Google Chrome

Business & Education

Chrome Browser
Deployment Guide

Set up and deploy Chrome browser in your organization

Table of Contents

About this guide

Introduction

Configure Chrome Options
- Best Practices Summary
- Legacy Browser Support
- Policies and Templates
- Cloud Policies
- Master Preferences
- Privacy

Chrome Deployment
- Methodology
- Prepare your installation package
- Installation Process
- Summary: Best Practices for Installation and Updates
- Configuration Options

Installation Procedure for Chrome
- Create a Distribution Point
- Configure Chrome Policies
- Change the configuration settings for the target group of users
- Install Extensions Automatically (optional)
- Assign GPO to a set of users
- Assign a Package
- Make Chrome the Default Browser (optional)
- Manage Google Updates (optional)
- Test your installation

Example Customer Configurations
- Healthcare organization in a regulated environment
- Public organization with 15,000 users
- Global enterprise of more than 35,000 users
- Global enterprise of more than 25,000 users
- Commercial organization with 1,000 users

Additional Resources

About this guide

This guide focuses on the two critical steps required for a successful Chrome deployment:

- **Configuration**: The considerations and decisions to building an installation package to deliver to each user
- **Deployment**: The timing and testing requirements for an installation package to deploy Chrome

This guide focuses on the Windows Installer (MSI) version of Chrome browser for business, which is available for Microsoft Windows 7 and later. It's possible to install a managed version of Chrome for Linux-based systems and to configure device-based policies on a Mac, but these configurations will not be covered in this guide.

This guide covers cloud-based policies and Legacy Browser Support, but for more in-depth documentation on these, please refer to the Chrome for business and education Help Center.

For detailed information on how to set Chrome as the default browser on domain-joined computers running Microsoft® Windows 10® and above, please refer to Make Chrome default browser on Windows 10.

The recommendations in this guide on deploying Chrome in an enterprise setting were gathered through our work with a variety of clients and environments in the field. We thank our customers and partners for sharing their experiences and insights.

What's covered	Instructions, recommendations, and critical considerations for deploying Chrome in an enterprise environment
Primary audience	Microsoft Windows administrators
IT environment	Microsoft Windows 7 and above
Deployment phases	Core IT, Early Adopter
Takeaways	Best practices checklist for the critical considerations and decisions of a Chrome deployment

Last updated: *December 19, 2017.*

Third-party products: This document describes how Google products work with the Microsoft Windows operating systems and the configurations that Google recommends. Google does not provide technical support for configuring third-party products. GOOGLE ACCEPTS NO RESPONSIBILITY FOR THIRD-PARTY PRODUCTS. Please consult the product's Web site for the latest configuration and support information. You may also contact Google Solutions Providers for consulting services.

©2017 Google LLC All rights reserved. Google and the Google logo are registered trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated. [CHROME-en-1.0]

Introduction

Chrome for business allows you to deploy and manage the Chrome browser for your organization. It consists of the Chrome browser and a set of admin tools, resources, and installer packages which allow an IT administrator to deploy and manage Chrome in an Enterprise environment. The admin tools allow administrators to configure, package, and deploy Chrome browser at the system level, and manage policies on an ongoing basis.

The Chrome browser offers the user many configuration options and settings to personalize and enhance their web browsing experience. When deploying Chrome, the administrator can control Chrome browser default settings and policies using the following methods:

- **Policies**: Can be used to enforce and maintain settings on client PCs. For example, you can enable auto-updates, and set the update interval, the default search engine, and the default browser.
- **Preferences**: Can be used to set the default value for particular setting, while still allowing the user flexibility to change the setting. For example, you can set the user's default homepage to the company intranet, set the home button to display in their toolbar, or allow the bookmarks bar to display in the toolbar.

For more detail on the differences between policies and preferences including additional examples, see Default user preferences in the help center.

Configure Chrome Options

Best Practices Summary

- Use Windows Group Policies (GPO policies) and cloud policy over preferences when possible. Unlike policies, preferences do not apply to previous installations of Chrome and are only applied to a single profile. Policies also override any preferences settings for a feature. Also note that the master_preference file can be changed and not enforced like group policies can.

  Remember that GPO is a machine policy. For example, GPO applies to any user that uses the computer, whereas cloud policy is tied to the user, and it only applies if the user is signed in to Chrome on their computer.

- We strongly recommend enabling Chrome auto-updates (this is the default policy setting) to ensure that users have the latest features and security fixes.

Legacy Browser Support

If your organization wants to take advantage of the Chrome browser, but your users still need to access legacy websites and web apps that require Microsoft Internet Explorer, you can use this feature to easily switch between browsers. The Chrome Legacy Browser Support extension allows administrator-designated websites to automatically launch in either Chrome and another browser. When your user clicks a link in Chrome that requires a legacy browser to open (such as a website with an embedded ActiveX control), the URL will automatically open in the legacy browser.

Administrators can specify which URLs to launch into a legacy browser and deploy this Chrome policy for the organization. Legacy Browser Support (LBS) requires Chrome 26 or higher. Learn more about LBS and how to set it up in the help center.

A companion Internet Explorer add-in for Legacy Browser Support enforces the administrator-defined policy that only whitelisted websites will open in MSIE while others launch in Chrome. Thus, a user attempting to go to Gmail in MSIE will see Gmail launch in Chrome instead of MSIE for an optimal experience.

Policies and Templates

The administration and configuration of Chrome policies differ depending on the target operating system. Chrome policies are applied differently depending on the client operating system. Across all desktop operating systems, cloud policies can apply to signed-in Chrome users.

- **Windows**—Group Policy using ADM or ADMX configuration templates. ADMX supercedes ADM files for Windows Vista and later. Consult your Windows support provider to find out which option is best for you.
  Note: There are separate templates for Chrome, Google Update, and LBS which all may need to be used to manage a Chrome deployment. The specific template being discussed in this guide will be called out as we discuss each one.
- **MacOS X**—Property list / .plist configuration file. Use your favorite systems management tool to push this file to client Macs.
- **Linux**—JavaScript Object Notation (JSON) configuration file. Use your favorite systems management tool to push this file to client PCs.

After selecting the right template for the target environment, the administrator needs to define which Chrome policies will be enforced in the enterprise environment. The Chromium.org site lists the supported policies for Chrome and can be applied via policy templates available in the the help center.

Cloud Policies

In addition to machine-based policies, you can optionally provide users with the convenience of having their open tabs, bookmarks, and theme synced with any PC where Chrome is installed.

Additionally, administrators can define pre-installation of Chrome apps, extensions, and themes when users sign in to Chrome.

These cloud policies are defined by administrators in the Google Admin console and are inclusive of the majority of policies that are available via the Chrome policy template deployed by GPO. These policies apply to users on any PC where the user signs in to Chrome with their Google account.

If you're a G Suite customer or have Chrome licenses, you can use cloud policies to manage Chrome for your users.

Administrators with access to the Admin console can synchronize users and their passwords with their LDAP server to manage user policy. More information can be found below:

- Google Cloud Directory Sync (GCDS)–Automatically add, modify, and delete users, groups, and non employee contacts to synchronize the data in your G Suite domain with your LDAP server.
- G Suite Password Sync (GSPS)–Automatically keep your user's Google account password in sync with their Microsoft Active Directory passwords.

These policies will be deployed and updated anytime the client has Internet connectivity. Unlike the typical

GPO policy push scenario which requires the PC to have LAN or VPN connectivity to the Active Directory controller, cloud policies can be pushed when the client PC has a connection to the public Internet. For instructions on how to set up cloud policies, see Set up user-based policies.

Note: Machine policies (GPO) take precedence over cloud policies when there's a conflict. For details, see Set Chrome policies for devices.

Master Preferences

The method to implement and associate a `master_preferences` file with the Chrome MSI is documented in the help center.

When users launch Chrome for the first time, the user's preference file is copied from the `master_preferences` file. We recommend you validate the `master_preferences` file with a JSON validator and formatter prior to deploying. After the `master_preferences` file has been verified, package it with the Chrome installation for deployment.

Privacy

The Google Chrome Privacy Policy describes how we treat personal information when you use Chrome browser and associated services such as Safe Browsing. You can review the latest version here, which outlines the data collected based on the feature being used.

