

Admin Guide

- [Overview](#)
- [Related Technologies](#)
- [Download Administrative Template](#)
- [Installing Google Desktop](#)
- [Configuration](#)
- [Use Group Policy](#)
- [Where Registry Keys Are Stored](#)
- [Policy Settings](#)
- [Preferences](#)
- [Google Enterprise Integration](#)
- [Updating Google Desktop](#)
- [Integrating Google Desktop and the Google Search Appliance or Google Mini](#)
- [Stylesheet Changes for Google Search Appliance Front Ends](#)
- [A Sample Integration of Google Desktop and Google Search Appliance](#)

Overview

[back to top](#)

Google Desktop, available on google.com, is installed and set up by end users. It searches a user's own computer, including files, email, viewed web pages, instant messages, images, music, video, and more. Google Desktop for Enterprise provides the same user functionality, plus indexing of Lotus Notes email, but is designed to work in an enterprise environment, distributable from a centralized corporate resource, and configured by a Windows administrator.

If the corporation also uses a Google Search Appliance or Google Mini for corporate intranet search, the administrator can configure Google Desktop for Enterprise to provide an integrated search experience, giving corporate users "one-stop searching" across all resources – their desktop with Google Desktop, the corporate intranet powered by Google Search Appliance or Google Mini, and the Internet with Google.com.

After configuration, search results for users in the enterprise will display relevant results from the user's computer, from Google.com, and from your intranet powered by the Google Search Appliance or Google Mini.

This guide contains information about setting up Google Desktop for the Enterprise and is for Windows domain administrators and administrators of the Google Search Appliance or Google Mini.

Related Technologies

[back to top](#)

Group Policy

Group Policy is an infrastructure technology that delivers and applies configurations or policy settings to targeted users and computers. [Microsoft Windows Group Policy](#) is one of these technologies.

Google Desktop for Enterprise is compatible with Windows Group Policy. Google provides a Group Policy Administrative Template, which allows enterprise administrators to edit and manage desktop-search-specific policies with Group Policy Management, Group Policy MMC SnapIn, or other Group Policy editor of choice. The resultant policies can then be applied to client machines through Active Directory, which results in registry modifications on the client machine. Google Desktop components use those registry settings.

Customers who do not use Active Directory and Group Policy for management can use their own administration mechanisms to modify the registry settings directly, through logon scripts or other mechanisms. See "Where Registry Keys are Stored" in this document for a registry settings table.

Administrative Template File

The downloadable Administrative Template file contains settings for Google Desktop and is described in detail in the document.

Google Search Appliance Stylesheet

Two new templates are added to the Google Search Appliance's XSLT Stylesheet for Google Desktop – the "desktop_tab" and the "desktop_results" template. See "Stylesheet Changes for Google Search Appliance -- Front Ends" in this document for more details.

Download Administrative Template

[back to top](#)

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

Installing Google Desktop

[back to top](#)

Google Desktop for the Enterprise is typically installed in one of three ways:

- directly by a user (requires administrator privileges on the machine)
- distributed by Group Policy Software Installation
- distributed by Systems Management Server (SMS).

Google Desktop for the Enterprise is intended for installation on multiple computers in an organization. It is not intended for installation by a single user on a single machine. A shortcut is placed on the desktops and in the Start menus for all users of the system. When another user runs Google Desktop from one of these shortcuts, it will be enabled for him or her, and run automatically whenever that user logs in to the machine.

User Installation

If users have administrator access to their local machines, they may install Google Desktop directly on their own by copying or downloading the MSI installation package to their machine and double-clicking on it.

Group Policy Software Installation

When using Group Policy Software Installation, Google Desktop may be either published (made available for installation) or assigned (forced install).

Published Installs

If the administrator chooses a published installation, Google Desktop will appear in the Windows Control Panel, in the "Add new programs" section under "Add/Remove Programs." Publishing the packages authorizes the installation to run with administrator privileges on the machine, even if the user installing it is not a local administrator. Publishing is done by user; software packages may not be published to machines. Users will be able to uninstall Google Desktop from their machines by going to the Control Panel's "Add/Remove Programs," selecting "Google Desktop" from the list of installed programs, and clicking on the "Remove" button, even if they are not local administrators.

Since published installs are performed interactively by the user, Google Desktop will be automatically enabled for the user that performed the installation. Other users of the machine can enable and run Google Desktop from the desktop or Start menu shortcuts.

Assigned Installs

If the administrator chooses an assigned installation, Google Desktop will automatically and silently install on the machine. If assigned by user, it will install the next time the user logs in. If assigned by machine, it will install the next time the machine is rebooted. Since assigned installs happen outside of a user session, they are performed silently and without user interaction. Consequently, Google Desktop will not be automatically enabled for any users. Users can enable and run Google Desktop from the desktop or Start menu shortcuts.

