
How to Configure Google Directory Services

<https://campus.barracuda.com/doc/68354897/>

This solution applies to the Barracuda Web Security Gateway 410 and higher running firmware version 12.x and higher.

When to use Google Directory Services

For all Chromebook deployments, when using the Barracuda Chromebook Security Extension, configure Google Directory Services as the authentication service the Barracuda Web Security Gateway will use to apply policies to Chromebook users and groups. Make sure to configure the Chromebook extension for your users on the **ADVANCED > Remote Filtering** page. See [How to Get and Configure the Barracuda Chromebook Security Extension](#) for details on configuration.

Requirements for using a Google Directory Services

Before you integrate with Google Directory Services, do the following:

1. Make sure you or your organization has a Google account with *read* access to Google Directory Services.
2. Edit the **hosts** file on the machine you use to log into and configure the Barracuda Web Security Gateway:
 - For Windows: Open a text editor that does not add extra characters and edit the **hosts** file, which is located in **C:\Windows\System32\drivers\etc**
 - For Unix/Linux/MacOS : Edit the **hosts** file, which is located in **/etc**

In the **hosts** file, add a line with the IP address of the Barracuda Web Security Gateway, followed by one space, and then the URL `mywsg.barracuda.com`.

For example: **10.1.1.1 mywsg.barracuda.com**

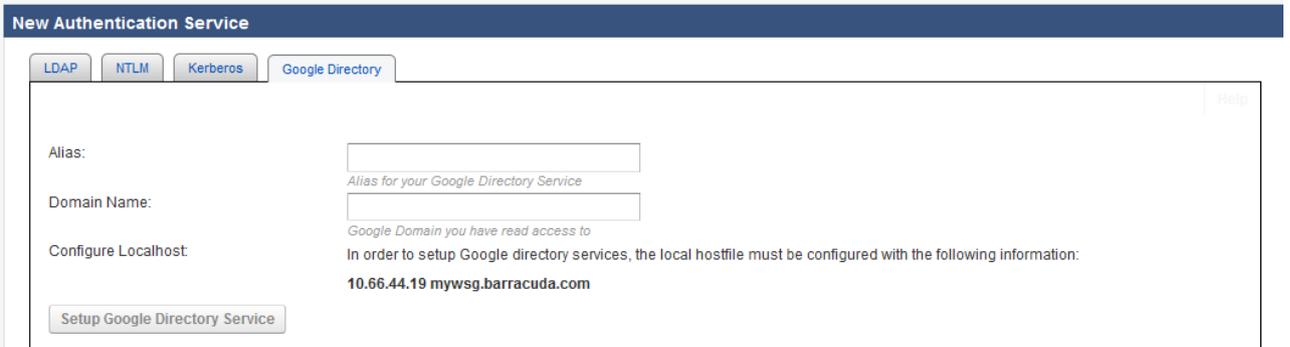
3. Save the **hosts** file.

Either before or after setting up Google Directory Services, you must configure the Barracuda Chromebook Security Extension as mentioned above.

Configure Google Directory Services on the Barracuda Web Security Gateway

1. Log into the Barracuda Web Security Gateway web interface as *admin*.

2. Go to the **USERS/GROUPS > Authentication** page. Follow instructions to configure an Alias by which to refer to the GDS authentication service and your Google domain (you must have read access to GDS for this domain). You will use the alias to select all Chromebook users when creating and assigning policies on the Barracuda Web Security Gateway.



The screenshot shows the 'New Authentication Service' configuration page with the 'Google Directory' tab selected. It includes input fields for 'Alias', 'Domain Name', and 'Configure Localhost'. A 'Setup Google Directory Service' button is visible at the bottom.

New Authentication Service

LDAP | NTLM | Kerberos | Google Directory

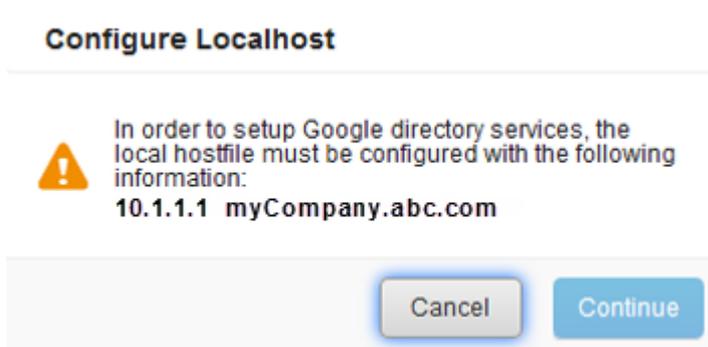
Alias:

Domain Name:

Configure Localhost:

Setup Google Directory Service

3. Click **Setup Google Directory Service**. In the **Configure Localhost** popup, assuming you have already edited your **hosts** file as described above, click **Continue**.



The screenshot shows the 'Configure Localhost' popup dialog. It contains a warning icon and text indicating that the local hostfile must be configured with specific information. The information provided is '10.1.1.1 myCompany.abc.com'. There are 'Cancel' and 'Continue' buttons at the bottom.

Configure Localhost

 In order to setup Google directory services, the local hostfile must be configured with the following information:
10.1.1.1 myCompany.abc.com

Cancel **Continue**

4. You are redirected to a Google page in your browser, prompting you to select and log into your Google account.
5. You are then prompted by Google to allow the Barracuda Web Security Gateway permissions to access users and groups of users on your Google domain. Click **Allow**.

Web Security Gateway would like to:

 View users on your domain 

 View groups on your domain 

 View organization units on your domain 

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other [Account Permissions](#) at any time.

Deny

Allow

In order to integrate with Google Directory Services, Barracuda had to create an application internal to the Barracuda Web Security Gateway that facilitates communication with Google Directory Services. This application must go through an approval process with Google, which has not yet been completed. As a consequence, when configuring Google Directory Services, you will see an error (as shown below) stating that the application is "untrusted", and this message can be safely ignored during the Google Directory Services configuration. This issue will be resolved when the application verification process with Google has completed.



This app isn't verified

This app hasn't been verified by Google yet. Only proceed if you know and trust the developer.

[Hide Advanced](#)

BACK TO SAFETY

Google hasn't reviewed this app yet and can't confirm it's authentic. Unverified apps may pose a threat to your personal data. [Learn more](#)

[Go to barracuda.com \(unsafe\)](#)

You are then redirected to the **USERS/GROUPS > Authentication** page on the Barracuda Web Security Gateway. You should see the alias of the GDS instance you created in the

Existing Authentication Services table on the page.

Existing Authentication Services		
ALIAS	TYPE	
Students	GADS	Edit Delete
Finance LDAP	LDAP	Edit Copy Delete

To disconnect from GDS, click **Delete** for the GDS instance (alias) in the table.

Figures

1. GDS New Auth.png
2. ConfigureLocalhostPopup.png
3. GDS WSG Allow Permissions.png
4. GDSAppNotVerified.png
5. GADS Existing Svce.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.