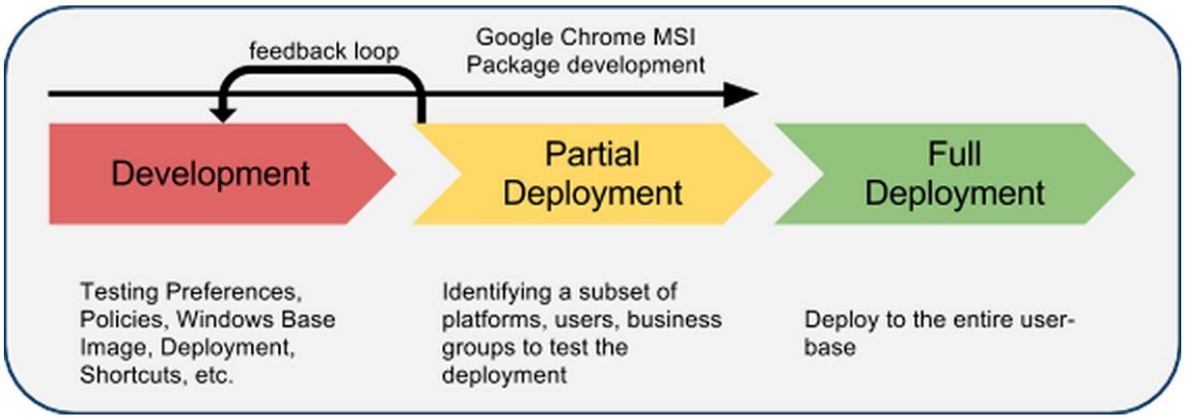
Note that in many cases, specific features can be disabled by the user or via policy to minimize the information sent to Google. These include but are not limited to:

- Chrome Sync with SyncDisabled
- Omnibox search suggestions with SearchSuggestEnabled
- Translate feature with TranslateEnabled
- Spellcheck feature with SpellCheckServiceEnabled
- Autofill feature with AutoFillEnabled
- Anonymous usage statistics and crash reports to Google with MetricsReportingEnabled

Chrome Deployment

Methodology

Enterprise software deployments require a phased roll-out to capture and resolve any issues before deploying the software company-wide. We recommend you deploy Chrome in a structured approach with the following phases: Development, Partial Deployment, and Full Deployment. This multi-step approach allows you to evaluate the deployment at each stage and make necessary changes. Below are some of the tasks that should be performed in each Chrome deployment phase:



Prepare your installation package

Chrome uses a standard MSI installer package and can be deployed via standard Windows deployment tools. Software deployment tools can bundle the MSI, preferences, bookmarks, and extensions. Some of the most common distribution methods are:

- Active Directory Group Policy Management
- HP Client Automation
- Microsoft System Center Configuration Manager

Use software delivery mechanisms to package, deliver, and maintain distributions of Chrome.

Installation Process

Chrome installations from an MSI package are installed at the system level and are available to all users. As a result, any user-level installation of Chrome, (i.e. a user's own Chrome installation), will be overridden. Here's where Chrome is installed and linked for the two types of Chrome installers:

- **User Level**: "%USER DATA%\Google\Chrome\Application\"
- **System Level**: "Program Files\Google\Chrome\Application\"

Note: Chrome will not allow an older version to be installed over a newer version. Any MSI of Chrome needs to be newer than the version already deployed (for example, Chrome 62 cannot overwrite Chrome 63). Information on how to deploy Chrome is documented on the Chromium site.

Test Your Installation Process

Some users may have downloaded and installed Chrome prior to your enterprise installation, and there will be a previous "user level" installation, as discussed above. In this case, Chrome will install for all users and leave the user data (preferences, cache, etc.) untouched, unless you choose to have your distribution software uninstall any previous installations. It will also attempt to repoint all of the default shortcuts to point to the new system level installation.

Important: Test your Chrome installation process to make sure it works correctly on your organization's Windows image and method of software distribution.

Application Globally Unique Identifiers (GUID)

When the Chrome browser is installed, it is entered into the Windows Registry with a GUID. There will also be a parent GUID for the Chrome binaries. Any Registry changes you wish to make should be made to the parent GUID, especially as it relates to automatic updating.

In Windows you can find these in the registry in these locations:

- Chrome Binaries

  ```
  {HKLM|HKCU}\Software\Google\Update\ClientState\{4DC8B4CA-1BDA-483E-B5FA-D3C12E15B62D}
  ```

- Chrome

  ```
  {HKLM|HKCU}\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
  ```

Important: The Chrome Binaries GUID will become the default for all installations. However, previous settings for an individual GUID will be maintained.

Summary: Best Practices for Installation and Updates

Chrome Options

- Leave auto-update enabled for Chrome browser.
    - Auto Update will provide the latest security updates.

Methodology

- Use a phased approach to test and deploy Chrome.
    - To ensure that there is no regression or loss of functionality for your users, have your IT group test the beta and dev channel of Chrome.
        - The beta channel gives a 4-6 week feature complete preview of the next stable chrome release.
        - The dev channel gives a 9-12 weeks preview of what's coming next - Keep in mind that the dev release may not be 100% stable.

Installation

- Customize the branding of the application with its shortcut text and icon through your software distribution mechanism.

Logging

- Increase logging for Windows installation to troubleshoot problems.
- Increase logging of your distribution software to log successful and failed installations.
- Use the logs created by the Chrome installation to troubleshoot errors.

Chrome Updates and Bandwidth

- Account for the increased network traffic for automatic updates to Chrome.
- Stagger your client installations so they don't all update at once.
- Delta updates between releases are typically only a few megabytes as opposed to a full update which is ~20 MB.
- There is currently no built-in facility for rate-limiting auto-updates or forcing them across several days. Multiple group policy objects (GPOs) can be set for segregated organization units to customize the `AutoUpdateCheckPeriodMinutes` parameter to a different value for each OU to ensure scattering of auto-update checks.

Configuration Options

You can make Microsoft Windows-related changes to your deployment through the software management system you have chosen.

A common option might be changing the icon image, text, and placement of a Chrome icon on the desktop. These options and others are done through your software management as they don't specifically apply to the configuration of Chrome itself.

Logging

There are two key points where logging data can be beneficial in any troubleshooting process. Each point is dependent on the amount of information you would like regarding the distribution and subsequent updates of Chrome.

Software Distribution

The software distribution packages mentioned above all have varying levels of logging capabilities. Depending on your need for this information, it is important to configure it to a point where you can confirm the success or failure of the installation, and any status codes or errors returned by the MSI.

Chrome MSI

The MSI itself can also be configured to increase its logging verbosity to provide more clarity on the success or any failure. It's important to understand why a particular installation of the MSI failed.

Separately, the logs created by the Chrome installation are defaulted to the highest verbosity level and located here:

- %TEMP%\chrome_installer.log

Important: %TEMP% should be the System temp directory and not the user-level system variable.

Chrome Updates

There are two important aspects to updating Chrome: Google Update (based on Omaha) and Network usage.

We highly recommended you allow Chrome to auto-update. For two primary reasons:

1. Access to the latest security patches and bug fixes
2. Support is only provided on the latest release of Chrome browser

For more information on auto-updates, see Managing Chrome browser updates on Windows.

Track Chrome Updates

Follow the Chrome Release blog to stay up-to-date on the latest changes to Chrome.

Google Update

Chrome uses an update engine called Google Update. While you can configure the update frequency, it's important to understand what logging options are available when troubleshooting updates to Chrome.

If you encounter issues updating Chrome, do the following:

1. Enable verbose logging in Google Updater
2. Invoke 'GoogleUpdate.exe /update'
    a. e.g., On Windows 7 it is located at "Program Files > Google > Update"
    b. Additional switches to GoogleUpdate.exe are located here
3. Recover the update log
    a. e.g., On Windows 7 it is located at "Program Data > Google > Update > Log"

There will also be a folder for each version installed here:

- C:\Program Files (x86)\Google\Chrome\Application

Google Update Policies

Note that there's a separate set of policies (and templates) for Google Update outside of Chrome. For more information on managing updates across Google products, see Install and update Google applications.

Network Bandwidth

Be mindful of network bandwidth requirements for updating Chrome. You can expect a new Chrome release every six weeks. Caching can be enabled via policy if your network infrastructure supports caching of update files.

The initial Chrome browser installation is approximately 50 MB. Subsequent updates from one version to the next are approximately 10–15 MB. Patch updates are typically 3–5 MB. Updates from a major version to a later non-consecutive major version usually require a new complete installation.

Installation Procedure for Chrome

This procedure covers the general installation of Chrome browser for business and updating group policies in a Windows environment with domain-joined computers. Screenshots and detailed setup steps are for Windows Server 2012 R2 Standard and are for illustration purposes only.

