



Enterprise Edition

[Google Desktop Home](#) > [Enterprise Edition](#) > Admin Guide

Admin Guide

Contents

- [Introduction](#)
- [Technical Overview](#)
- [Downloading the Software](#)
- [Configuring the Group Policies](#)
 - [General Preferences](#)
 - [Indexing and Capture Control](#)
 - [Enterprise Integration](#)
- [Installing Google Desktop on User Machines](#)
 - [Msiexec Installation Options](#)
- [Updating Google Desktop](#)
- [Pushing Out the Policy to User Registries](#)
- [Integrating Google Desktop with the Google Search Appliance or Google Mini](#)
- [Reference: Registry Keys](#)

Introduction

Google Desktop searches the contents of a user's computer, including files, email messages, viewed web pages, instant messages, images, music, video, and more. Users install Google Desktop from desktop.google.com, and they configure it for themselves. In contrast, Google Desktop for Enterprise is designed for an enterprise environment. A Windows administrator configures Google Desktop for Enterprise and distributes it from a central corporate resource. Google Desktop for Enterprise provides all the user features of Google Desktop, and also indexes Lotus Notes email.

This guide contains information about setting up Google Desktop at an enterprise level and is written for Windows administrators. Any domain administrator can take advantage of the centralized configuration and control features of Google Desktop for Enterprise.

If the enterprise uses a *search appliance* (Google Search Appliance or Google Mini) for internal search, you can provide an integrated search experience. From one search interface, Google Desktop provides information from the user's desktop, the search appliance provides information from the corporate intranet, and Google.com harnesses the Internet.

Technical Overview

Google Desktop for Enterprise makes use of Microsoft Group Policy and Active Directory, a services infrastructure that delivers and applies configurations to users and computers. If you are unfamiliar with Group Policy technology, see the [Microsoft Group Policy documentation](#).

The package for Google Desktop for Enterprise includes an administrative template that defines policies for Google Desktop. You import the administrative template into the Group Policy Management Console or into your Group Policy editor of choice, and then edit the policy settings. Next, you use Active Directory to apply the template to client machines. This action creates and sets the value of the Google Desktop keys in each targeted machine's registry. Alternatively, you can use other administration mechanisms, such as logon scripts, to directly modify the registry settings of user machines.

The rest of this document tells you how to download and configure Google Desktop for Enterprise, and then how to push out the installation to users. For information on how to create an integrated search experience with Google Search Appliance or Google Mini, see [Integrating Google Desktop with Google Search Appliance or Google Mini](#).

Downloading the Software

The administrative template and the installer are available for download from <http://desktop.google.com/enterprise>. Download the template and the installer to your domain controller.

Configuring the Group Policies

To view and modify the Google Desktop Group Policy, open your Group Policy editor. Import the Google Desktop administrative template (.adm) file. Under Administrative Templates\Google\Google Desktop, you'll see the following categories:

- [Preferences](#) define the settings of Google Desktop options. Preference policies make user functions unavailable. If a policy is set to Disabled or Not Configured, a user's own settings generally control the feature.
- [Indexing and Capture Control](#) policies define the type of information that is added to your index, how long it is kept, and so on.
- [Enterprise integration](#) specifies the integration between Google Desktop and Google Search Appliance or Google Mini.

The next sections list and describe each policy, by category. For each policy, the "Since" column lists the first Google Desktop version to support the policy.

Note: The version number reported by the About page for Google Desktop 5.5 (v5.5) begins with **5.5**, **5.6**, or **5.7** — for example, 5.7.0801.01629. The version number for Google Desktop 5 (v5) begins with **5.1**. The version number for Google Desktop 4.5 (v4.5) begins with **5.0**. For more information, see the [Release Notes](#) page.

