TRUSTWAVE MAILMARSHAL CLOUD

Using Connector Agent with Google Workspace LDAP

Table of Contents

About This Document **2**

Configuring GWS **2**

Adding a new client 2

Configuring Access Permissions 2

Downloading the Generated Certificate 2

Enabling the LDAP Service 3

Creating Credentials 3

Using stunnel **3**

Installing stunnel 3

Entering the Google Certificate 3

Configuring Stunnel as a Windows Service 4

Configuring MailMarshal Connector Agent **4**

Adding a Connector 5

Adding User Groups 6

Reviewing Setup **6**

About Trustwave **8**

About This Document

This document describes the necessary steps to retrieve user groups for use by MailMarshal Cloud from Google Workspace (GWS) via LDAP, using the Trustwave Connector Agent (CA).

GWS requires two forms of authentication, both a Client Certificate and username/password.

The CA does not natively support Client Certificates. The helper application stunnel is used to manage the client certificate.

Note: This document uses a sample domain arikimera-gws.com

Use your own GWS domain when setting up your instance of the Connector Agent.

Configuring GWS

To configure GWS for LDAP, follow the steps in the Google support article

https://support.google.com/a/topic/9048334?hl=en

Adding a new client

From the Google Admin Console, create a new LDAP client:

- **Name:** Trustwave Connector
- **Description:** Connector from Trustwave MailMarshal Cloud

Configuring Access Permissions

Follow the steps in the Google support article

https://support.google.com/a/answer/9058751?hl=en

Specify the following access:

- **Verify User Credentials:** No access
- **Read User Information:** Either select **Entire domain,** or select the specific OU groups that contain users that will be filtered by MailMarshal Cloud

Click **Add.**

A certificate will be generated.

Downloading the Generated Certificate

Download the generated certificate and save it to a location on your local computer

Enabling the LDAP Service

In GWS Admin Console, turn on the LDAP service.

Creating Credentials

Follow the steps in the Google support article

https://support.google.com/a/answer/9048541#generate-access-codes

In GWS Admin Console, under LDAP > Clients, click the Authentication tab.

Generate New Credentials

Save the username and password for later use.

Using stunnel

The CA does not natively support certificate authentication. You can use the stunnel method as recommended by Google at https://support.google.com/a/answer/9089736#stunnel

Installing stunnel

Download and install stunnel for Windows from www.stunnel.org/downloads.html

The name of the required file ends with “-win64-installer.exe” (e.g. stunnel-5.72-win64-installer.exe)

Run the installation file and install it to the default location of “C:\Program Files (x86)\stunnel” (if installing to another location, make a note for further steps.)

When prompted, run stunnel.

Entering the Google Certificate

Locate the certificate saved from the Google Admin Console. The filenames use the format “Google_2027_07_23_86041” (the name indicates the certificate expiration date).

Extract the .crt and .key files from the certificate download to the location “C:\Program Files (x86)\stunnel\config”

In stunnel, click Configuration > Edit Configuration. The file will open in notepad (or your default text editor).

Locate the line containing “Service definitions”

Add lines as in the example below.

Caution:

- Ensure there are no blank lines between the entries.

- **Replace the sample certificate names with the names of the files you downloaded and extracted**

```
[ldap-gws]
client=yes
accept=127.0.0.1:1636
connect=ldap.google.com:636
cert=Google_2027_07_23_86041.crt
key=Google_2027_07_23_86041.key
```

Save the file.

In the stunnel application, select **Configuration > Reload Configuration**

Terminate the stunnel application (File > Terminate)

Close the stunnel application.

Configuring Stunnel as a Windows Service

To ensure that the Connector Agent can use stunnel after you log out or restart the computer, install it as a Windows Service.

Run the following commands (in the directory `C:\Program Files (x86)\stunnel\bin`):

- `stunnel.exe -install`
- `net start stunnel`

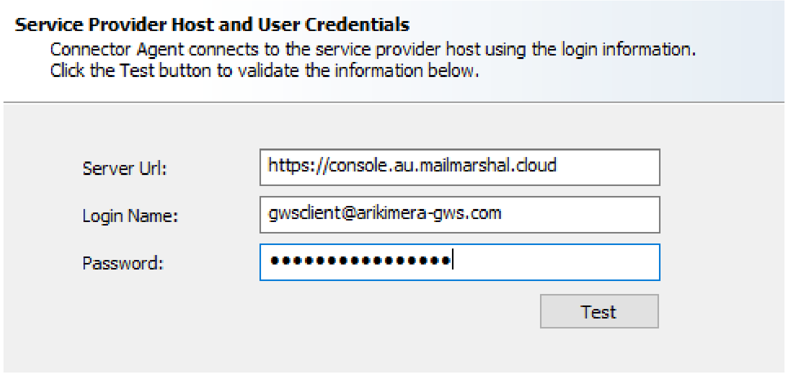
Note: After running stunnel interactively, you may need to log out, or restart the computer, before stunnel will start as a service.

