

CONFIGURATION GUIDE

Using MailMarshal Cloud with Exchange Online

Table of Contents

About This Document	1
1 Trustwave MailMarshal Cloud for Anti-Malware with Exchange Online	2
2 Networking and DNS Setup	2
3 Provisioning Trustwave MailMarshal Cloud	3
4 Configuring Exchange Online	4
4.1 Set up a connector to send outgoing messages through MailMarshal Cloud	5
4.2 Set up a connector to accept incoming messages from MailMarshal Cloud	7
4.3 Set up Connection Filter Exclusions	8
4.4 Set up the SEG Connector Agent for Azure AD	10
About Trustwave	13

About This Document

This document is for the use of email administrators who are using Trustwave MailMarshal Cloud to accept and filter messages from the Internet, and a cloud based solution to host user mailboxes.

This document provides specific instructions for configuration with Microsoft Exchange Online.

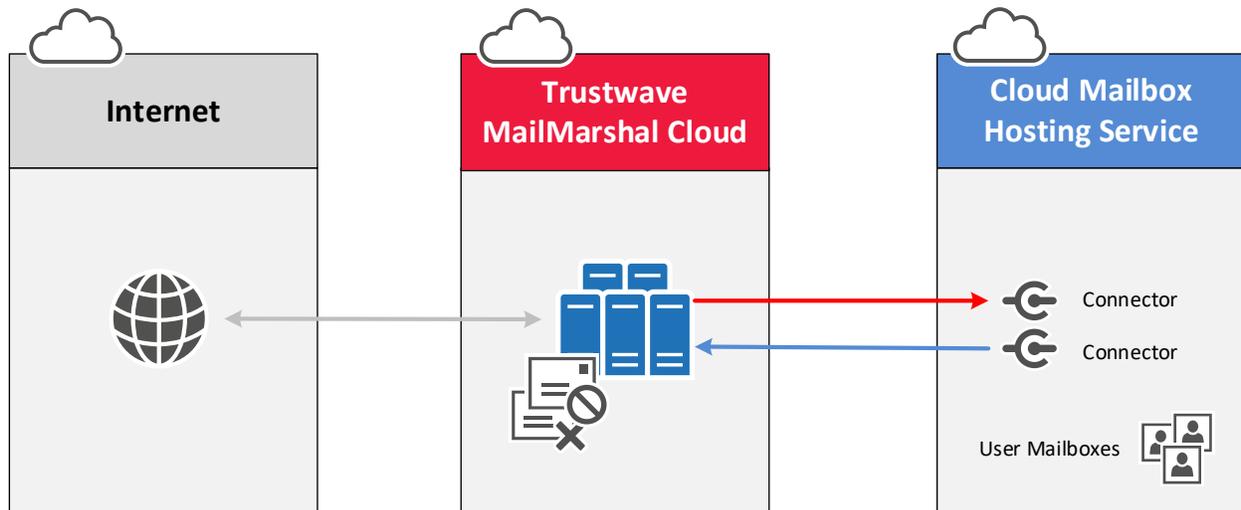


Note: Microsoft frequently re-organizes the management interfaces. Exact steps may differ, but the concepts are the same.

The same ideas can be used to configure other cloud-based mailbox hosting solutions. (For Google G Suite, see the separate document with detailed instructions.)

1 Trustwave MailMarshal Cloud for Anti-Malware with Exchange Online

In this scenario, the organization hosts user mailboxes on a cloud-based service such as Microsoft Exchange Online. The organization uses the Trustwave MailMarshal Cloud service to provide filtering of spam and malware, and other policy controls for both inbound and outbound messages.



2 Networking and DNS Setup

1. Configure MX records for all your local domains to point to the Trustwave MailMarshal Cloud environment.
2. Add the MailMarshal Cloud server to your SPF record as an include. Also include the Office365 SPF record.



Note: The settings depend on the regional instance of MailMarshal Cloud configured for your customer account when provisioned. For details of the configuration data required, see the details for your instance (US, Australia, or EU) linked from the [MailMarshal Cloud Information](#) page.

In most cases MX records are updated when you are ready to direct email into the new environment (after all other configuration is complete).

3 Provisioning Trustwave MailMarshal Cloud

Trustwave Provisioning or Managed Security Services must configure MailMarshal Cloud to accept and deliver email for your domains.

1. MailMarshal Cloud will deliver email incoming for your managed domains to the cloud hosting environment. Provide the delivery details to Trustwave.
 - For Exchange Online, use the “MX endpoint” of your Exchange Online environment (such as `yourexampldomain-com.mail.protection.outlook.com`).
2. MailMarshal Cloud will accept email relaying (messages sent to other domains “from” your managed domains) based on the configured inbound delivery addresses. For Exchange Online, to ensure that the relaying addresses are up to date, Trustwave will also configure relaying based on the SPF records published by the service.