General Preferences

Policy	Description	Effect of Disabled or Unconfigured Policy	Since
Turn off Advanced Features options	Enabling this policy prevents Google Desktop from sending Advanced Features data to Google (for either improvements or personalization), and users can't change these options. Enabling this policy also prevents pre-5.5 versions of Google Desktop from sending data. Note: In releases before 5.5, this policy was called "Do not send Advanced Features data." See Sending Anonymous Data to Google for examples of using this policy.	If the user has a pre-5.5 version of Google Desktop, the user can choose whether to enable sending data to Google. If the user has version 5.5 or later, the "Turn off Improve Google Desktop option" and "Do not send personalization info" policies are used instead.	v1
Turn off Improve Google Desktop option	Enabling this policy prevents Google Desktop from sending improvement data, including crash reports and anonymous usage data, to Google. Note: This policy applies only to version 5.5 or later and doesn't affect previous versions of Google Desktop. Also note that this policy can be overridden by the "Turn off Advanced Features options" policy. See Sending Anonymous Data to Google for examples of using this policy.	If this policy is disabled, improvement data is sent to Google and the user can't change the option. If this policy is not configured, the user can choose whether to enable the Improve Google Desktop option.	v5.5
Do not send personalization info	Enabling this policy prevents Google Desktop from displaying personalized content, such as news that reflects the user's past interest in articles. Personalized content is derived from anonymous usage data sent to Google. Note: This policy applies only to version 5.5 or later and doesn't affect previous versions of Google Desktop. Also note that this policy can be overridden by the "Turn off Advanced Features options" policy. See Sending Anonymous Data to Google for examples of using this policy.	If this policy is disabled, personalized content can be displayed for all users, and users can't disable this feature. If this policy is not configured, users can choose whether to enable personalization in each gadget that supports this feature.	v5.5
Turn off Google Web Search Integration	Enabling this policy prevents Google Desktop from displaying Desktop search results in queries to google.com . Note: This feature does not transmit any secure, private, or local data to Google. Disabling this functionality limits the user experience and should be avoided.	The user can choose whether to include Desktop search results in queries to google.com or Google Search Appliance or Google Mini.	v1
Turn off Quick Find	Enabling this policy causes Google Desktop to turn off the Quick Find feature, which lets you see results as you type.	A user can choose whether to enable the feature.	v2
Encrypt Index Data	Enabling this policy causes Google Desktop to turn on Windows Encrypting File System (EFS) for the folder that contains the Google Desktop index and related user data. The policy takes effect the next time that Google Desktop starts. There is no analogous user-controlled setting for encrypting the index. Note that Windows EFS is available only on NTFS volumes, so if a user's data is on a FAT volume, the policy has no effect.	This policy has no effect when disabled or not configured.	v1
Choose display option	This policy sets the Google Desktop display option: Sidebar, Deskbar, Floating Deskbar or none.	The user can choose a display option.	v4.5

Sending Anonymous Data to Google

Google Desktop has always offered users the choice of sending anonymous data to Google for the purpose of improving Google Desktop. This data includes crash reports, the list of installed gadgets, features used, Google Desktop version, and so on.

Note: Please send improvement data. It doesn't slow down your system or reveal anything about you or your company, and it really does help make Google Desktop better.

Version 5.5 introduced a second reason to send anonymous usage data: *personalization*. Personalization allows Google Desktop to customize itself to the user's interests

and preferences. For example, if a user decides to personalize the Google News gadget, Desktop can learn which articles the user enjoys, enabling the News gadget to deliver news that's more relevant to the user. The data sent to Google can include news topics, sites, or articles the user has read.

In pre-5.5 releases, a single policy controls whether users can send anonymous usage data to Google. In 5.5+, two additional policies give you finer control over the two kinds of data. For backwards compatibility, the previous policy is still respected, but its name has changed from "Do not send Advanced Features data" to "Turn off Advanced Features options."

The following table shows how to use these policies. If any of your users might have Google Desktop 5.5 or a more recent version, then follow the instructions for v1-v5.5+. In the table, "n/a" means the policy doesn't exist by that name in that release. A "—" means that the setting of that policy doesn't matter.

Send Improvement Data?	Send Personalization Data?	Users' Google Desktop Version	Policy			
			Do not send Advanced Features data	Turn off Advanced Features options	Turn off Improve Google Desktop option	Do not send personalization info
Yes	Yes	v1-v5.5+	n/a	Disable or don't configure	Disable	Disable
Yes	User's choice	v1-v5.5+	n/a	Disable or don't configure	Disable	Don't configure
Yes	No	v1-v5	Disable or don't configure (no way to force sending improvement data)	n/a	n/a	n/a
		v1-v5.5+	n/a	Disable or don't configure	Disable	Enable
User's choice	Yes	v1-v5.5+	n/a	Disable or don't configure	Don't configure	Disable
User's choice	User's choice	v1-v5.5+	n/a	Disable or don't configure	Don't configure	Don't configure
User's choice	No	v1-v5	Disable or don't configure	n/a	n/a	n/a
		v1-v5.5+	n/a	Disable or don't configure	Don't configure	Enable
No	Yes	v1-v5.5+	n/a	Disable or don't configure	Enable	Disable
No	User's choice	v1-v5.5+	n/a	Disable or don't configure	Enable	Don't configure
No	No	v1-v5	Enable	n/a	n/a	n/a
		v1-v5.5+	n/a	Enable	—	—

Indexing and Capture Control

Each one of the following policies can be set to Enabled, Disabled, or Not Configured, as follows:

- If a policy is enabled, the corresponding capture component or feature is disabled, and the user cannot change the setting.
- If a policy is disabled or not configured, the user preference applies, and the user can change the setting.

Administrators can apply policies to individual users and individual machines, so policy settings can appear in either the user section or the machine section. If policy settings appear in both the user section and the machine sections, the following rules generally should be applied, although specific configuration policies can have custom precedence rules.

1. For policies that simply enable or disable a feature, the machine policy takes precedence over the user policy.
2. For blacklists and other text fields, the union of the policies is used.