SMS Installation

SMS provides a greater variety of installation options, but basically divides into per-user vs. per-machine installs, as well as attended vs. unattended installs.

Unattended installs should only be performed when no user is logged in to the machine. Performing an unattended install with a user logged in may result in an incomplete installation that will require a local administrator to complete.

Regardless of SMS settings, Google Desktop will always be installed and available for all users on the machine. However, we recommend that SMS be configured to do per-machine (ALLUSERS=1) installations only.

Attended (interactive) installations will result in Google Desktop being automatically enabled for the user that performs the installation. Unattended (silent) installs will not be enabled until the user runs Google Desktop from the desktop or Start menu shortcuts.

Note: Never perform a silent installation when a user is logged in. If certain applications (such as Internet Explorer, Office applications, etc.) are running, the Google Desktop will not be able to fully install.

Multiple Users on a Single Machine

If a user later wishes to disable Google Desktop just for themselves, but leave Google Desktop installed for other users on the machine, they may do so by clicking the system tray icon, selecting "Exit" and then unchecking the "Start Google Desktop when my computer starts" checkbox.

Configuration

[back to top](#)

Here is information about distributing, deploying, and configuring Google Desktop and providing integration with the Google Search Appliance.

Use Group Policy

[back to top](#)

Google Desktop for Enterprise adds support for Windows Group Policy that allows a domain administrator to configure certain settings for users and computers on the domain. Active Directory allows Group Policy Objects to be applied to various subsets of users and computers. A Group Policy Object (GPO) can be applied to either the domain as a whole, or an Organizational Unit within that domain. Group Policy Objects can be edited either using the Active Directory management console or the Group Policy Management Console. The Group Policy Object editor allows you to edit policies for both computers and users.

Important: When a Group Policy Object is applied to **users**, only settings in the **user** part of the policy object are applied, and when a Group Policy Object is applied to **computers**, only settings in the **computer** part of the policy object are applied. (A GPO that has only user settings does nothing if applied only to computers.)

Where Registry Keys Are Stored

[back to top](#)

Certain areas of the registry are reserved for group policy settings. These areas are protected with Access Control Lists that prevent tampering by non-administrative users.

The location for user policies is:
HKCU\Software\Policies

The location for machine policies is:
HKLM\Software\Policies

Google will add a subkey under each location named "Google\Google Desktop," where policy settings will reside. The subkey is added to the policy section only when policy is applied, so if no policies are applied, the subkey will not be present. Whenever possible, all keys and values will parallel the corresponding user preferences section of the registry.

Registry keys under Google\Google Desktop\Preferences

This table lists all registry keys that will be controlled by group policy. The last four table columns are:

- Default Key - the default registry key setting
- User Pref - whether the registry change affects the user preference setting
- User UI - whether the registry change affects the user interface
- Group Policy Setting - whether a group policy setting exists for this key

Name	Type	Description	Example	Default Value	Def Key	User Pref	User UI	Group Policy Setting
file_extensions_to_skip	REG_SZ	Comma-delimited extension list.	",tmp,temp,log"	tmp, temp, log, pst, dat, 000, pf, xml, obj ,pdb	N	Y	N	Y
onebox_mode	REG_DWORD	Controls insertion of GDS OneBox in google.com	1	1	N	Y	Y	Y
blacklist-1	REG_SZ	String values of Schema IDs	"2"	""	N	Y	P	Y
blacklist-2	REG_SZ	String values of File Extensions	"XLS"	""	N	Y	P	Y
blacklist-3	REG_SZ	String values of protocol identifiers	"HTTPS"	"HTTPS"	N	Y	P	Y
blacklist-6	REG_SZ	String values of URI substrings (contains)	"http://www/hr/"	""	N	Y	Y	Y
blacklist-12	REG_SZ	String values of Component IDs	"53", "{Guid-Identifier-String}"	""	N	Y	P	Y
blacklist-13	REG_SZ	String values of security features	"SECUREOFFICE"	""	N	Y	Y	Y
error_report_on	REG_DWORD	Controls reporting of crash + usage data	1	1	N	Y	Y	Y
hyper_off	REG_DWORD	Controls Quick Find	1	1	N	Y	Y	Y
policy_search_location_whitelist	REG_SZ	String values of specific folders to index	c:\userdata	""	N	N	Y	Y
user_search_locations	REG_DWORD	Controls user ability to add search locations	1	1	N	Y	Y	Y
email_days_to_retain	REG_DWORD	Control number of days to retain emails	30	30	N	N	N	Y
webpage_days_to_retain	REG_DWORD	Control number of days to retain webpages	30	30	N	N	N	Y
file_days_to_retain	REG_DWORD	Control number of days to retain files	30	30	N	N	N	Y
im_days_to_retain	REG_DWORD	Control number of days to retain IM	30	30	N	N	N	Y

Registry keys under Google\Google Desktop\Enterprise

This table lists all registry keys that will be controlled by group policy. The last four table columns are:

- Default Key - the default registry key setting
- User Pref - whether the registry change affects the user preference setting
- User UI - whether the registry change affects the user interface
- Group Policy Setting - whether a group policy setting exists for this key

Name	Type	Description	Example	Default Value	Def Key	User Pref	User UI	Group Policy Setting
disallow_plugins	REG_DWORD	Disallows installation of 3rd party plugins	1	0	N	Y	N	Y
plugin_whitelist	REG_SZ	Whitelist of plugins that may be installed, despite disallow_plugin_install setting	"{Guid-Identifier-String}"		N	N	N	Y
autoupdate_host	REG_SZ	Hostname to query for autoupdate availability	"www.corp.google.com"	"desktop.google.com"	N	N	N	Y
GSAHosts	REG_SZ	List of GSA hostnames in company	"search.corp.google.com"	""	N	N	N	Y
PolicyUnawareClientProhibitedFlag	REG_DWORD	Prevents GDS 1.0 from installing/running	1	0	N	N	N	Y
minimum_allowed_version	REG_SZ	Minimum version of GDS allowed to install/run	2.2005.0401.0600	0.0.0.0	N	N	N	Y
maximum_allowed_version	REG_SZ	Maximum version of GDS allowed to install/run	2.9999.9999.9999	9999.9999.9999.9999	N	N	N	Y
enterprise_tab_text	REG_SZ	Name to use for Google Search Appliance search tab	"intranet"	""	N	N	N	Y
enterprise_tab_homepage	REG_SZ	URL of Google Search Appliance homepage	<http://search.intranet.company.com>	""	N	N	N	Y
enterprise_tab_homepage_query	REG_DWORD	Indicates whether search homepage URL supports "q=query" parameter	1	0	N	N	N	Y
enterprise_tab_results	REG_SZ	URL for Google Search Appliance query results	http://search.intranet.company.com/search?q=[DISP_QUERY]	""	N	N	N	Y
enterprise_tab_results_query	REG_DWORD	Indicates whether query results URL supports "q=query" parameter	1	0	N	N	N	Y
alternate_user_data_dir	REG_SZ	String value of alternate user data directory parameter	c:\desktopdata	""	N	N	N	Y
max_allowed_outlook_connection	REG_DWORD	Control maximum allowed outlook connections	400	400	N	N	N	Y
disallow_ssd_service	REG_DWORD	Control sharing of web history and documents across computers	1	1	N	Y	N	Y
max_exchange_indexed_rate	REG_DWORD	Control maximum number of emails that are indexed per minute	60	60	N	N	N	Y

Prohibit Installation of Policy-Unaware Versions

This policy affects only Google Desktop 1.0. When enabled, this policy prevents new installations of Google Desktop 1.0. Instead, users will receive an error that installation of Google Desktop has been prohibited by their administrator. If the user already has Google Desktop installed, they will receive the same error when they try to run it.

If this policy is not configured or disabled, the policy has no effect.

Preferences**Do not send Advanced Features data**

Enabling this policy prevents Google Desktop from sending data required to enable Advanced Features, including anonymous usage data and crash reports, to Google. If this policy is disabled or not configured, the user can choose whether to enable Advanced Features.

Turn off Google Web Search Integration

Enabling this policy prevents Google Desktop from displaying Desktop search results in queries to google.com. If this policy is disabled or not configured, the user can choose whether to include Desktop search results in queries to google.com or Google Search Appliance or Google Mini.

Note: No part of this feature / policy is associated with transmitting any secure, private, or local data to Google. Disabling this functionality limits the user experience and should be avoided.

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. If this policy is disabled or not configured, the user can choose whether to enable it.

Indexing and Capture Control

Each one of the following policies may be Enabled, Disabled, or Not Configured. If a policy is Enabled, the corresponding capture component or feature is disabled and the user is prevented from changing the setting.

If an item is Disabled or Not Configured, the user preference applies, and the user may change the setting.

Note: This may seem counterintuitive, but it is a common convention for administrative templates.

Administrators can apply policy to individual users and/or machines, so all of the policy settings may appear in either the user or the machine section. If policy settings are present in both the user and machine sections of policy, the following general set of rules should be applied. Specific configuration items/policies may have custom precedence rules.

1. For simple enable/disable feature policies, the machine policy (if present) takes precedence over user policy.
2. For blacklists and similar text fields, the union of the policies is used.

Prevent indexing of Email

This policy controls indexing of Email messages. If this policy is enabled, Google Desktop will not index and store Email messages. If this policy is not configured or disabled, the user may choose whether or not to allow indexing of Email messages.

Prevent indexing of web pages

This policy controls indexing of web browser history. If this policy is enabled, Google Desktop will not index web pages that the user views, either via HTTP or HTTPS. If this policy is not configured or is disabled, the user may choose whether to allow indexing of web pages.