You can download the standalone Chrome MSI or the Chrome Enterprise Bundle. The bundle contains Chrome MSI, Chrome Legacy Browser Support (LBS) extension, and administrative policy templates. For more information, see Download Chrome Enterprise Bundle.

The scenario assumes two machines: (server) and (client), both on the `chromeforwork.com` Active Directory domain.

Create a Distribution Point

To publish or assign a computer program, you must create a distribution point on the publishing server:

1. Log on to the server computer as Administrator.
2. Download the latest Chrome Browser MSI package from https://enterprise.google.com/chrome/chrome-browser/
3. Create a shared network folder where you will put the Microsoft Windows Installer package (.msi file) that you want to distribute.
   Note: This share MUST be accessible by your client machine. The client machine will request the file from this location. Verify the share is working correctly.
4. Set permissions on the share to allow access to the distribution package.

Configure Chrome Policies

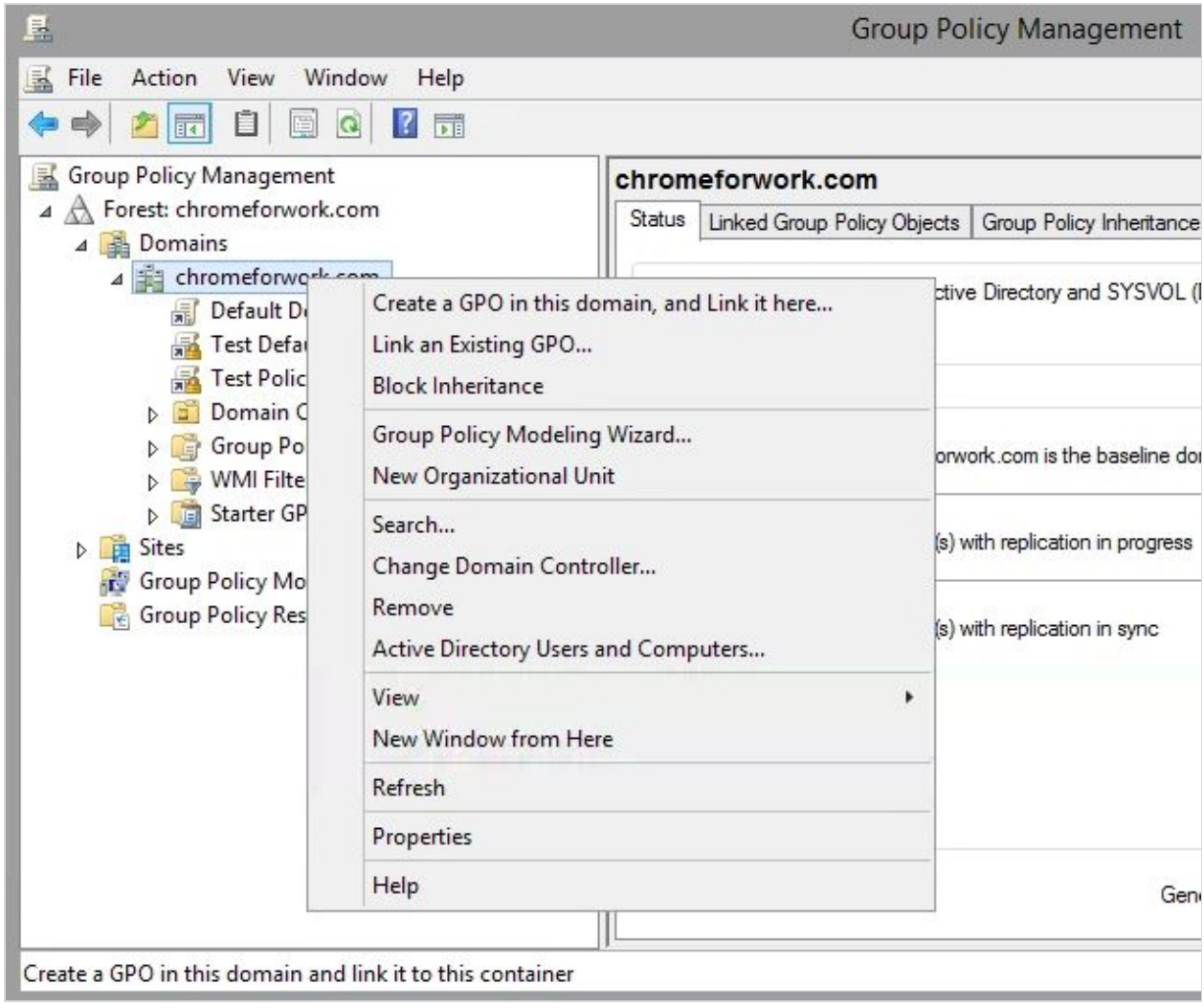
To add Chrome Browser Policies to the deployment:

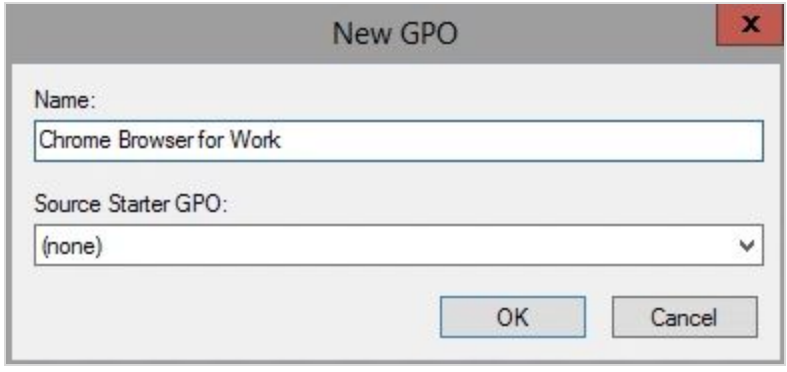
1. Download the latest ADM/ADMX policy templates for Chrome browser from https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.

   Note: The instructions below are for manually adding a GPO template (.adm file) if you are **not** using centralized GPO storage. If you **are** using centralized GPO storage, please unpack and save ADM/ADMX policy templates for Chrome browser to where your local administrative GPO templates are stored (e.g. C:\Windows\PolicyDefinitions). If you do so, you can skip step 5 below.

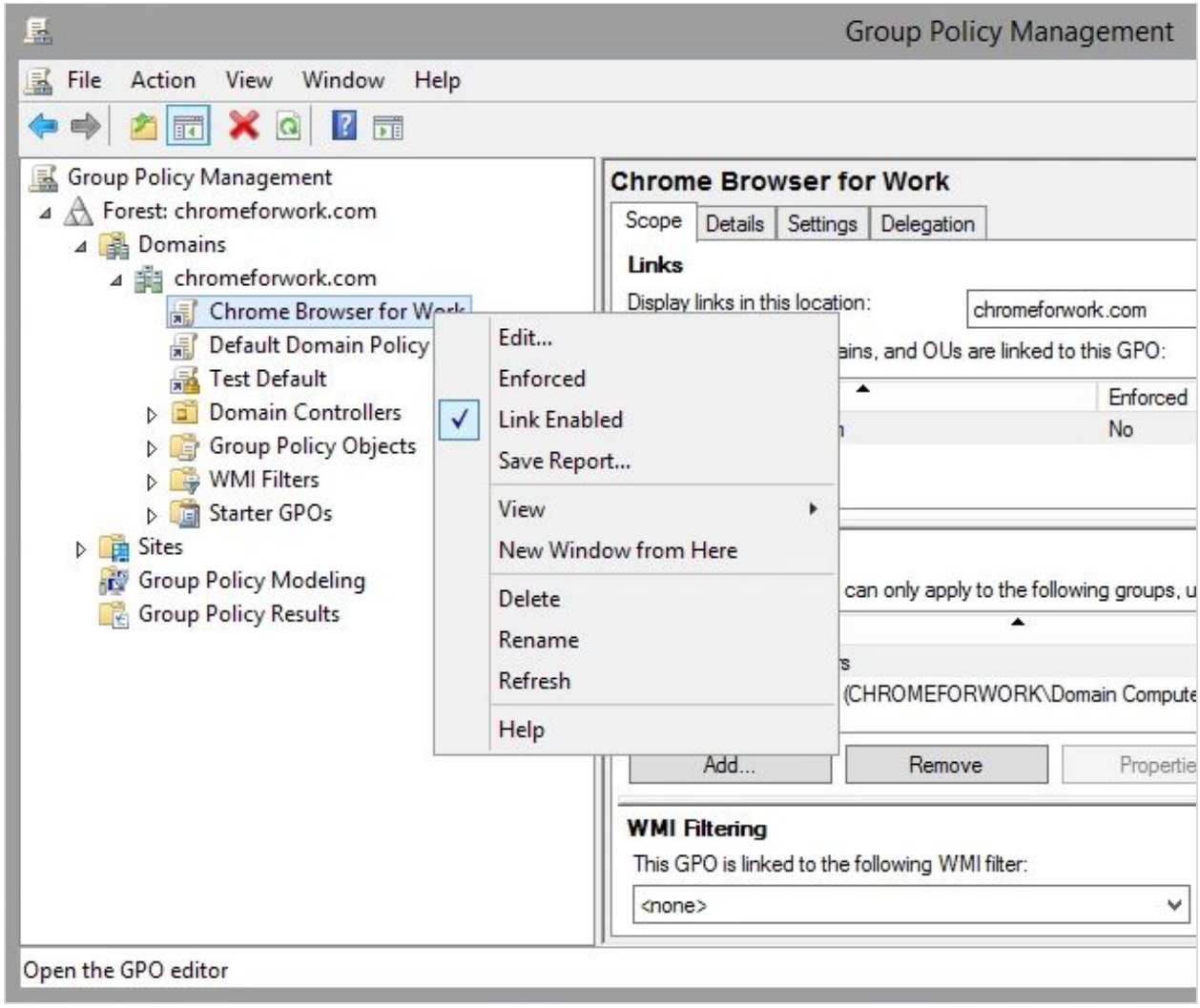
2. Load the Group Policy Management Tool.
   Go to **Server Manager > Tools > Group Policy Management**.

