Protecting a domain in AVG AntiSpam is quick, simple and accomplished through a solution provider login. When you first login to the portal, click on “Customers” and then click “New Customer” to create a new customer.

Service/Domain Provisioning

1. Please log in as the solution provider at https://cloudcare.avgcloud.net. If you’d like to brand the login page, you can add /login?domain=example.com (replace example.com with your domain name).

   Click on Customers and then click on New Customer:

   ![Customers page with New Customer option selected]

2. Enter a descriptive name for your customer.

   ![Add New Customer form]

   - Customer Name: Example
   - Type: Solution Provider
3. Use this page to enter each of the domains used for email by your enterprise, together with the corresponding delivery destinations for incoming mail sent to this domain. Set it as the primary domain.

4. Enter the trusted IP address of the sending server. Trusted hosts are servers that are allowed to send mail through the AVG AntiSpam server to remote addresses.
5. Customer Properties. Here you can configure security policies for your customer:

New User Security Settings

Which security mode would you like to use?
- Allow-Listing
- Content Filtering
  - Cautious (Low - 90)
  - Optimized (Medium - 75)
  - Aggressive (High - 60)
  - Custom: 90 (0 - 100, where 0 will block all and 100 will block none)

- Spoofing Prevention: This will block all messages that originate outside the enterprise but appear to be both from and to domains inside the enterprise.

How would you like to handle spam?
- Vaporize messages from senders on the block list instead of quarantining them
  - Send a challenge/response or change-of-address request to the sender
  - Flag the subject line
  - Flag the subject line and deliver to delegate: [Field]
  - Vaporize
  - Quarantine the message and send a challenge/response or change-of-address request to the sender
  - Quarantine only
- Block incoming newsletters and bulk mailings

New User Address Settings

When sending a message to a new outside contact:
- Use the primary address and automatically add that contact to the allow list
- Create a new Protective Address and use it for all future communication with that contact

- Allow the use of Addresses-on-the-Fly
- Use this alias for outbound communications: user: [Field]

New User Message Format Options

- Format delivery for Microsoft Outlook
- Attach a Control Panel to the bottom of all incoming messages
  - Control Panel language: [Field] (English)
- Add a note to outbound messages
Creating Users

AVG AntiSpam offers three ways to create user accounts and import email addresses.

Manual Configuration/CSV Import

This method is recommended for smaller sites and servers that are not running Microsoft Exchange and do not have an LDAP directory. Manual configuration allows you to add users one by one or you can use a CSV spreadsheet to import names, primary addresses, and email aliases directly into AVG AntiSpam.

1. Manual (Users > New User):

2. CSV Import (Users > Import Users):
3. LDAP Sync (Users > LDAP Setup)

This method is recommended for larger deployments of Microsoft Exchange or environments with high user turnover. By configuring LDAP sync, you will be assured that all changes made in Active Directory users will sync over to AVG AntiSpam.

![LDAP Setup for Example](image)

The customer's firewall **must** be configured to allow TCP connections on ports **389** or **636 (SSL)** from ALL of the following subnets:

- 100.42.120.96/255.255.255.224 (CIDR: 100.42.120.96/27)
- 100.42.115.0/255.255.255.224 (CIDR: 100.42.115.0/27)
- 208.70.208.0/255.255.252.0 (CIDR: 208.70.208.0/22)

**Primary Domain:** example.com

**LDAP Host:**

Enter an IP (e.g. 123.12.12.123) or a **fully qualified domain name** (e.g. xyz.test.net)

**LDAP Port 389 (Default; non-secure)**

[Test Connection]
Network Configuration

In order to properly secure your domains, you need to make a couple changes on your network.

First, you have to change your MX record to point all of your inbound mail to AVG AntiSpam. This way, AVG AntiSpam will stand in front of your mail server to scan and filter all email that is sent to your network.

Once the MX records have been changed, you will need to configure your server to send outbound mail through AVG AntiSpam using a smart host. This will allow us to scan all of your outbound mail.

The next step is to lock down the server to only accept mail from AVG AntiSpam IP addresses. This will ensure that all mail is filtered by AVG AntiSpam.

Last step, if needed: Create an SPF record in DNS.

1. MX Record

Please modify your MX record and change it to:

mx1.avgcloud.net
mx2.avgcloud.net

You should not have any other MX records listed for your domain name.

2. Outbound Smart Host

Please modify your SMTP server to route all outbound mail through the following smart host:

outbound.avgcloud.net

3. Exchange Access Restriction Procedure

To ensure that no mail is presented to your mail server without being processed by AVG AntiSpam, you will need to restrict all IP access to your mail server with the exception of the following AVG AntiSpam IP addresses:

100.42.120.96/27
100.42.115.0/27
208.70.208.0/22

4. SPF Record

If you are using the outbound filtering service and have a need for an SPF record on your domain, you will want to make sure that your domain has the following added to its SPF. This is the only entry that is needed:

v=spf1 ip4:100.42.120.96/27 ip4:100.42.115.0/27 ip4:208.70.208.0/22 ~all