Prevent indexing of text files

This policy controls indexing of text files. If this policy is enabled, Google Desktop will not index text files. If this policy is not configured or is disabled, the user may choose whether to allow indexing of text files.

Prevent indexing of media files

This policy controls indexing of media files. If this policy is enabled, Google Desktop will not index media files. If this policy is not configured or is disabled, the user may choose whether to allow indexing of media files.

Prevent indexing of contacts

This policy controls indexing of MS Outlook's contact list. If this policy is enabled, Google Desktop will not index the contact list. If this policy is not configured or is disabled, the user may choose whether to allow indexing of contacts.

Prevent indexing of calendar entries

This policy controls indexing of MS Outlook's calendar entries. If this policy is enabled, Google Desktop will not index calendar entries. If this policy is not configured or is disabled, the user may choose whether to allow indexing of calendar entries.

Prevent indexing of tasks

This policy controls indexing of MS Outlook's tasks. If this policy is enabled, Google Desktop will not index tasks. If this policy is not configured or is disabled, the user may choose whether to allow indexing of tasks.

Prevent indexing of notes

This policy controls indexing of MS Outlook's notes. If this policy is enabled, Google Desktop will not index notes. If this policy is not configured or is disabled, the user may choose whether to allow indexing of notes.

Prevent indexing of journal entries

This policy controls indexing of MS Outlook's journal entries. If this policy is enabled, Google Desktop will not index journal entries. If this policy is not configured or is disabled, the user may choose whether to allow indexing of journal entries.

Prevent indexing of Word documents

This policy controls indexing of MS Word documents. If this policy is enabled, Google Desktop will not index Word documents. If this policy is not configured or is disabled, the user may choose whether to allow indexing of Word documents.

Prevent indexing of Excel documents

This policy controls indexing of MS Excel documents. If this policy is enabled, Google Desktop will not index Excel documents. If this policy is not configured or is disabled, the user may choose whether to allow indexing of Excel documents.

Prevent indexing of PowerPoint documents

This policy controls indexing of MS PowerPoint documents. If this policy is enabled, Google Desktop will not index PowerPoint documents. If this policy is not configured or is disabled, the user may choose whether to allow indexing of PowerPoint documents.

Prevent indexing of PDF documents

This policy controls indexing of PDF documents. If this policy is enabled, Google Desktop will not index PDF documents. If this policy is not configured or is disabled, the user may choose whether to allow indexing of PDF documents.

Prevent indexing of secure web pages

This policy controls indexing of secure web pages. If this policy is enabled, Google Desktop will not index web pages that the user views via HTTPS. If this policy is not configured or is disabled, the user may choose whether to allow indexing of secure web pages.

Prevent indexing of specific web sites and folders

This policy lets you prevent Google Desktop from indexing specific websites or folders by containing a list of URI substrings to exclude from indexing. If an item's URL or path name contains any of these specified strings, it will not be indexed. If this policy is not configured or is disabled, the administrator can prevent any item whose URI matches any of the specified strings from being indexed. For example, adding "http://images.company.com" would prevent anything in the company's images web server from being indexed. Adding "C:\SensitiveCompanyData" would prevent indexing of anything in that folder on the user's local machine.

The User setting for this on the preference page is as follows:

Don't search these items or files with the following paths. Put each entry on a separate line.

Examples:

http://www.domain.com/

c:\Documents and Settings\username\Private Files

This policy has no effect when disabled or not configured.

Prevent indexing of IM chats

This policy disables indexing of Instant Messaging chat programs. If this policy is disabled or not configured, the user can choose whether to index IM chat conversations.

Prevent indexing of password-protected Office documents (Word, Excel)

This policy controls indexing of password-protected Office documents. If this policy is enabled, Google Desktop will not index password-protected Office documents. If this policy is not configured or is disabled, the user may choose whether to allow indexing of password-protected Office documents.

Prevent indexing of specific extensions

This policy blocks indexing of files with any specified extensions provided. Enter a list of file extensions, separated by commas, to exclude from indexing. This policy has no effect when disabled or not configured.

Do not send anonymous usage data

Enabling this policy prevents Google Desktop from sending error-reporting anonymous usage data to Google. If this policy is disabled or is not configured, the user can choose whether or not to allow sending of anonymous usage data.

Turn off Google Web Search Integration

Enabling this policy prevents Google Desktop from displaying Google Desktop results in queries to google.com and, if configured, your intranet search powered by the Google Search Appliance or Google Mini. If this policy is disabled or is not configured, the user can choose whether or not to include Google Desktop results in queries to google.com and your intranet.

Encrypt Index Data

Enabling this policy causes Google Desktop to turn on Windows file encryption for the folder containing the Google Desktop index and related user data the next time it is run. Google Desktop does not provide a user-controlled setting for encrypting the index; this setting is exposed only via Group Policy. Note that Windows EFS is only available on NTFS volumes. If the user's data is stored on a FAT volume, this policy will have no effect. This policy has no effect when disabled or not configured.