3. Navigate to your domain to create a GPO object.
    a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com**.
    b. Right-click **chromeforwork.com** and select **Create a GPO in this domain…**
    c. Create a new GPO policy called *Chrome Browser for Work*.

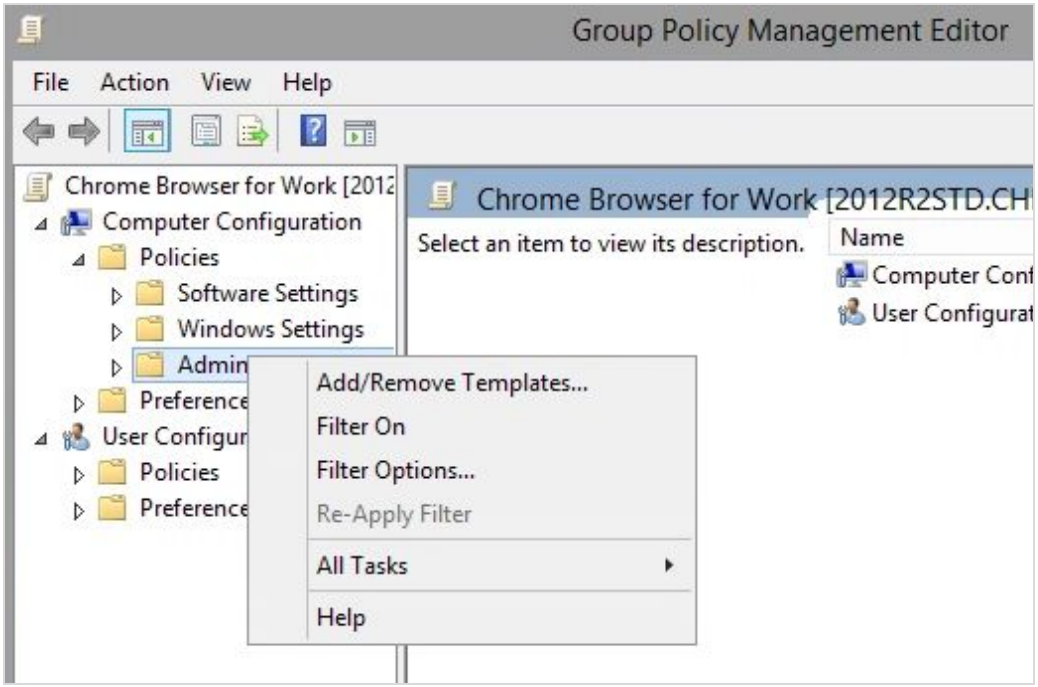




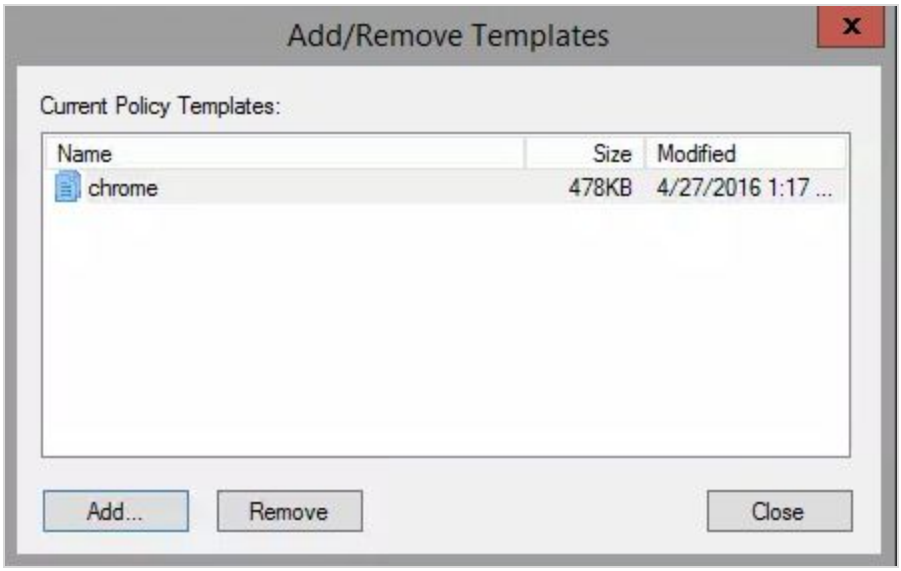
4. Navigate to the newly created GPO object.
    a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com > Chrome Browser for Work**.
    b. Right-click **Chrome Browser for Work** and select **Edit** to load the Group Policy Management Editor.



5. Add the Chrome ADM/ADMX policy template for Chrome browser to the GPO object in Group Policy Management Editor.
   Note: This step can be skipped if you are using centralized GPO storage and have already saved Chrome ADM/ADMX policy templates to centralized storage, as described in step 1 above.
   a. Find **Computer Configuration > Policies > Administrative Templates...**
   b. Right-click **Administrative Templates**, and select **Add/Remove Templates**.