Policy	Description	Effect of Disabled or Unconfigured Policy	Since
Prevent indexing of Email	This policy controls the indexing of email messages. If this policy is enabled, Google Desktop does not index and store email messages. Also see Prevent indexing of Gmail .	The user can choose whether to allow indexing of email messages.	v1
Prevent indexing of Gmail.	Enabling this policy prevents Google Desktop from indexing Gmail messages. This policy is in effect only when the policy Prevent indexing of email is disabled. When that policy is enabled, all email indexing is disabled, including Gmail indexing.	If both this policy and "Prevent indexing of email" are disabled or not configured, a user can choose whether to index Gmail messages.	v4.5
Prevent indexing of web pages	This policy controls the indexing of web browser history. If this policy is enabled, Google Desktop does not index web pages that the user views using HTTP or HTTPS.	The user can choose whether to allow indexing of web pages.	v1

Prevent indexing of text files	This policy controls the indexing of text files. If this policy is enabled, Google Desktop does not index text files.	The user can choose whether to allow indexing of text files.	v1
Prevent indexing of media files	This policy controls the indexing of media files. If this policy is enabled, Google Desktop does not index media files.	The user can choose whether to allow indexing of media files.	v1
Prevent indexing of contacts	This policy controls the indexing of Microsoft Outlook's contact list. If this policy is enabled, Google Desktop does not index the contact list.	The user can choose whether to allow indexing of contacts.	v2
Prevent indexing of calendar entries	This policy controls the indexing of Microsoft Outlook's calendar entries. If this policy is enabled, Google Desktop does not index calendar entries.	The user can choose whether to allow indexing of calendar entries.	v2
Prevent indexing of tasks	This policy controls the indexing of Microsoft Outlook's tasks. If this policy is enabled, Google Desktop does not index tasks.	The user can choose whether to allow indexing of tasks.	v2
Prevent indexing of notes	This policy controls the indexing of Microsoft Outlook's notes. If this policy is enabled, Google Desktop does not index notes.	The user can choose whether to allow indexing of notes.	v2
Prevent indexing of journal entries	This policy controls the indexing of Microsoft Outlook's journal entries. If this policy is enabled, Google Desktop does not index journal entries.	The user can choose whether to allow indexing of journal entries.	v2
Prevent indexing of Word documents	This policy controls the indexing of Microsoft Word documents. If this policy is enabled, Google Desktop does not index Word documents.	The user can choose whether to allow indexing of Word documents.	v1
Prevent indexing of Excel documents	This policy controls the indexing of Microsoft Excel documents. If this policy is enabled, Google Desktop does not index Excel documents.	The user can choose whether to allow indexing of Excel documents.	v1
Prevent indexing of PowerPoint documents	This policy controls the indexing of Microsoft PowerPoint documents. If this policy is enabled, Google Desktop does not index PowerPoint documents.	The user can choose whether to allow indexing of PowerPoint documents.	v1
Prevent indexing of PDF documents	This policy controls the indexing of PDF documents. If this policy is enabled, Google Desktop does not index PDF documents.	The user can choose whether to allow indexing of PDF documents.	v1
Prevent indexing of ZIP files	This policy controls the indexing of ZIP files. If this policy is enabled, Google Desktop does not index ZIP files.	The user can choose whether to allow indexing of ZIP files.	v3
Prevent indexing of secure web pages	This policy controls the indexing of secure web pages. If this policy is enabled, Google Desktop does not index web pages that the user views via HTTPS.	The user can choose whether to allow indexing of secure web pages.	v1
Prevent indexing of specific web sites and folders	<p>This policy lets you prevent Google Desktop from indexing specific web sites or folders. You specify a list of URI substrings to exclude from indexing. If an item's URL or path name contains any of the specified strings, it is not indexed.</p> <p>As an example, if this policy is enabled, adding <code>images.example.com</code> excludes from the index everything in the company's images web server. Adding "C:\SensitiveCompanyData" prevents indexing of anything in that folder on the user's local machine.</p> <p>The user setting for this preference is "Don't search these items or files with the following paths."</p>	None.	v1
Prevent indexing of IM chats	This policy disables indexing of instant messaging chat programs.	The user can choose whether to index IM chat conversations.	v1
Prevent indexing of password-protected Office documents (Word, Excel)	This policy controls the indexing of password-protected Microsoft Office documents. If this policy is enabled, Google Desktop does not index password-protected Microsoft Office documents.	The user can choose whether to allow indexing of password-protected Microsoft Office documents.	v1
Prevent indexing of specific extensions	This policy blocks indexing of files with specified extensions. Enter a list of file extensions to exclude from indexing, separating the entries with commas.	None.	v1
Disallow user to add search locations to index	Enabling this policy prevents the user from adding any additional drives and networked folders to index.	None.	v2
Allow indexing of specific folders	Use this policy to specify additional drives and networked folders to index.	None.	v2
Only retain emails that are less than x days old	This policy allows you to configure Google Desktop to retain only emails that have been in the index for the specified number of days or fewer.	None.	v3
Only retain webpages that are less than x days old	This policy allows you to configure Google Desktop to retain only web pages that have been in the index for the specified number of days or fewer.	None.	v3
Only retain files that are less than x days old	This policy allows you to configure Google Desktop to retain only files that have been in the index for the specified number of days or fewer.	None.	v3

Only retain IM that are less than x days old	This policy allows you to configure Google Desktop to retain only instant messages that have been in the index for the specified number of days or fewer.	None.	v3
Remove deleted items from the index	This policy removes deleted items from the index and cache. Deleted items will no longer be searchable.	None.	v4
Allow historical indexing for multiple users simultaneously	Enabling this policy allows a computer to generate first-time indexes for multiple users simultaneously.	Historical indexing happens only for the logged-in user that was connected last; historical indexing for any other logged-in user happens the next time that other user connects.	v5

Enterprise Integration

These settings specify how users in your enterprise will use Google Desktop.