Email Retention

This policy allows you to configure Google Desktop to retain only emails that are less than the specified number of days old in the index. This policy has no effect when disabled or not configured.

Webpage Retention

This policy allows you to configure Google Desktop to retain only webpages that are less than the specified number of days old in the index. This policy has no effect when disabled or not configured.

File Retention

This policy allows you to configure Google Desktop to retain only files that are less than the specified number of days old in the index. This policy has no effect when disabled or not configured.

IM Retention

This policy allows you to configure Google Desktop to retain only instant messages that are less than the specified number of days old in the index. This policy has no effect when disabled or not configured.

Google Enterprise Integration

[back to top](#)

In the Administrative Template are settings to use when you integrate Google Desktop with the Google Search Appliance or Google Mini. These features are specific to Enterprise installations of Google Desktop.

Block AutoUpdate

Enabling this policy prevents Google Desktop from automatically checking for and installing updates from 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. You should check <http://desktop.google.com/enterprise/> for updates.

If this policy is disabled or not configured, Google Desktop will periodically check for updates from desktop.google.com.

Enterprise Search Tab

This policy allows you to add a search tab for your Google Search Appliance to Google Desktop and google.com web pages. You must provide the name of the tab, such as "Intranet", as well as URLs for the search homepage and for retrieving search results. Use [DISP_QUERY] in place of the query term for the search results URL.

Google Desktop will insert the tab on your corporate search page only when the page comes from a server that has been specified in the "Google Search Appliances" group policy.

Google Search Appliances

The Google Search Appliances setting controls integration with a Google Search Appliance, if present. Here is where you specify the fully qualified domain name of the Google Search Appliance(s) in your corporation. When properly configured, Google Desktop will insert Google Desktop results into the results of queries on the Google Search Appliance.

Prohibit Policy-Unaware Versions

This policy prohibits installation and execution of versions of Google Desktop that are unaware of group policy (version 1.0). Enabling this policy will prevent users from installing or running version 1.0 of Google Desktop. This policy has no effect when disabled or not configured.

Minimum Allowed Version

The Minimum Allowed Version setting prohibits installation or use of Google Desktop unless it is at least the indicated version. This policy allows you to prevent installation and/or execution of older versions of Google Desktop by specifying the minimum version you wish to allow. When enabling this policy, you should also enable the "Prohibit Policy-Unaware Versions" policy to block versions of Google Desktop that did not support group policy. This policy has no effect when disabled or not configured.

Google Desktop versions are expressed with numbers corresponding to the build date such as 2.2005.0401.0600. To see the version number, click on the About link on the Google Desktop page for the given installation.

Maximum Allowed Version

The Minimum Allowed Version setting prohibits installation and use of Google Desktop that is greater than the indicated version. This policy allows you to prevent installation and/or execution of newer versions of Google Desktop by specifying the maximum version you wish to allow. This policy has no effect when disabled or not configured.

Disallow Plug-ins

The Disallow Plug-ins setting prohibits installation and use of third-party plug-ins. Enabling this policy will prevent installation of Google Desktop plugins. You can use this policy in combination with the "Plugin whitelist" policy to allow only specific plug-ins to be installed. If this policy is disabled or not configured, users may install any plug-in.

Plug-in Whitelist

The Plug-in Whitelist allows specific third-party plug-ins to be installed and used, overriding the general policy that disallows plug-in installations. A whitelist is necessary only if you have enabled the Disallow Plug-ins policy. This policy can be used in combination with the "Disallow Plugins" policy to allow only a specific set of Google Desktop plug-ins to be installed. When using this policy, you must enable the "Disallow Plugins" policy. For each plug-in you wish to allow, add the CLSID or PROGID of the plug-in. This policy has no effect when disabled or not configured.

Alternate User Data Directory

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 will be appended at the end of the path. This policy has no effect when disabled or not configured.

Note: Storing user data on network volumes could greatly impact performance and is not recommended.

Reporting server

This policy allows you control how Google Desktop sends data required for Advanced Features. If a user has selected to allow sending of Advanced Features data, Google Desktop will send specially-formed HTTP requests to google.com containing this data. This policy allows you to tell Google Desktop to send those requests to your own webserver for collection and review. You can then use the provided tools to filter Google Desktop reporting data from your webserver logs and send the results to Google. Note that News personalization will not work for your users if you enable this option.

Maximum allowed Outlook connections

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.

The default value is 400. Because users rarely have as many as 400 email folders, Google Desktop rarely reaches the limit.

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.

This policy has no effect when disabled or not configured.

Disallow sharing of web history and documents across computers

Enabling this policy will prevent Google Desktop from sharing the user's web history and document contents across the user's different Google Desktop installations. This policy has no effect when disabled or not configured.