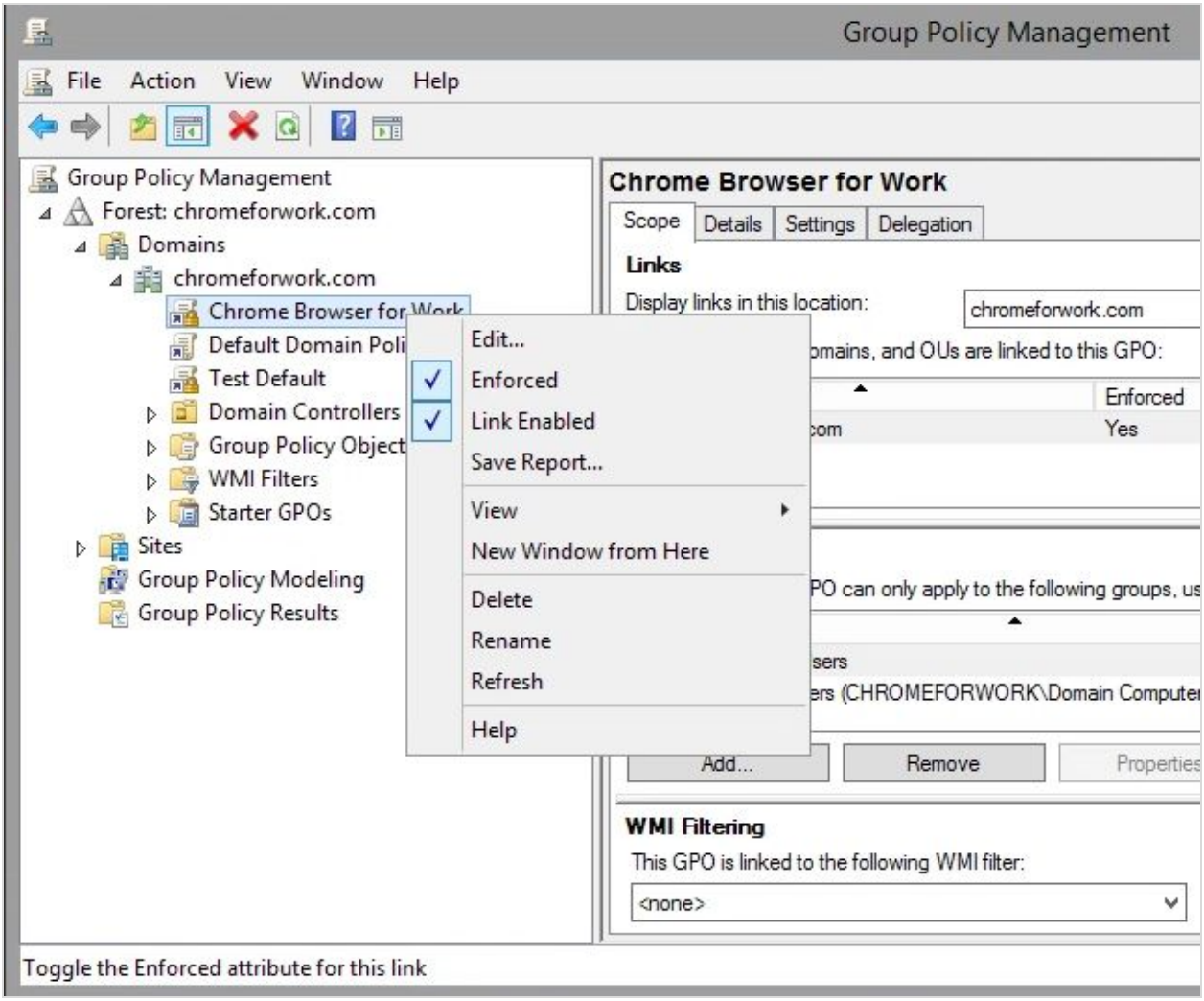


   c. Add the chrome.adm template via the dialog.



   d. Once completed, a Google / Chrome folder will appear under *Administrative Templates* if it's not there already.

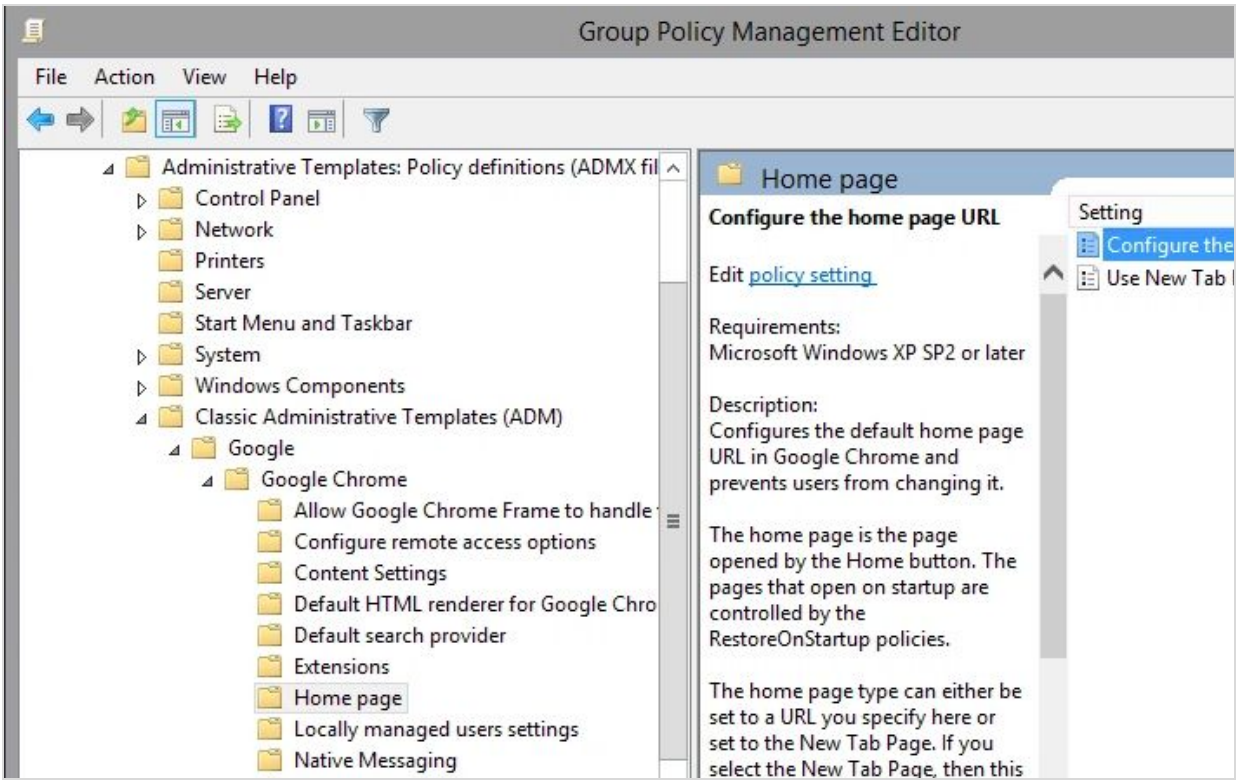
6. Enforce the GPO object.
    a. Find **Group Policy Management** > **Forest:chromeforwork.com** > **Domains** > **chromeforwork.com** > **Chrome Browser for Work**.
    b. Right-click **Chrome Browser for Work** and select **Enforced**.



Change the configuration settings for the target group of users

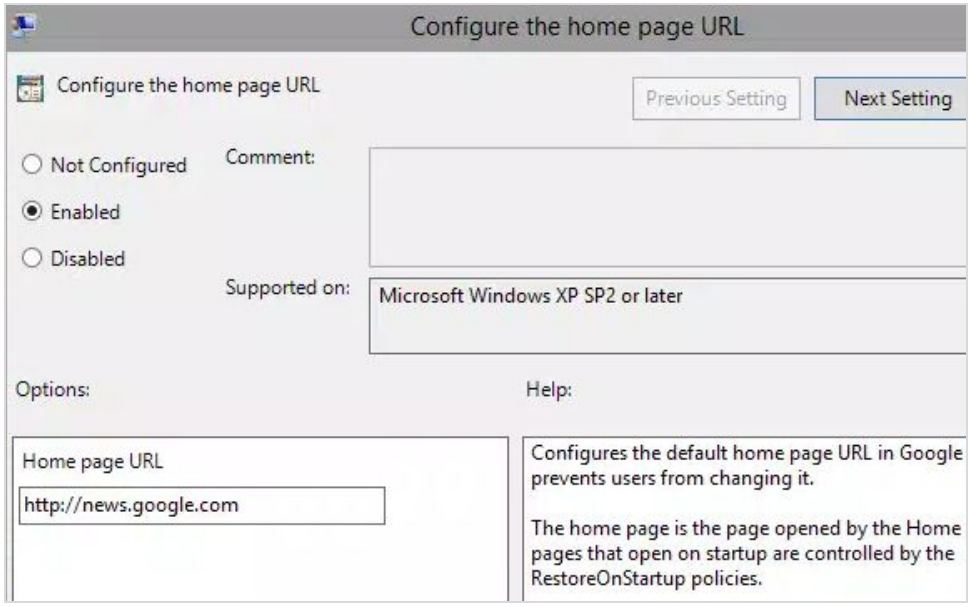
There are many policies you may want to control. For the purposes of this guide, we will walk through the steps of setting up homepage and disabling anonymous usage metric collection. These are two policies administrators commonly set up. A full list of supported policies is at http://www.chromium.org/administrators/policy-list-3.

1. Navigate to the newly created GPO object in the Chrome Management Policy Editor.
    a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com > Chrome Browser for Work**.
    b. Update the policies defined in the Chrome template as needed:



2. Set the Home page.
   This is the URL that users see when they first open the browser or click the "home" button.

   a. Find the **Home page** folder under **Google > Google Chrome** and change the two policies:
      - Enable a new homepage URL and provide a URL.
      - Make sure **Use New Tab Page as Homepage** is enabled.



   b. Find the **Show Home button on toolbar** policy under **Google > Google Chrome**:
      - Enable the policy.