Policy	Description	Effect of Disabled or Unconfigured Policy	Since								
Block AutoUpdate	Enabling this policy prevents Google Desktop from automatically checking for and installing updates from desktop.google.com . If you enable this policy, you must distribute updates to Google Desktop using Group Policy, SMS, or a similar enterprise software distribution mechanism. Check http://desktop.google.com/enterprise/ for updates.	Google Desktop periodically checks for updates from desktop.google.com .	v1								
Use system proxy settings when auto-updating	Enabling this policy makes Google Desktop use the machine-wide proxy settings (as specified using proxycfg.exe, for example) when performing auto-updates (if auto-updates are enabled).	Google Desktop uses the logged-on user's Internet Explorer proxy settings when checking for auto-updates (if auto-updates are enabled).	v4.5								
Prohibit Policy-Unaware Versions	This policy prohibits installation and execution of version 1.0 of Google Desktop, which is unaware of group policy. Enabling this policy prevents users from installing or running a version of Google Desktop that you cannot administer.	None.	v1								
Minimum Allowed Version	The Minimum Allowed Version setting prohibits users from installing or using a Google Desktop version that is older than the specified version. When enabling this policy, you should also enable the "Prohibit Policy-Unaware Versions" policy to block the initial version of Google Desktop, which did not support group policy. Google Desktop versions are expressed with numbers corresponding to the build date such as 2.2005.0401.0600. To view the version number, click the About link on the Google Desktop page for the given installation.	None.	v1								
Maximum Allowed Version	This policy prohibits users from installing or using a Google Desktop version that is newer than the specified version.	None.	v1								
Disallow Gadgets	This policy prevents the use of all Google Desktop gadgets. The policy applies to gadgets that are included in the Google Desktop installation package (built-in gadgets) and to gadgets that a user might want to add later (non-built-in gadgets). You can prohibit use of all non-built-in gadgets, but allow use of built-in gadgets. To do so, enable this policy and then select the option "Disallow only non-built-in gadgets." You can supersede this policy to allow specified built-in and non-built-in gadgets. To do so, enable this policy and then specify the gadgets you want to allow under "Gadget Whitelist."	Users can install any gadget.	v1								
Allow silent installation of gadgets	Enabling this policy lets you specify a list of Google Desktop gadgets that can be installed without confirmation from the user. Add a gadget by placing its class ID (CLSID) or program identifier (PROGID) in the list, surrounded with curly braces ({}).	None.	v4								
Gadget Whitelist	<div>This policy specifies a list of Google Desktop gadgets that you want to allow, as exceptions to the "Disallow gadgets" policy. This policy is valid only when the "Disallow gadgets" policy is enabled. To whitelist a built-in gadget, add its class ID to the list, surrounded by curly braces ({}). Do not include the gadget name. For example, to allow the Analog Clock gadget, add {DF83CBC5-6FAD-4074-BF03-8254392DEFA0} to the list.</div> <table><tr><th>Gadget</th><th>Class ID</th></tr><tr><td>Analog Clock</td><td>{DF83CBC5-6FAD-4074-BF03-8254392DEFA0}</td></tr><tr><td>Battery Meter</td><td>{B63B113D-DEE2-4a70-BC8B-FE77DDD40778}</td></tr><tr><td>Digital Clock</td><td>{5EBA73D8-8A97-47de-A373-2BCBDCA3D539}</td></tr></table> <td>None.</td> <td>v1</td>	Gadget	Class ID	Analog Clock	{DF83CBC5-6FAD-4074-BF03-8254392DEFA0}	Battery Meter	{B63B113D-DEE2-4a70-BC8B-FE77DDD40778}	Digital Clock	{5EBA73D8-8A97-47de-A373-2BCBDCA3D539}	None.	v1
Gadget	Class ID										
Analog Clock	{DF83CBC5-6FAD-4074-BF03-8254392DEFA0}										
Battery Meter	{B63B113D-DEE2-4a70-BC8B-FE77DDD40778}										
Digital Clock	{5EBA73D8-8A97-47de-A373-2BCBDCA3D539}										