Maximum allowed exchange indexed rate

This policy allows you to specify the maximum number of emails that are indexed per minute. This policy has no effect when disabled or not configured.

Updating Google Desktop

[back to top](#)

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

Note: AutoUpdate will not complete successfully for users who do not have local administrative access. If users within the corporation do not have local administrative privileges to their machines, an alternate update strategy needs to be enabled using other software distribution mechanisms.

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

Integrating Google Desktop and the Google Search Appliance or Google Mini

[back to top](#)

There are two basic steps for providing enterprise users with an integrated search experience across their desktop, the intranet, and the Internet. Integrating Google Desktop for Enterprise will include a link to your intranet search, powered by a Google Search Appliance or Google Mini, on the users' Google.com homepage and on your intranet search page. This will also allow a user to see desktop search results integrated into your intranet search results on one search page. To provide this functionality to your users, you must do the following.

Configuring Google Desktop for Integration

To enable this user functionality, activate the Web Search Integration feature (no policy applied) for the user. Then, follow the instructions in this guide to enable the Enterprise Search Tab policy and Google Search Appliances policy.

Google Desktop and Google.com web pages use JavaScript to rewrite search tab URLs -- to reflect edits to the search query term -- by adding or modifying the URL with an HTTP GET parameter, "q=query_term." When a user enters a query term with Web selected, then clicks Desktop to go to the Google Desktop homepage, the query term is automatically set. Similarly, on a search results page, a user can modify the query term, click on the Desktop tab, and get Google Desktop results for the modified query term. If your search homepage or results page do not support specifying the query term this way (or use a parameter other than "q" for the query term), do not check the boxes for the homepage URL and/or results URL.

Example

Here is a sample integration of XYZcompany.com, Google Desktop Search, and Google Search Appliance. The example assumes you have Group Policy implemented.

1. Go to <http://desktop.google.com/enterprise> and download the Administrative Template and the installer to your domain controller.
2. Enable Enterprise Search Tab policy and use the following settings:
 - o Tab Name: XYZ Intranet
 - o Homepage URL: <http://search.corp.XYZcompany.com/>
 - o Do not check the "homepage supports &q=" box.
 - o Query Results URL: [http://search.corp.xyz.com/search?site=internal&client=internal&output=xml_no_dtd&proxystylesheet=internal&q=\[DISP_QUERY\]](http://search.corp.xyz.com/search?site=internal&client=internal&output=xml_no_dtd&proxystylesheet=internal&q=[DISP_QUERY])
 - o **Do** check the "search results page supports &q=" box.
3. Enable Google Search Appliances policy. In this example, the Google Search Appliance has a front end that is on another server, so we add the following two entries:
 - o search
 - o search.corp.XYZcompany.com

Stylesheet Changes for Google Search Appliance Front Ends

[back to top](#)

The XSLT Stylesheet contains two additional templates to use with Google Desktop. The "desktop_tab" template should be called in the page header. The "desktop_results" template should be called from both the results page template and the "no results" template. The additions to the stylesheet appear like this:

```
<xsl:template name="desktop_tab">
<xsl:if test="CUSTOM/HOME">
<xsl:comment>trh2</xsl:comment>
</xsl:if>
<xsl:if test="Q">
<xsl:comment>trl2</xsl:comment>
</xsl:if>
</xsl:template>
```

```
<xsl:template name="desktop_results">
<xsl:comment>tro2</xsl:comment>
</xsl:template>
```

A Sample Integration of Google Desktop and Google Search Appliance

[back to top](#)

Overview

Here is an overview of how to integrate Google Desktop for Enterprise (GDfE) on a single machine with a Google Search Appliance (GSA).

This document only covers integrating a single GDfE installation (on one computer) with a Google Search Appliance. If you need to perform this integration on multiple machines, you can use the Windows Group Policy framework to do so. The Group Policy framework is a very powerful system for distributing software and configuration information to multiple Windows computers, but if used improperly it can cause problems. If you are not familiar with the Group Policy framework, please consult a Windows administrator before attempting to do this. Google can not provide support for Group Policy issues.

This integration document was developed during August 2005 using GDfE v1.0 release and GSA software v4.4.18. Also, the examples use gsademo1.google.com as the Google Search Appliance, which is a demonstration machine.

- [GDfE Configuration - Personal Setup](#)
- [GSA Configuration](#)

Google Desktop for Enterprise Configuration - Personal Setup

These instructions will walk you through the process of configuring Google Desktop for Enterprise on an individual machine to talk to your Google Search Appliance. Once this configuration is completed, you should see an appliance search tab on www.google.com and on your desktop search results. To allow Google Desktop to insert results and tabs in your Google Search Appliance results, you will need to complete the [GSA Configuration](#).

Note: Configuration of Google Desktop for Enterprise will require Administrator access to the machine that you are installing on.