3. Disable anonymous usage statistics and crash information.
   Administrators can turn off sending any crash information or anonymous statistics to Google.

   a. Find the **Enable reporting of usage and crash-related data** policy under **Google > Google Chrome**:
      - Disable the policy

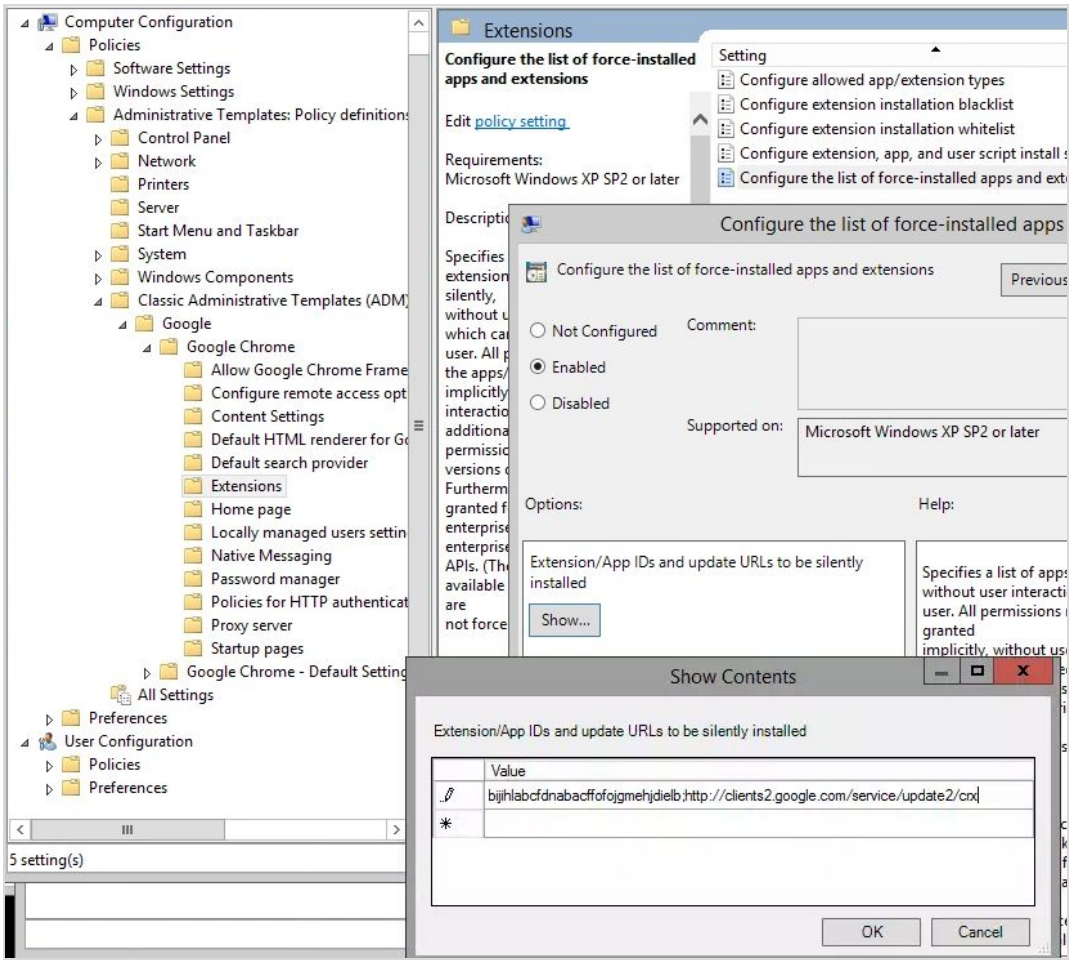
   Note: In both examples above, you can apply these policies at the device or user level by changing the policy under Computer Configuration or User Configuration.

Install Extensions Automatically (optional)

Another policy to try is to force install an extension automatically on Chrome. Let's try setting up **KeepAwake** via the `ExtensionInstallForcelist` policy in the Extension set of policies.

The ID for the Chrome web store version is: `bijihlabcfdnabacffofojgmehjdielb`
The Auto-Update link needed is: `http://clients2.google.com/service/update2/crx`

`bijihlabcfdnabacffofojgmehjdielb;http://clients2.google.com/service/update2/crx`



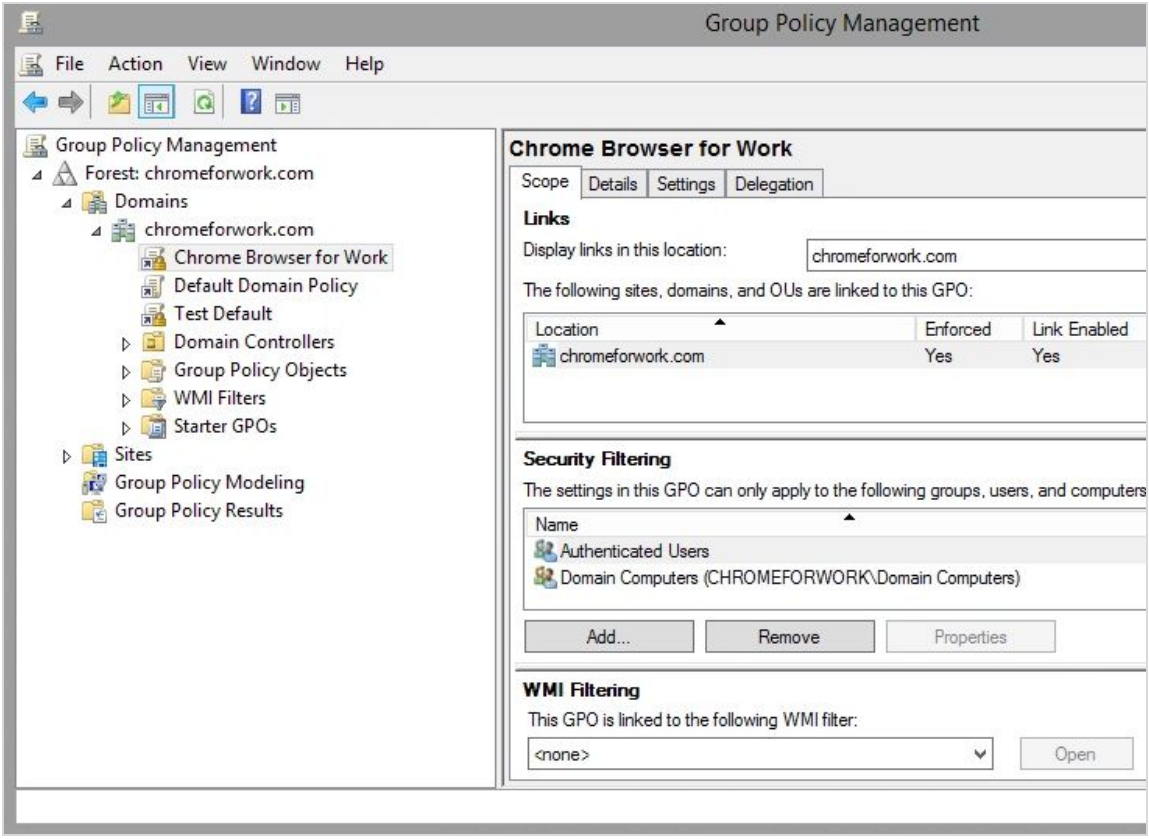
For privately hosted apps (i.e., not in the Chrome Web Store), use a string such as:
`pckdojakecnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml`
… where the URL is specified to the internal app's update.xml rather than the public-facing clients2.google.com URL.

The policies can then be applied to the target users and/or machines. Depending on the network's configuration, this may require time for the policy to propagate. Policies may be propagated manually by running `gpupdate` on the client workstation.

Assign GPO to a set of users

Now let's define which devices and users will be managed by the GPO policies we defined.

1. Navigate to the Chrome Browser For Work GPO object in the Chrome Policy Management tool
   a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com > Chrome Browser for Work** and select it.
2. Assign the GPO object to all devices in the domain.
   a. In the Security Filtering pane, click **Add**.



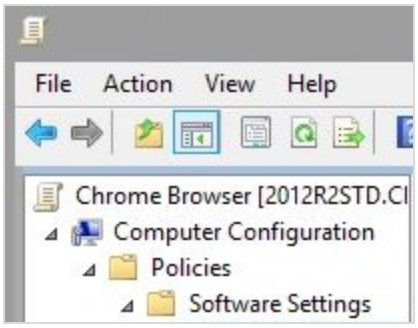
   b. In the **Select User, Computer, or Group** window, type the name of the object you want to add, click **Check Names** (to verify the name you entered), and then click **OK**.
   c. You can type Domain Computers to add all workstations and servers joined to this domain (as shown in the example below) or you can specify a different group of computers.