Tip: The default domain in Exchange Online must be a domain configured in MailMarshal Cloud.

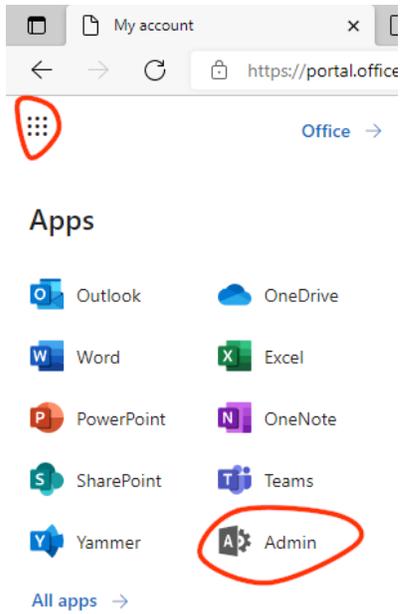
4 Configuring Exchange Online

You will set up two connectors to route email between MailMarshal Cloud and Exchange Online.

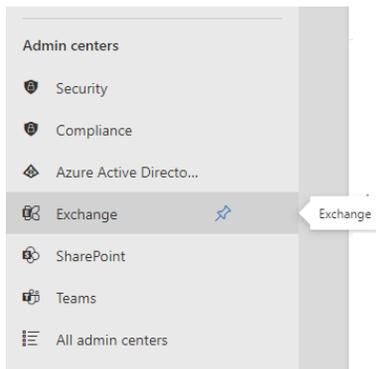
To complete this step, you must have an Office 365 Administrator credential with permission to create connectors. You may find that the validation process only works with a Microsoft browser.

To create a connector in Office 365:

1. From the Office site, open the app menu and click **Admin** (If you do not see Admin, click **All apps**).



2. From the Admin left menu, click **Exchange** to go to the Exchange Admin Center.



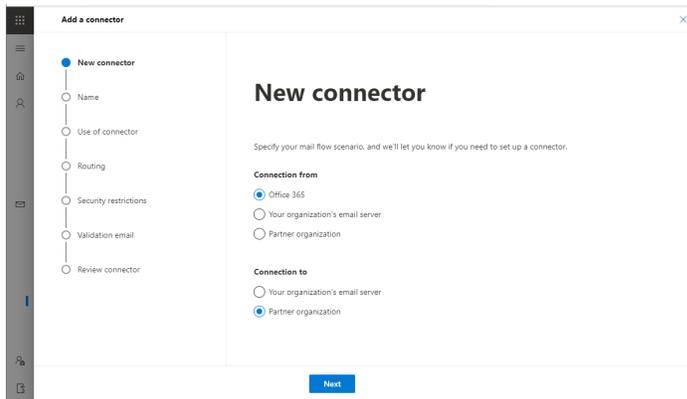
3. Next, expand **mail flow**, and then click **connectors**.

4.1 Set up a connector to send outgoing messages through MailMarshal Cloud

1. To start the Connector wizard, click **Add a connector**.
2. On the first screen, choose a connector as follows:

Connection from
Office 365
Connection to
Partner Organization

Click **Next**.

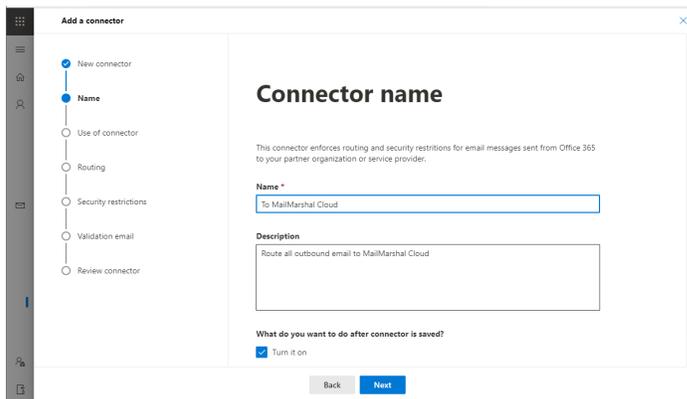


The screenshot shows the 'Add a connector' wizard in Exchange Online. The left sidebar contains a progress indicator with steps: New connector (selected), Name, Use of connector, Routing, Security restrictions, Validation email, and Review connector. The main content area is titled 'New connector' and includes the following options:

- Connection from:**
 - Office 365
 - Your organization's email server
 - Partner organization
- Connection to:**
 - Your organization's email server
 - Partner organization

A 'Next' button is located at the bottom right of the main content area.