1. Install Google Desktop for Enterprise

- Download Google Desktop for Enterprise from <http://desktop.google.com>
- **Note:** The standard desktop version will not support all the options necessary for integration. The link to the Enterprise version is located on the bottom of the page.
- Uncompress the ZIP file containing the GDfE install.
- Run the extracted file: `GoogleDesktopSearchSetup.msi`

2. Install the template that will allow an Administrator to edit the options for GDfE

- From the Run command in the Start menu, enter this command: `gpedit.msc`
- In the left-hand pane of the management console, right-click the Administrative Templates item under User Configuration and choose the [Add/Remove Templates](#) option.
- In the subsequent dialog box, click the `Add...` button.
- Select the `GoogleDesktopSearch.adm` file that was extracted from the GDfE download.
- Close the Add/Remove Templates dialog box.

3. Configure the GDfE policies to allow it to insert desktop results into your GSA results

- In the left-hand pane of the group policy editor you opened in the step above, select [User Configuration -> Administrative Templates -> Google -> Google Desktop Search -> Enterprise Integration](#)
- In the right-hand pane, double-click on the [Google Search Appliances](#) item.
- In the Properties dialog that appears,
 - Select the [Enabled](#) radio button option
 - Click the [Show...](#) button.
- In the Show Contents dialog box, click the `Add...` button.
- In the Add Item dialog box, enter the [host name of your Google Search Appliance](#) (Ex: gsademo1.google.com)
- Click `OK` 3 times to accept all changes.

4. Configure the GDfE policies to add an appliance tab to primary Google and desktop Google search pages

- In the left-hand pane of the group policy editor you opened in the step above, select [User Configuration -> Administrative Templates -> Google -> Google Desktop Search -> Enterprise Integration](#)
- In the right-hand pane, double-click on the [Enterprise Search Tab](#) item.
- In the Properties dialog that appears,
 - Select the [Enabled](#) radio button option.
 - Enter the [Tab name](#) that you would like to use for your Enterprise search tab. (Ex: Intranet)
 - Enter the [Search homepage URL](#) for your Google Search Appliance.
Ex: `http://gsademo1.google.com/search?site=default_collection&client=integrated_frontend&proxystylesheet=integrated_frontend&output=xml_no_dtd&proxycustom=<HOME/>`
 - Deselect the [Check if search homepage...](#) option
 - Enter the Search results URL for your Google Search Appliance
Ex: `http://gsademo1.google.com/search?q=[DISP_QUERY]&site=default_collection&client=integrated_frontend&proxystylesheet=integrated_frontend&output=xml_no_dtd`
 - Select the [Check if search results...](#) option
- Click `OK` to accept all changes.

5. Close the group policy editor.

GSA Configuration

[Back to top](#)

These instructions will walk you through the process of configuring the Google Search Appliance to work with configured Google Desktop for Enterprise installations. Once both configurations are completed, you should see desktop search results appear just above your appliance search results and all the Google search tabs will be visible on your appliance search pages. If you have not completed the [GDfE Configuration - Personal Setup](#), then you will not see any visible changes after following these steps.

Note: The configuration of the Google Search Appliance described below requires XSLT coding that is not supported by the Google Support team. If you are not familiar with XSLT, please consult an XSLT programmer before attempting these steps.

Modifying XSLT Code

This section describes best practices for editing XSLT code when working with the Google Search Appliance. The following section will describe the specific XSLT code changes that need to be made to support GDfE integration.

1. In the GSA admin console, select the front end that you would like to modify.
2. On the Format tab of the front end, select the **Edit underlying XSLT code** option, if you have not done so previously.
3. Copy the content of the Raw XSLT Code field to your favorite text editor
 - o **Note:** Since the GSA admin console times out after 15 minutes, it's good to work on any code changes in a separate text editor.
4. Save 2 copies of the code you just copied to disk: One as a backup, and the other as a working version.
 - o **Note:** It's always good practice to save off a backup version, so that you can start from the beginning in case something goes wrong.
5. When you want to load changes into the appliance, copy the entire style sheet from your text editor and replace all the text in the Raw XSLT Code field.
 - o **Note:** It's easier to copy the whole style sheet, then to scroll around and copy sections.
 - o **Note:** You may have to log into the GSA admin console again, if more than 15 minutes has transpired.
 - o **Note:** Don't forget to hit the Save XSLT Code button and wait for the screen to refresh.
6. Try out your XSLT changes to make sure that they accomplish what you expect
 - o **Note:** The GSA caches XSLT code for performance reasons when satisfying search requests. To force a reload, you must submit the `&proxyreload=1` parameter with the search request URL sent to the GSA.
 - o **Note:** You can quickly get the search request URL by using the Test Center, and viewing the Properties of the middle frame window.

XSLT Changes to Support Google Desktop for Enterprise Integration

This section provides the details of how to modify the XSLT code to add the necessary tags to the HTML output for Google Desktop for Enterprise integration. These changes are just one example of how the tags can be added, and are based on the default style sheet that ships with the GSA. You may wish to begin with the default style sheet and these changes to understand the code before working on your own customized version.