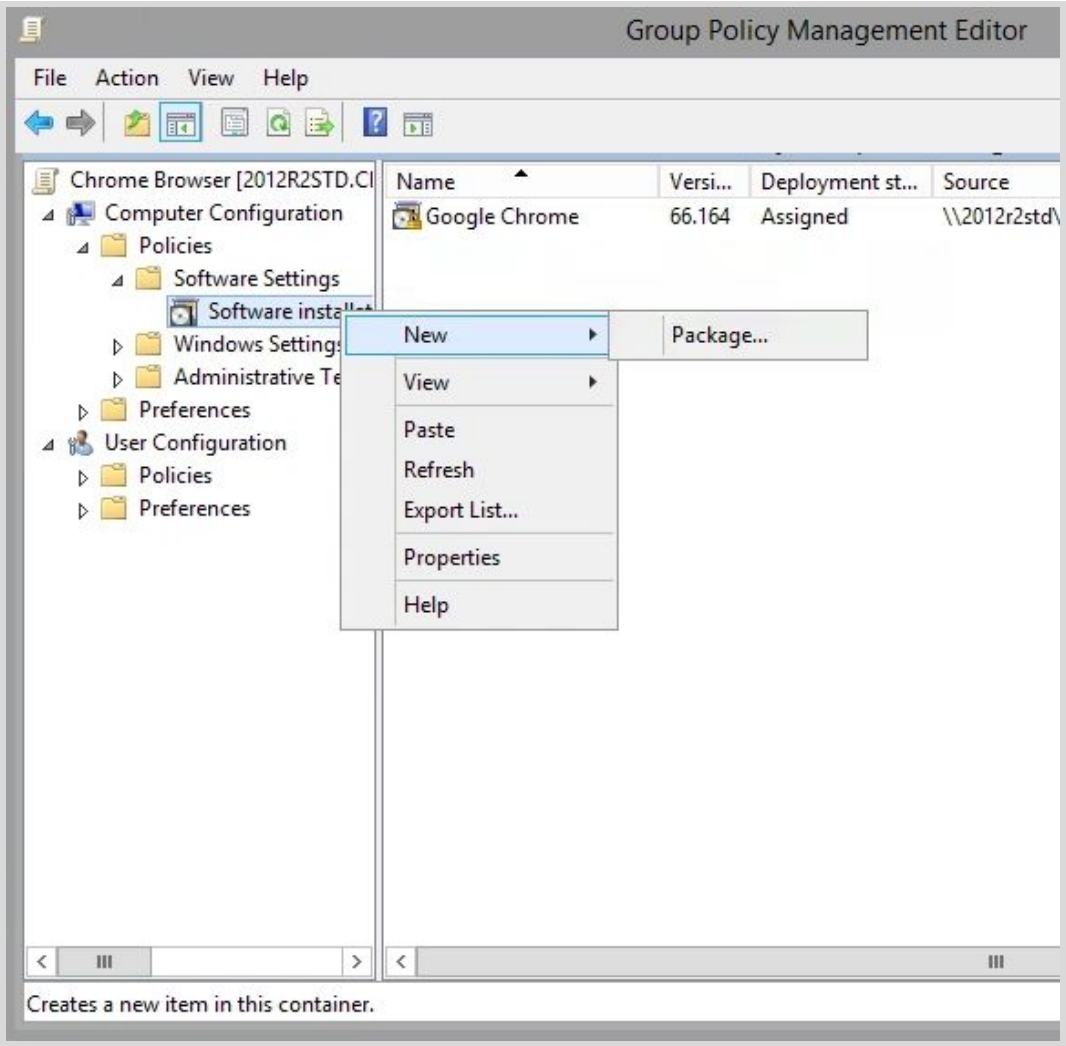
Assign a Package

To install Chrome on computers or users that belong to the domain:

1. Navigate to the newly created GPO object in the Chrome Management Policy Editor.
    a. Find **Group Policy Management** > **Forest:chromeforwork.com** > **Domains** > **chromeforwork.com** > **Chrome Browser for Work**.
2. Under **Computer Configuration**, expand **Software Settings**.



3. Right-click **Software installation**, point to **New**, and then click **Package**.



4. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, `\\server\Packages\GoogleChromeStandaloneEnterprise.msi`.
    a. **Important:** If you use the Browse button to access the location, make sure that you use the UNC path to the shared installer package. Remember that the client machine will look for the file at this specified location.
5. Click **Open**.
6. Click **Assigned**, and then click **OK**. The package is listed in the right pane of the Group Policy window.
7. Close the Group Policy snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.

Note: At this point, you have created a policy to deploy and install Chrome on the endpoint and are ready to test the installation.

Make Chrome the Default Browser (optional)

You may also choose to set Chrome as the default browser. Please take a look at the following instructions for making Chrome the default browser for different versions of Windows:

- Windows 8, 10 - Detailed instructions can be found here.
    - Create a default application association XML file.
    - Create a GPO policy (separate of Chrome Browser for Work policy).
    - Set a default associations configuration file.
- Previous versions of Windows
    - Enable the "DefaultBrowserSettingEnabled" policy.

Manage Google Updates (optional)

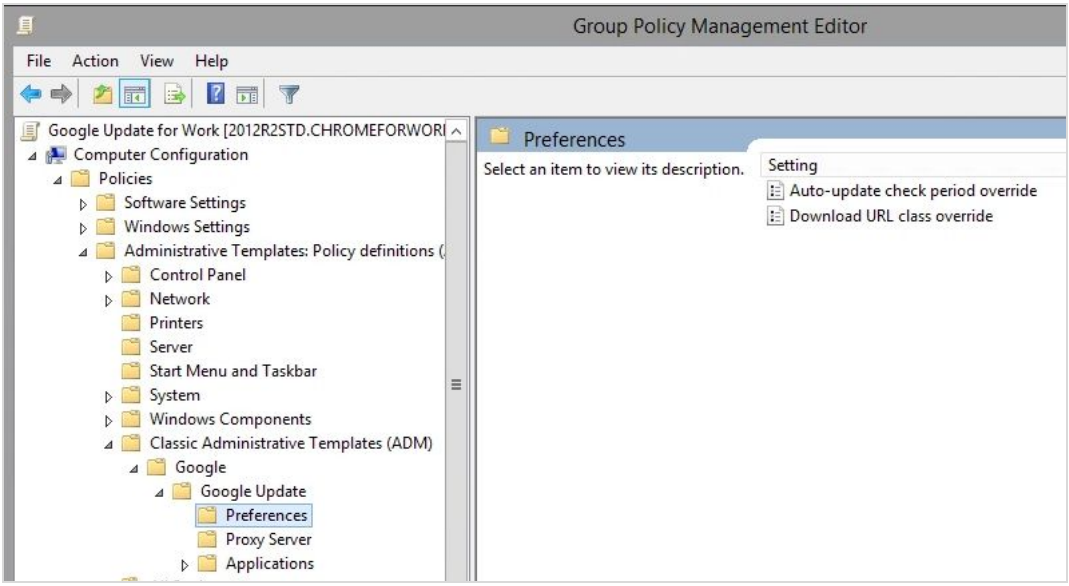
You may also choose to manage how Chrome handles auto updates with Google Update. There are two policies that control Google Update's general behavior.

- **Auto-update check period override**—use this policy to set the period of auto update checks.
- **DownloadPreference**—when enabled this policy can be used to cache updates to reduce external network bandwidth. Use of this policy will result in the server responding with a payload that could be cached by downstream proxies or similar types of content caching solutions. This is a best effort policy and should be verified and tested.

For more details on these two policies, see Install and update Google applications.

1. Download the latest ADM/ADMX policy templates for Google Update from http://dl.google.com/update2/enterprise/GoogleUpdate.adm or http://dl.google.com/update2/enterprise/googleupdateadmx.zip
2. Load the Group Policy Management Tool:
    a. **Server Manager > Tools > Group Policy Management**
3. Navigate to your domain to create a GPO object:
    a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com**.
    b. Right-click **chromeforwork.com** and select **Create a GPO in this domain…**
    c. Create a new GPO policy called **Google Update for Work**.
4. Navigate to the newly created GPO object:
    a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com > Google Update for Work**.
    b. Right-click **Google Update for Work** and select **Edit** to load the Group Policy Management Editor.