	<table><tr><td>Email</td><td>{634E2122-6BB7-430f-B452-CF04C8722C47}</td></tr><tr><td>Google Calendar</td><td>{95c665af-74b2-4c61-b62e-8b7ce8e886f3}</td></tr><tr><td>Google Talk</td><td>{54648593-C279-476d-82AF-9CFCB45313B4}</td></tr><tr><td>Maps</td><td>{3C66FE03-4FB7-497c-850F-60265842D043}</td></tr><tr><td>Media Player</td><td>{7CEAD8F9-51DB-4365-829A-E67DBDF1B3E1}</td></tr><tr><td>News</td><td>{ECCB4495-7F5B-4b4e-A887-7A66BE948AC1}</td></tr><tr><td>Orkut</td><td>{AAE49563-84D9-487b-AC42-7B2683B48C1F}</td></tr><tr><td>Photo</td><td>{4516155C-B94E-4334-8D26-D4BF0932581C}</td></tr><tr><td>Quick View</td><td>{50EDABE0-140C-406d-A8B9-32652145560A}</td></tr><tr><td>Scratch Pad</td><td>{65E256AC-B335-4004-8C6A-5A7F986CD0A4}</td></tr><tr><td>Search Box</td><td>{44B0B5D8-55C9-46b4-9CCA-62842C9B3BFF}</td></tr><tr><td>Stock</td><td>{F11D7457-2381-4337-977F-4090C75EBC23}</td></tr><tr><td>System Monitor</td><td>{2F47A051-6AA3-4E7A-A5F5-2446708AFA18}</td></tr><tr><td>To Do</td><td>{3872340B-239E-4c1c-A783-0E2A5E28383B}</td></tr><tr><td>Weather</td><td>{87EE4771-AC3D-4AFB-9358-78BB7AC03DBA}</td></tr><tr><td>Web Clips</td><td>{FBA13A6F-E595-48b7-AB73-2630042A4E93}</td></tr><tr><td>Wireless Meter</td><td>{C6F815A3-B859-4eba-83D1-AC097805C2EA}</td></tr></table> <p>To whitelist a non-built-in gadget, add its class ID (CLSID) or program identifier (PROGID), surrounded by curly braces ({}).</p>	Email	{634E2122-6BB7-430f-B452-CF04C8722C47}	Google Calendar	{95c665af-74b2-4c61-b62e-8b7ce8e886f3}	Google Talk	{54648593-C279-476d-82AF-9CFCB45313B4}	Maps	{3C66FE03-4FB7-497c-850F-60265842D043}	Media Player	{7CEAD8F9-51DB-4365-829A-E67DBDF1B3E1}	News	{ECCB4495-7F5B-4b4e-A887-7A66BE948AC1}	Orkut	{AAE49563-84D9-487b-AC42-7B2683B48C1F}	Photo	{4516155C-B94E-4334-8D26-D4BF0932581C}	Quick View	{50EDABE0-140C-406d-A8B9-32652145560A}	Scratch Pad	{65E256AC-B335-4004-8C6A-5A7F986CD0A4}	Search Box	{44B0B5D8-55C9-46b4-9CCA-62842C9B3BFF}	Stock	{F11D7457-2381-4337-977F-4090C75EBC23}	System Monitor	{2F47A051-6AA3-4E7A-A5F5-2446708AFA18}	To Do	{3872340B-239E-4c1c-A783-0E2A5E28383B}	Weather	{87EE4771-AC3D-4AFB-9358-78BB7AC03DBA}	Web Clips	{FBA13A6F-E595-48b7-AB73-2630042A4E93}	Wireless Meter	{C6F815A3-B859-4eba-83D1-AC097805C2EA}		
Email	{634E2122-6BB7-430f-B452-CF04C8722C47}																																				
Google Calendar	{95c665af-74b2-4c61-b62e-8b7ce8e886f3}																																				
Google Talk	{54648593-C279-476d-82AF-9CFCB45313B4}																																				
Maps	{3C66FE03-4FB7-497c-850F-60265842D043}																																				
Media Player	{7CEAD8F9-51DB-4365-829A-E67DBDF1B3E1}																																				
News	{ECCB4495-7F5B-4b4e-A887-7A66BE948AC1}																																				
Orkut	{AAE49563-84D9-487b-AC42-7B2683B48C1F}																																				
Photo	{4516155C-B94E-4334-8D26-D4BF0932581C}																																				
Quick View	{50EDABE0-140C-406d-A8B9-32652145560A}																																				
Scratch Pad	{65E256AC-B335-4004-8C6A-5A7F986CD0A4}																																				
Search Box	{44B0B5D8-55C9-46b4-9CCA-62842C9B3BFF}																																				
Stock	{F11D7457-2381-4337-977F-4090C75EBC23}																																				
System Monitor	{2F47A051-6AA3-4E7A-A5F5-2446708AFA18}																																				
To Do	{3872340B-239E-4c1c-A783-0E2A5E28383B}																																				
Weather	{87EE4771-AC3D-4AFB-9358-78BB7AC03DBA}																																				
Web Clips	{FBA13A6F-E595-48b7-AB73-2630042A4E93}																																				
Wireless Meter	{C6F815A3-B859-4eba-83D1-AC097805C2EA}																																				
Alternate User Data Directory	<p>This policy allows you to specify a directory for storing user data for Google Desktop (such as index data and cached documents). You may use [USER_NAME] or [DOMAIN_NAME] in the path to specify the current user's name or domain. If [USER_NAME] is not specified, the user name is appended at the end of the path.</p> <p>Storing user data on network volumes can negatively affect performance.</p>	None.	v1																																		
Maximum allowed Outlook connections	<p>This policy specifies the maximum number of open connections that Google Desktop maintains with the Exchange server. Google Desktop opens a connection for each email folder that it indexes. If insufficient connections are allowed, Google Desktop cannot index all the user email folders.</p> <p>The default value is 400. Because users rarely have as many as 400 email folders, Google Desktop rarely reaches the limit.</p> <p>If you set this policy's value above 400, you must also configure the number of open connections between Outlook and the Exchange server. By default, approximately 500 connections are allowed. If Google Desktop uses too many of these connections, Outlook might be unable to access email.</p>	None.	v2																																		
Disallow sharing and receiving of web history and documents across computers	<p>This policy prevents Google Desktop from sharing the user's web history and document contents across the user's different Google Desktop installations, and also prevents Google Desktop from receiving such shared items from the user's other machines.</p>	None.	v3																																		
Disallow sharing of web history and documents across computers	<p>This policy prevents Google Desktop from sending the user's web history and document contents from this machine to the user's other machines. It does not prevent reception of items from the user's other machines.</p>	None.	v3																																		
Maximum allowed Exchange indexing rate	<p>This policy allows you to specify the maximum number of emails that are indexed per minute.</p>	None.	v2																																		
Disallow storage of gadget content and settings	<p>This policy prevents users from storing their gadget content and settings with Google. When the policy is enabled, users will be unable to access their gadget content and settings from other computers and all content and settings will be lost if Google Desktop is uninstalled.</p>	None.	v4																																		
Enable or disable safe browsing	<p>Google Desktop safe browsing informs the user whenever they visit any site which is a suspected forgery site or may harm their computer. Enabling this policy turns on safe browsing; disabling the policy turns it off.</p>	<p>If this policy is not configured, the user can select whether to turn on safe browsing.</p>	v5																																		