Template Change (result_page_header)

1. Remove TD cell (and contents) that contain links to Advanced Search, Alerts and Help. This will make space for the tabbed search options.
2. Move TR start and end tags from the first row into the `xsl:if` statement containing the logo. This removes an extra row in the header if the logo is not used.

Template Change (search_box)

1. Right after the FORM start tag, add this code. This adds the tabs for the different search options of the search box.

```
<table cellpadding="4" cellspacing="0">
  <tr>
    <xsl:call-template name="desktop_tab"/>
  </tr>
</table>
```

2. Add a cell right after the cell containing the search box and button. This adds smaller version of Advanced Search, Alerts and Help links to the right of the search box.

```
<td nowrap="1">
  <font size="-2">
    <xsl:if test="$show_result_page_adv_link != '0'">
      <xsl:call-template name="nbsp"/>
      <xsl:call-template name="nbsp"/>
      <a href="{ $adv_search_url }">
        <xsl:value-of select="$adv_search_anchor_text"/>
      </a>
      <br/>
    </xsl:if>
    <xsl:if test="$show_alerts_link != '0'">
      <xsl:call-template name="nbsp"/>
      <xsl:call-template name="nbsp"/>
      <a href="{ $alerts_url }">
        <xsl:value-of select="$alerts_anchor_text"/>
      </a>
      <br/>
    </xsl:if>
    <xsl:if test="$show_result_page_help_link != '0'">
      <xsl:call-template name="nbsp"/>
      <xsl:call-template name="nbsp"/>
      <a href="{ $help_url }">
        <xsl:value-of select="$search_help_anchor_text"/>
      </a>
    </xsl:if>
  <br/>
</font>
</td>
```

Template Change (results)

1. Add `xsl:if` statement around top navigation and sorting options table. It will improve the spacing of results if these options are not used (recommended with desktop results inserted).

```
<xsl:if test="($show_top_navigation != '0') or ($show_sort_by != '0')">
...
</xsl:if>
```

2. Add this line between the synonym handling and the results detail output. This call defines where the desktop search results will be inserted in the appliance search results page.

```
<xsl:call-template name="desktop_results"/>
```

Template Change (no_RES)

1. Add this as the first line of code in this rule, right below the `xsl:param` tag. This call defines where the desktop search results will be inserted into the appliance empty results page.

```
<xsl:call-template name="desktop_results"/>
```

Template Change (style)

1. Replace style commands for `q` class using the following code. This allows the tabs to show underlines in the appliance search results, just like `google.com` and the desktop results.

```
.q a:visited, .q a:link, .q a:active, .q {color:#0000cc;}
```

Template Additions (desktop_tab and desktop_results)

1. Add the following templates right before the final template (which swallows tags not covered by previous templates). These templates define the tabs that will appear at the top of the appliance search results page, as well as inserting the tags that the Google Desktop application is looking for.

```
<xsl:template name="desktop_tab">
<!-- *** Show the Google tabs *** -->
<font size="-1">
<a class="q" onClick="return window.qs?qd(this):1" href="http://www.google.com/search?q={$qval}">Web</a>
</font>
<xsl:call-template name="nbsp4"/>

<font size="-1">
<a class="q" onClick="return window.qs?qd(this):1" href="http://images.google.com/images?q=
{$qval}">Images</a>
</font>
<xsl:call-template name="nbsp4"/>

<font size="-1">
<a class="q" onClick="return window.qs?qd(this):1" href="http://groups-beta.google.com/groups?q=
{$qval}">Groups</a>
</font>
<xsl:call-template name="nbsp4"/>

<font size="-1">
<a class="q" onClick="return window.qs?qd(this):1" href="http://news.google.com/news?q={$qval}">News</a>
</font>
<xsl:call-template name="nbsp4"/>

<font size="-1">
<a class="q" onClick="return window.qs?qd(this):1" href="http://froogle.google.com/froogle?q=
{$qval}">Froogle</a>
</font>
<xsl:call-template name="nbsp4"/>

<font size="-1">
<a class="q" onClick="return window.qs?qd(this):1" href="http://local.google.com/local?q=
{$qval}">Groups</a>
</font>
<xsl:call-template name="nbsp4"/>

<!-- *** Show the desktop and web tabs *** -->
<xsl:if test="CUSTOM/HOME">
<xsl:comment>trh2</xsl:comment>
</xsl:if>
<xsl:if test="Q">
<xsl:comment>trl2</xsl:comment>
</xsl:if>
```

```
<!-- *** Show the appliance tab *** -->
<font size="-1"><b>Appliance</b></font>

</xsl:template>

<xsl:template name="desktop_results">
<xsl:comment>tro2</xsl:comment>
</xsl:template>
```