5. Add the ADM/ADMX policy template for Google Update to the GPO object in Group Policy Management Editor:
    a. Find **Computer Configuration > Policies > Administrative Templates...**
    b. Right-click **Administrative Templates**, and select **Add/Remove Templates**.
    c. Add the GoogleUpdate.adm template via the dialog.
    d. Once complete, a Google / Google Update folder will appear under *Administrative Templates* if it's not there already.
6. Enforce the GPO object:



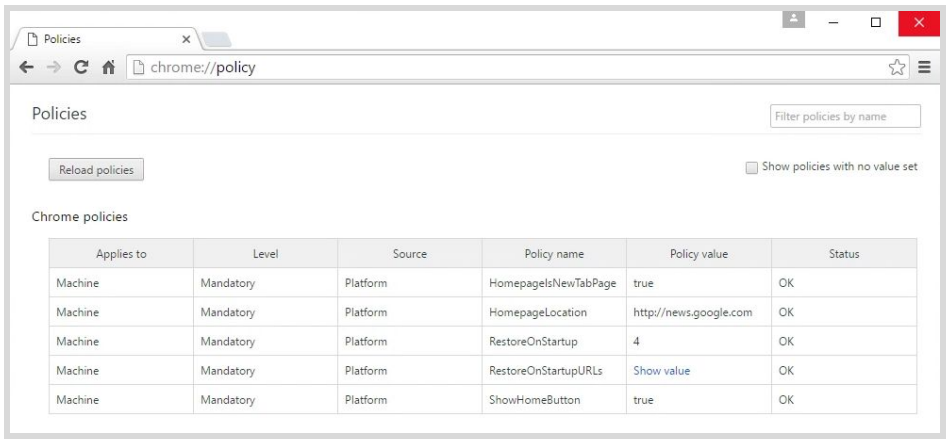
    a. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com > Google Update for Work**.
    b. Right-click **Google Update for Work** and select **Enforce**.

7. Assign the Google Update GPO to the same set of users as the Chrome Browser GPO:
    a. Navigate to the Google Update For Work GPO object in the Chrome Policy Management tool.
        i. Find **Group Policy Management > Forest:chromeforwork.com > Domains > chromeforwork.com > Google Update for Work** and select it.
    b. Assign the GPO object to all devices in the domain.
        i. In the **Security Filtering** pane, click **Add**.
        ii. In the **Select User, Computer, or Group** window, type the name of the object you want to add, click **Check Names** (to verify the name you entered), and click **OK**.
        iii. You can type **Domain Computers** to add all workstations and servers joined to this domain (as in the example below) or you can specify a different group of computers.

Test your installation

Test if Chrome is automatically installed on the target machine:

1. Start the assigned client machine.
2. When the client computer restarts, the managed software package is automatically installed.
3. If it does not install, open the command prompt and run the following command:
   `gpupdate /force`
4. Restart the computer.
5. On client machine, launch Chrome. The settings you applied in step 3 should be noticeable on the test machine. Congratulations!
6. To further verify the policies being applied to Chrome and the user signed-in, go to the address: **chrome://policy** to see all policies being applied.



If the policies have not propagated to the test machine / user, you may be able to run “gpupdate” to refresh policy settings.

On the client machine, use REGEDIT to view the registry settings:

- The client workstation settings are held at HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome

Example Customer Configurations

Healthcare organization in a regulated[1] environment

Chrome configuration

The following were set through GPO policies unless otherwise noted:

Regulation focused

- Disabled the sending of crash information and anonymous usage statistics to Google
- Disabled autofill
- Disabled translate
- Disable Chrome sync
- Disable SearchSuggest
- Blocked installation of Data Saver extension

General configuration

- Force installed LBS on machines, due to a few legacy web applications, and configured to launch IE when needed to based on a known list of incompatible apps
- Show Home Button on the toolbar
- Set the homepage to internal intranet portal
- New tab defaults to the homepage

Software management configuration

- Pushed package via existing software distribution mechanism for Windows
- IT maintained a set of test machines on beta channel to ensure all core web applications used by the business function correctly before the next stable release
- Turned on auto update with Google Update but have a policy template ready (and tested) to stop updates if an issue occurs

Deployment decisions

- Deployed the package on initial pilot machines without any PII information
- Adjusted group policies based on testing and feedback from users while reviewing any policy changes for impact to HIPAA compliance
- Partial deployment to early adopter machines to test deployment with revised policies, including machines collecting PII information
- Deployed to the entire user base after three months of testing by early adopters, location by location over the next 6 months

1. This example configuration is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer should independently evaluate its own particular use of Chrome Browser with enforced policies as appropriate to support its legal compliance obligations.

Public organization with 15,000 users

Chrome Configuration

The following were set through GPO policies unless otherwise noted

- Disabled Extensions and the Default Browser check
- Internet Explorer Favorites and History were not imported
- Changed the default search engine to Google
- Altered the Group Policy Object (GPO) to allow Chrome to self-update on a scheduled basis once the latest version was released and internally tested and approved
- Changed the registry to use Chrome for all mailto: links in any browser so mail links users clicked on would load in Gmail

Software Management Configuration

- Created a desktop shortcut pointing to “email.domain.com” with custom text
- Created shortcuts to additional services in the Windows Start bar: Calendar, Contacts, Documents, Groups, Mail, Sites, and Video

Deployment Decisions

Background: During the deployment process, a new version of Chrome was released.

- Performed two partial deployments with previous version of Chrome
    - First to approximately 8% of their client machines and then incorporated feedback
    - Second to 25% of their client machines
- Performed a Full deployment of the current version of Chrome over the course of two weeks prior to their G Suite go-live
- Allowed the client machines on the previous version of Chrome upgrade to the latest version by enabling the auto-update GPO
- Once all machines were on the latest version of Chrome, the GPO to disable auto-updates was enabled

Global enterprise of more than 35,000 users

Chrome Configuration

The following were set through GPO policies unless otherwise noted

- Used a master_preferences file to disable the default browser check

Software Management Configuration

- Changed the registry to allow Chrome to self-update at a 14 day interval
- With their distribution software they created a shortcut on the desktop to open the URL "email.domain.com" with Chrome

Deployment Decisions

- Deployed the package on a few initial pilot machines and all their base images
- Made changes to the package based on feedback from the testing deployment
- Partial deployment to 400 of their client machines to test the deployment of the package
- Full deployment to the entire user base over a 48 hour period

Global enterprise of more than 25,000 users

Chrome Configuration

The following were set through GPO policies unless otherwise noted

- Due to legacy web application requirements, customer chose to disable default browser check via master preference file
- Configured to update once a week
- Show Home Button on the toolbar
- Enabled and set the default search provider to Google
- Set the homepage to www.google.com
- New tab defaults to the homepage
- Disable the password manager
- Three tabs opened on the browser launch to (Mail, Sites, Help Site)
- Configure auto-update to check once per week

Software Management Configuration

- Push package via software distribution or batch file along with Google Talk Plugin
- Package distribution handled through LANDesk via an AutoIt script
- Disabled placing an icon on desktop via software distribution

Deployment Decisions

- Development of the package on 20 initial beta users
- Made changes to the distribution script based on feedback from the pilot group. Customer decided to use distribution script rather than alter the package (LANDesk)
- Current iterations remove previous Chrome packages as a safeguard
- The Chrome package was pushed to a pilot of 200 users to ratify installation and settings
- Further deployment was based on the G Suite rollout schedule. General practice was to push Chrome to users two weeks before they were migrated to Gmail

Commercial organization with 1,000 users

Chrome Configuration

The following were set through policies unless otherwise noted

- Used a master_preferences file to set default homepage to company Sites page to help users know where to start
- Use vbscript to set default mail handler to Chrome so when users click on mail links in an application or browser it opens Gmail
- During testing an hourly check-in for updates was configured, after testing a 7 day interval was chosen

Deployment Decisions

- Created a test OU and added a few pilot machines
- Adjust group policies based on testing and feedback
- Full deployment to the entire user base before the G Suite Go-Live

Additional Resources

Chrome for business and education Help Center

A collection of help articles covering deployment and frequently asked questions

Chrome Enterprise Bundle

Information about the single package that contains all the tools and components you need to deploy Chrome in your enterprise.

Legacy Browser Support

Learn how to switch between Chrome and legacy sites that require Internet Explorer

Chromium Documentation for Administrators

A source of detailed documentation and common problems

Chrome version

The current version per platform and release

Remotely install software (Microsoft KB)

For Windows Server 2003 and in Windows Server 2008

Chrome for business support policy

Details about what we support with Chrome for business

Windows Quick Start Guide

Answers to many common questions for IT administrators when rolling out the Chrome browser.