Installing Google Desktop on User Machines

Google Desktop is intended for installation on multiple computers in an organization. Google Desktop supports MSI installation, so you can use your preferred installation method.

The following table lists the installation options and provides comments.

Installation Method	Comment
Have users install Google Desktop themselves	Users with administrator access to their computers can install the .msi file themselves, if you make it available on a server.
Use Group Policy Software Installation	You can publish or assign the installation.
Use Systems Management Server (SMS)	<p>Google Desktop is installed and available for all users on the machine. We recommend that you configure SMS to do per-machine installations only by setting ALLUSERS=1.</p> <p>Attended (interactive) installations cause Google Desktop to be automatically enabled for the user who performs the installation. Unattended (silent) installs are enabled only when the user runs Google Desktop from one of the shortcuts.</p> <p>Never perform an unattended installation when a user is logged in to the machine. Such an installation typically cannot complete properly.</p>

Msiexec Installation Options

This section describes command-line options you can use when installing Google Desktop using `msiexec`. You can specify two kinds of options when installing Google Desktop:

- Standard `msiexec` options, such as `/i` and `/q`.
- Google Desktop options such as `-noshortcut` and `-defaultdisplay`, which are specified using the `GDCMDARGS` property.

Here's an example of both kinds of options in a single installation command:

```
msiexec /i gd.msi GDCMDARGS="-noshortcut"
```

You can use more than one of each kind of option. Example:

```
msiexec /i gd.msi /q GDCMDARGS="-noshortcut -gtype=4"
```

Here are some typical commands:

- Install Google Desktop with just the clock, weather, and scratch pad gadgets in the sidebar.

```
msiexec /i gd.msi GDCMDARGS="-gtype=4"
```

- Install Google Desktop without adding a shortcut.

```
msiexec /i gd.msi GDCMDARGS="-noshortcut"
```

- Silently install Google Desktop with no visible sidebar or search box, and without adding a shortcut.

```
msiexec /i gd.msi /q GDCMDARGS="-defaultdisplay none -noshortcut"
```

The following table lists some commonly used `msiexec` options. You can get a complete list by going to a shell window and entering the command `msiexec`.

Standard msiexec Option	Description
<code>/fvomus gd.msi</code>	Install the specified copy of Google Desktop even if the user has installed a more recent version.
<code>/i gd.msi</code>	Install Google Desktop.
<code>/q</code>	Install or uninstall without displaying anything to the user.
<code>/x gd.msi</code>	Uninstall Google Desktop.