Configuring MailMarshal Connector Agent

To install the MailMarshal Connector Agent, download and run the Connector Agent installer.

For general information, see the MailMarshal Cloud *Customer Guide*, available from https://support.trustwave.com/MailMarshalCloud/

Once you have installed the Connector Agent, configure the Service Provider host and user credentials as per the location specified in your provisioning documentation (see the example screenshot below).



Service Provider Host and User Credentials
Connector Agent connects to the service provider host using the login information.
Click the Test button to validate the information below.

Server Url: https://console.au.mailmarshal.cloud

Login Name: gwsclient@arikimera-gws.com

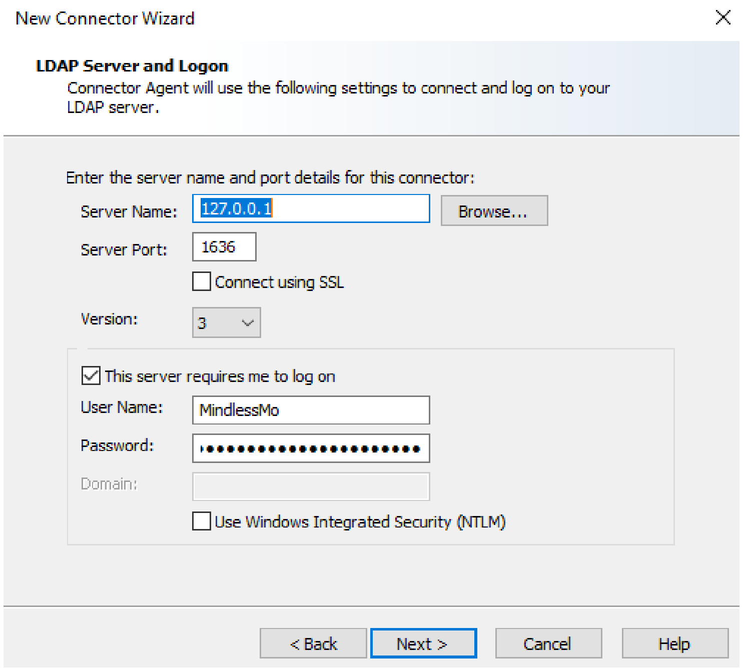
Password: ●●●●●●●●●●●●●●●●

Adding a Connector

To connect to GWS LDAP, add a connector using the local stunnel service.

In the New Connector Wizard, select **LDAP Directory > Generic LDAP Server**

- **Server Name:** 127.0.0.1
- **Port:** 1636
- **Version:** 3
- Select (check) **This server requires me to log on**
    - **User Name:** The user selected in Google LDAP settings above
    - **Password:** The password generated in Google LDAP settings



New Connector Wizard

LDAP Server and Logon
Connector Agent will use the following settings to connect and log on to your LDAP server.

Enter the server name and port details for this connector:

Server Name: 127.0.0.1

Server Port: 1636

□ Connect using SSL

Version: 3

☑ This server requires me to log on

User Name: MindlessMo

Password: ●●●●●●●●●●●●●●●●●●●●●

Domain:

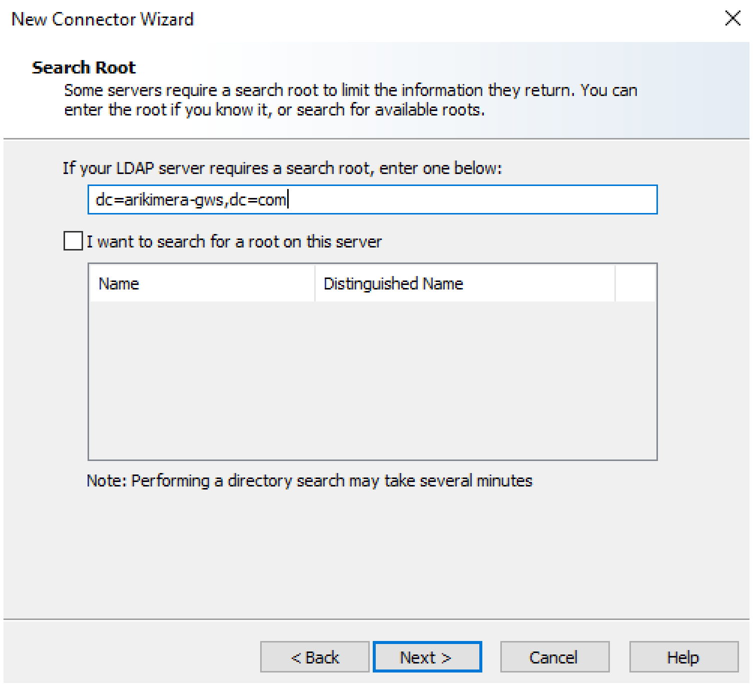
□ Use Windows Integrated Security (NTLM)

