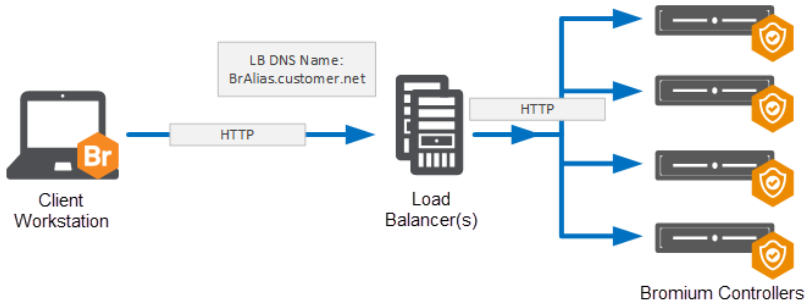
SSL to SSL

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.

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