The next table lists options that can be passed to Google Desktop by setting the `GDCMDARGS` property. Example: `msiexec /i gd.msi GDCMDARGS="-noshortcut -gtype=4"`

GDCMDARGS Option	Description
defaultdisplay <i>displaymode</i>	Change the initial display mode. Without this option, the sidebar is initially displayed along the edge of the screen. The value of <i>displaymode</i> is one of the following: <ul style="list-style-type: none"> • deskbar: Don't display the sidebar; instead, display a search box in the user's taskbar. • minibar: Like deskbar, except that the search box floats on the user's desktop. Also known as a <i>floating deskbar</i>. • none: Don't display the sidebar or the search box.
-default_sidebar= <i>number</i>	Specify the sidebar mode. The value of <i>number</i> is one of the following: <ul style="list-style-type: none"> • 0: Sidebar not always on top • 1: Sidebar always on top; this is the default value • 3: Enable auto-hide, which causes the sidebar to slide onto the user's screen when the mouse is near the screen's edge and disappear again once the mouse is no longer on the sidebar
-gtype= <i>number</i>	Specify which gadgets should be in the sidebar, by default. The value of <i>number</i> is one of the following: <ul style="list-style-type: none"> • 0: the default gadgets for that Google Desktop release • 1: clock, news, scratch pad, photos • 2: clock, news, scratch pad, weather • 3: clock, news, scratch pad • 4: clock, weather, scratch pad
-noshortcut	Don't create a shortcut on the Windows desktop for Google Desktop.

Updating Google Desktop

Google AutoUpdate ensures that users are running the most current version of Google Desktop. Google Desktop clients ping Google's update server daily to request updates. When an update is available, it is automatically downloaded and installed on the client.

If corporate policy prohibits this type of update, or if users do not have local administrative privileges, use Group Policy or other software management systems such as SMS to keep clients up to date.

Pushing Out the Policy to Users

Once you have configured the Google Desktop Group Policy, you need to push it to users. To do so, create an Active Directory Group Policy Object (GPO), edit it from the Active Directory Management Console or the Group Policy Management Console, and apply the GPO to the whole domain, or to an Organizational Unit of that domain.

When you push out the policies, end-user registries are updated with the following subkeys:

- User policies for Google Desktop: HKCU\Software\Policies\Google\Google Desktop
- Machine policies for Google Desktop: HKLM\Software\Policies\Google\Google Desktop

These subkeys are created in areas of the registry that are reserved for group policy settings. The settings are protected with access control lists that prevent tampering by non-administrative users.

For information about the registry keys used for Google Desktop for Enterprise, refer to [Reference: Registry Keys](#).

Integrating Google Desktop and the Google Search Appliance or Google Mini

Integrating Google Desktop for Enterprise with Google Search Appliance or Google Mini enables you to combine desktop search results and enterprise search results on a single page. Desktop search results are served by Google Desktop, and enterprise search results are served by the search appliance.

On www.google.com, a user can type a single search query and then apply that search query to various search services by clicking the links that appear above the search field. These are called top links. For example, one search query can apply to Groups or Images, depending on which top link the user clicks. When you integrate Google Desktop with a search appliance, new top links appear above your search field, as follows:

- When a user views the Google.com web page or a Google Desktop search page, a top link for your enterprise search appears. For example, if your enterprise search application is called Searchlight, a link for Searchlight appears.
- When a user views your enterprise search page, a top link for Desktop appears.

This section gives instructions for integrating with Google Search Appliance 4.6.x or later or Google Mini 4.4.102.x or later. If you are using an older version, please update to the latest search appliance software. You can find update instructions and software at the [Enterprise Support Site](#).

If you update the search appliance software, be sure to update the stylesheet so that it's based on the default stylesheet for the new software version. The software update instructions explain how to update the stylesheet without losing custom XSLT modifications.

The following instructions describe how to integrate Google Desktop on a single computer with a search appliance. To make these changes for multiple users, use Windows Group Policy.

Note: You must have Administrator access to the machine that you want to integrate with the search appliance.

Edit the GoogleDesktop.adm template and go to the Enterprise Integration policy folder. For information on the location of the policies, see the [Configuring the Group Policies](#) section. Configure the following policies:

Policy	Description
Enterprise Search Tab	<p>This policy allows you to add a top link for your appliance search to your www.google.com and desktop search pages. Google Desktop inserts the top link on your corporate search page only when the page comes from a server that has been specified in the group policy called Google Search Appliances.</p> <p>In the properties page of the policy, do the following:</p> <ul style="list-style-type: none"> • Enable the policy. • Enter the name of the top link for your appliance search. • Enter the URL for the search page of your search appliance. Example: <code>http://search.company.com/search?site=default_collection&client=integrated_frontend&proxystylesheet=integrated_frontend&output=xml_no_dtd&proxycustom=<HOME/></code> Note: Do not configure the policy to check whether the search homepage supports <code>&q=<query></code>. • Enter the search results URL for your search appliance. Example: <code>http://search.company.com/search?q=[DISP_QUERY]&site=default_collection&client=integrated_frontend&proxystylesheet=integrated_frontend&output=xml_no_dtd</code> • Configure the policy to check whether the search results page supports <code>&q=<query></code>. Enabling the policy to do this lets Google carry over query terms across all the search services; for example, search queries entered in the Web search service are automatically carried over to the Desktop search service.
Google Search Appliances	<p>This policy enables Google Desktop to insert desktop results into the search results of queries made on the search appliance.</p> <p>In the properties page of the policy, do the following:</p> <ul style="list-style-type: none"> • Enable the policy. • Enter the host name of your search appliance. Example: <code>search.company.com</code>.

