Moving from Barracuda Email Security Gateway to Email Gateway Defense

https://campus.barracuda.com/doc/96023061/

This article describes what to expect when moving from Barracuda Email Security Gateway to Email Gateway Defense.

There are two options for moving:

- Converting from Barracuda Email Security Gateway data to Email Gateway Defense data.
- Migrating all of your existing settings – including settings, domains, and users – from the Barracuda Email Security Gateway to Email Gateway Defense.

Option 1: Converting Data

Before Conversion

Before you can begin the conversion process, you must complete the following steps.

1. Create a Barracuda Networks Account

You must have a Barracuda Networks account.

1. Create an account in Barracuda Cloud Control, as described in Create a Barracuda Cloud Control Account.
2. Start a free trial of Email Gateway Defense, as described in Set Up Email Gateway Defense for Microsoft 365.

   Note that you must purchase a license for Email Gateway Defense before the 14-day trial period expires.

2. Add Domains and Test Connectivity

1. Add and verify your domains as described in Step 2 - Configure Microsoft 365 for Inbound and Outbound Mail.
2. Test domain connectivity by sending a test email. Repeat this sequence for each domain.
   1. In Barracuda Cloud Control, select **Email Gateway Defense** in the left panel.
   2. Navigate to the **Domains** page. For the appropriate Domain Name, go to **Settings > Edit**. At the top of the **Domain Settings** page, under **Mail Server**, click **Test**.
   3. Enter an email address and click **Send**. The system sends a message to the email address you specify, with the return address *Barracuda Networks Email Test*.

3. Open IP Ports to Receive Email

Open IP ports on your firewall, based on your region, as described in Email Gateway Defense IP Ranges Used for Configuration.

4. Open Ports for LDAP Synchronization

Open your firewall ports to allow the IP address ranges for LDAP connectivity based on your Barracuda Networks instance, as described in Email Gateway Defense IP Ranges Used for Configuration.

The Conversion Process

Converting data from Barracuda Email Security Gateway to Email Gateway Defense requires the following steps:

1. Convert and import configurations
2. Copy users into Email Gateway Defense
3. Change MX records to point to Email Gateway Defense

1. Convert and Import Configurations

For this step, you can convert your configurations manually or you can choose to use Barracuda Networks' conversion tool. For instructions on using the conversion tool, refer to Conversion Tool for Migrating to Email Gateway Defense.

> This article contains all of the required steps for complete migration from Barracuda Email Security Gateway to Email Gateway Defense. If you choose to use the conversion tool, you must still perform all of the other steps described in this article.

Configurations to Import

The following table lists configurations in Barracuda Email Security Gateway that you must convert to a format compatible with Email Gateway Defense.

Email Security Gateway	Email Gateway Defense
Block/Accept > IP filters	**Inbound Settings > IP Address Policies**
Allowed IP/Range	IP Blocking / Exemption

Blocked IP/Range	IP Blocking / Exemption (Tagging is not an option)
Block/Accept > Recipient Filters	**Inbound Settings > Recipient Policies**
Allowed Recipients	Recipient Policies
Blocked Recipients	Recipient Policies (Tagging is not an option)
Encrypted Sender Addresses and Domains (Outbound Only)	-
Redirected Sender Addresses and Domains (Outbound Only)	-
Block/Accept > Sender Filters	**Inbound Settings > Sender Policies**
Allowed Senders	Sender Policies
Blocked Senders	Sender Policies (Tagging is not an option)
Encrypted Sender Addresses and Domains (Outbound Only)	-
Redirected Sender Addresses and Domains (Outbound Only)	-
Block/Accept > Content Filtering	**Inbound Settings > Content Policies**
Content Filters	Message Content Filter (Subject, Header, Body)
Attachment Content Filters	Message Content Filter (Attachments)
Predefined Filters	Predefined Filters
Block/Accept > Content Filtering	**Outbound Settings > Content Policies**
Content Filters	Message Content Filter (Subject, Header, Body)
Attachment Content Filters	Message Content Filter (Attachments)
Predefined Filters	Predefined Filters
Block/Accept > Attachment Filters	***Inbound* Settings > Content Policies**
Attachment Filename Filters	Attachment Filter
Attachment File Type Filters	-
Attachment MIME Type Filters	Attachment Filter
Password Protected Archive Filtering	Attachment Filter
Block/Accept > Attachment Filters	***Outbound* Settings > Content Policies**
Attachment Filename Filters	Attachment Filter
Attachment File Type Filters	-
Attachment MIME Type Filters	Attachment Filter
Password Protected Archive Filtering	Attachment Filter

If you are using multi-factor authentication (MFA), you must configure user authentication with

Microsoft Entra ID.