Click **Next.**

On the **Search Root** page, enter the details of your domain.

For “example.com”, you would enter

```
dc=example,dc=com
```



New Connector Wizard

Search Root

Some servers require a search root to limit the information they return. You can enter the root if you know it, or search for available roots.

If your LDAP server requires a search root, enter one below:

dc=arikimera-gws,dc=com

□ I want to search for a root on this server

Name	Distinguished Name

Note: Performing a directory search may take several minutes

Complete the Connector Wizard.

Adding User Groups

From the main window of the Connector Agent, select the Connector > User Groups tab, and click **New**.

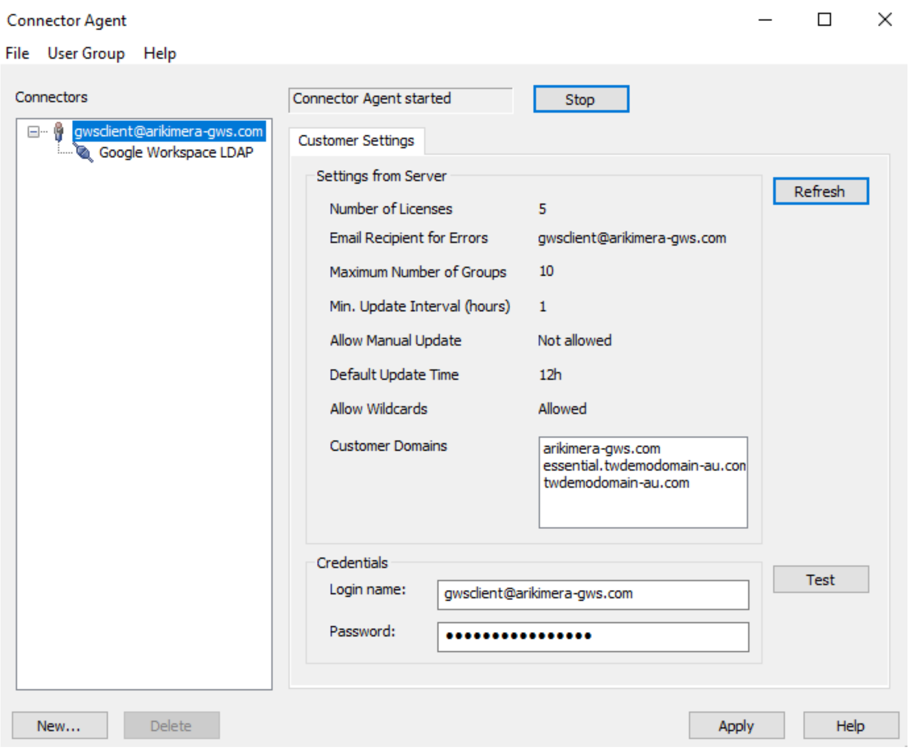
To add groups, you can browse, or enter details in DN format.

For more information, see Help for each window, and see also the *Customer Guide*.

Reviewing Setup

When setup is complete, the main page of the Connector Agent will appear similar to the below image.

To see details of the groups selected for import and the current membership, click the connector name.



Connector Agent started

Settings from Server

Number of Licenses	5
Email Recipient for Errors	gwsclient@arikimera-gws.com
Maximum Number of Groups	10
Min. Update Interval (hours)	1
Allow Manual Update	Not allowed
Default Update Time	12h
Allow Wildcards	Allowed
Customer Domains	arikimera-gws.com essential.twdemodomain-au.con twdemodomain-au.com

Credentials

Login name: gwsclient@arikimera-gws.com

Password: ••••••••••••••••

Important::

- Groups will be imported on a schedule as noted.
- **Manual update or more frequent update is generally not allowed.**

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave Fusion® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.