After you configure the group policies, you can start testing the integration.

Reference: Registry Keys

The tables below list and explain the Google Desktop registry keys that are controlled by the group policy. For each registry key name, the tables list the name, type, description, and default value and give an example. In addition, note the following:

- The column "User Option" specifies whether the key has an analogous end-user setting. If there is an analogous end-user setting, the administrative setting controls use of the end-user setting.
- The table's last column, "Affects UI?" specifies whether the group policy setting is made visible to the user. For example, a group policy setting might disable a user feature by graying out a user option.
- All values for REG_SZ type keys are strings.

The following registry keys are under `Policies\Google\Google Desktop\Preferences`:

Name	Type	Description	Default Value	Example	User Option	Affects UI?
file_extensions_to_skip	REG_SZ	Comma-delimited extension list	tmp, temp, log, pst, dat, 000, pf, xml, obj, pdb	,tmp,temp,log	Y	N
onebox_mode	REG_DWORD	Controls insertion of Google Desktop OneBox in google.com	1	1	Y	Y
blacklist-1	Key	List of schema IDs	""	2	Y	Y
blacklist-2	Key	List of file extensions	""	XLS	Y	Y
blacklist-3	Key	List of protocol identifiers	""	HTTPS	Y	Y
blacklist-6	Key	List of URI substrings (contains)	""	http://www/hr/	Y	Y
blacklist-12	Key	List of Component IDs	""	53, {Guid-Identifier-String}	Y	Y
blacklist-13	Key	List of security features	""	SECUREOFFICE	Y	Y
error_report_on	REG_DWORD	Controls reporting of crash + usage data	1	1	Y	Y
hyper_off	REG_DWORD	Controls Quick Find	1	1	Y	Y

policy_search_location_whitelist	REG_SZ	String values of specific folders to index	""	c:\userdata	N	Y
user_search_locations	REG_DWORD	Controls user ability to add search locations	1	1	Y	Y
email_days_to_retain	REG_DWORD	Control number of days to retain emails	30	30	N	N
webpage_days_to_retain	REG_DWORD	Control number of days to retain web pages	30	30	N	N
file_days_to_retain	REG_DWORD	Control number of days to retain files	30	30	N	N
im_days_to_retain	REG_DWORD	Control number of days to retain IM	30	30	N	N
display_mode	REG_DWORD	Control the way that Google Desktop is displayed: Sidebar, Deskbar, Floating Deskbar or none.	(none)	1	Y	Y
blacklist-pop	Key	List of email products that Google Desktop cannot access by means of the POP client.	""	gmail	Y	Y

The following registry keys are under Google\Google Desktop\Enterprise. None of these registry keys affect the user interface.

Name	Type	Description	Default Value	Example	User Option
disallow_gadgets	REG_DWORD	Disallows installation and use of all gadgets.	0	1	Y
disallow_only_non_builtin_gadgets	REG_DWORD	Disallows installation and use of non-built-in gadgets only.	1	1	N
gadget_whitelist	REG_SZ	Whitelist of gadgets that can be installed, superseding settings for disallow_gadgets and disallow_only_non_builtin_gadgets.		{Guid-Identifier-String}	N
install_confirmation_whitelist	REG_SZ	Whitelist of gadgets that can be installed without user confirmation.			N
autoupdate_host	REG_SZ	Hostname to query for autoupdate availability	desktop.google.com	""	N
GSAHosts	REG_SZ	List of GSA hostnames in company	""	search.corp.example.com	N
PolicyUnawareClientProhibitedFlag	REG_DWORD	Prevents Google Desktop 1.0 from installing/running	0	1	N
minimum_allowed_version	REG_SZ	Minimum version of Google Desktop that user can install and run	0.0.0.0	2.2005.0401.0600	N
maximum_allowed_version	REG_SZ	Maximum version of Google Desktop that user can install and run	9999.9999.9999.9999	5.9999.9999.9999	N
enterprise_tab_text	REG_SZ	Name to use for Google Search Appliance search tab	""	intranet	N
enterprise_tab_homepage	REG_SZ	URL of Google Search Appliance home page	""	http://search.intranet.example.com	N
enterprise_tab_homepage_query	REG_DWORD	Indicates whether search homepage URL supports "q=query" parameter	0	1	N
enterprise_tab_results	REG_SZ	URL for Google Search Appliance query results	""	http://search.intranet.example.com/search?q=[DISP_QUERY]	N
enterprise_tab_results_query	REG_DWORD	Indicates whether query results URL supports "q=query" parameter	0	1	N
alternate_user_data_dir	REG_SZ	String value of alternate user data directory parameter	""	c:\desktopdata	N
max_allowed_outlook_connection	REG_DWORD	Control maximum allowed connections for Outlook	400	400	N

disallow_ssd_service	REG_DWORD	Control sharing of web history and documents across computers	1	1	Y
max_exchange_indexing_rate	REG_DWORD	Control maximum number of emails indexed per minute	60	60	N

©2008 Google - [Privacy Policy](#) - [Terms and Conditions](#) - [Copyright Notices](#)