2. Copy Users into Email Gateway Defense

Use this section to set up directory services for one or more of your domains. You can use either Azure AD (now Microsoft Entra ID) or LDAP directory services to enable single sign on (SSO) and synchronization of users lists.

- **LDAP** – Configure LDAP authentication through your organization's LDAP servers. Refer to How to Configure User Authentication Using LDAP for details.
- **Azure AD** – Configure user authentication through your organization's Microsoft Entra ID service. Refer to How to Configure User Authentication with Microsoft Entra ID for step-by-step instructions.

3. Change Your MX Records to point to Email Gateway Defense

Update your MX records to point to Email Gateway Defense, as described in How to Set Up MX Records for Domain Verification.

After Conversion

After you complete the conversion process, perform the following steps:

1. Verify Email Flow

Send a test email to each of your domains to verify that you configured your account and migrated your settings correctly.

In Email Gateway Defense, navigate to **Overview > Message Log** to ensure that you can see the messages.

2. (Optional) Configure Outbound Email for Email Gateway Defense

Optionally follow *Step 7. Configure Outbound Mail* in Configure Microsoft 365 for Inbound and Outbound Mail.

Caveats

- Message Log data will not be transferred to Email Gateway Defense.
- Per user settings must be added separately.
- Domain-specific settings are not transferred automatically.
- Sender and Recipient Encryption exemptions will NOT be transferred to Email Gateway Defense.
- End users must log into a different URL to access quarantined email.

- If you have an existing Cloud Protection Layer or Barracuda Networks account into which you are migrating data, all of the existing data in that account will be replaced by the data from your Email Gateway Defense device.
- Inbound and outbound rate control limits can be customized in Barracuda Email Security Gateway, but not in Email Gateway Defense. Refer to the following articles for details:
  - Inbound Rate Control
  - Outbound Rate Control

Important

- When importing configurations, copy your settings to the *global account* level, and *not* to the *domain* level.
- You must manually add configurations that are not moved by the conversion tool.
- Ensure that you have migrated all the settings and configurations needed.

Option 2: Migrating All Settings, Domains, and Users

In this option, contact Barracuda Networks Technical Support for assistance with migrating all of your Barracuda Email Security Gateway settings, domains, and users to Email Gateway Defense.

Important

- If you are migrating to an *existing* Barracuda Cloud Protection Layer or Email Gateway Defense account, note that all of the data in that account will be replaced by the data from your Barracuda Email Security Gateway account.
- Domains added to Email Gateway Defense during a migration are unverified. (See more on this below.)
- If you were using Barracuda Cloud Protection Layer or Email Gateway Defense prior to the migration, your email will stop working after the migration is complete. To ensure that your mail does not stop, *before you start the migration*, change your MX records to point directly to either your Barracuda Email Security Gateway or to your mail server. *After the migration is complete and you have verified your domain*, you can then point your MX records to the new Email Gateway Defense MX record, found for your domain(s) in Email Gateway Defense.
- Before beginning migration, make a backup of your account configuration. This will back up your current account level settings, in case you want to go back to them. It will not back up the domain level settings or your users and their settings.

After migration is completed, check the Email Gateway Defense service settings to ensure that the migrated information is correct.

Note that Message Log data will not be transferred to the Barracuda Email Gateway Defense.

Note again that domains moved through migration are not verified. Verifying each domain individually:

- Proves that you are authorized to manage mail in that domain.
- Allows you to activate each domain at your own pace.
- Does not allow Email Gateway Defense to start processing mail for a domain before it is ready.
- Enables you to correct the Destination Mail Server in Email Gateway Defense for each domain.

The last step of the migration process is to change your MX records for each domain to point to Email Gateway Defense. It is important that the MX record you use is the correct one for each domain. Each domain has its own unique MX record. Note that MX records must all point to Email Gateway Defense. Any MX records pointing elsewhere will compromise the protection from spam and attacks provided by Email Gateway Defense.

Review the Email Gateway Defense articles in Barracuda Campus to ensure you have no problems with your migration.

If you have any questions on moving from Barracuda Email Security Gateway to Email Gateway Defense, contact Barracuda Networks Technical Support.