3. On the next screen, give the connector a name and a detailed description. If you want to enable this routing immediately, check the box **Turn it on**. Click **Next**.



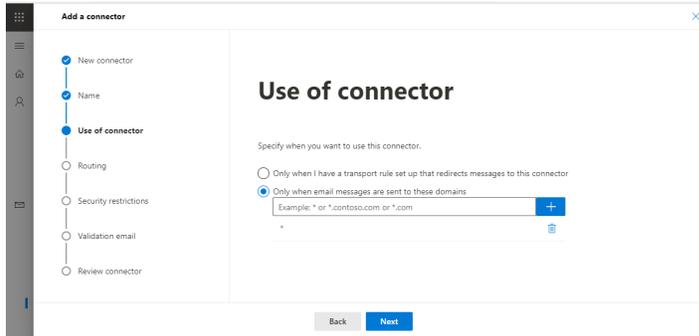
The screenshot shows the 'Add a connector' wizard in Exchange Online, Step 2: Connector name. The left sidebar shows the progress indicator with 'Name' selected. The main content area is titled 'Connector name' and includes the following fields and options:

- Name ***: A text input field containing 'To MailMarshal Cloud'.
- Description**: A text area containing 'Route all outbound email to MailMarshal Cloud'.
- What do you want to do after connector is saved?**: A checkbox labeled 'Turn it on' which is checked.

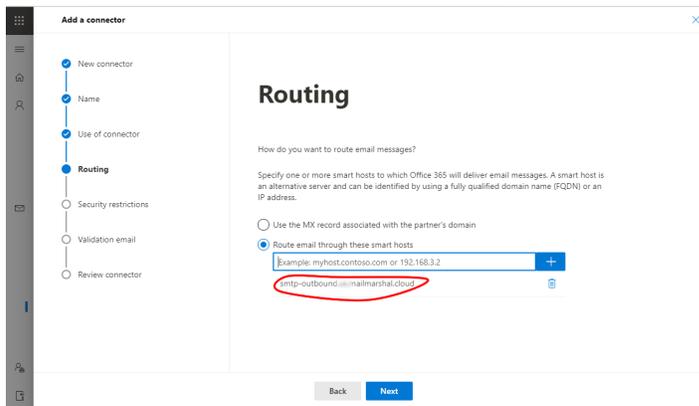
'Back' and 'Next' buttons are located at the bottom of the main content area.

4. On the following screen (Use of connector), select *Only when email messages are sent to these domains*.

In the field, enter * and then click + to add the entry. Click **Next**.



5. On the next screen (Routing), select *Route email through these smart hosts*.
6. Enter the externally resolvable hostname of the Trustwave MailMarshal Cloud server, then click + to add the entry. For details of the name required, see the connection details for your instance (US, Australia, or EU) linked from the [MailMarshal Cloud Information](#) page.

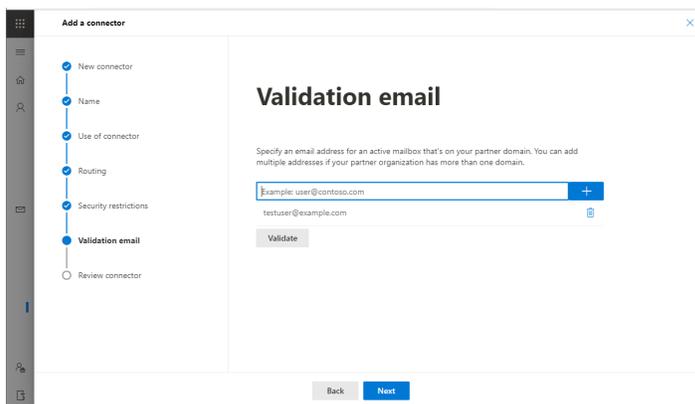


7. On the following screen (Security restrictions), the *Always use Transport Layer Security* box should be selected.
8. Ensure that your connector validates. You will need to add a deliverable email address where a message can be sent for validation. Because this connector is used for all outbound messages, you can enter any address outside your managed domains.



Tip: The default domain in Exchange Online will be used as the domain of the From address. Be sure that this domain is one of your domains configured in MailMarshal Cloud. If it is not, the validation email will be rejected with the message 550 Cannot determine unique tenancy.

If your Exchange Online environment includes domains that are not configured in MailMarshal Cloud, you must configure a Transport Rule to limit the messages sent through this connector.



9. Save the connector.

4.2 Set up a connector to accept incoming messages from MailMarshal Cloud



Note: When you set up a connector as described in this section, Exchange Online will ONLY accept incoming SMTP messages that are sent from the MailMarshal Cloud servers at the IP addresses you specify. Messages from any other source will be refused.

This connector is required to ensure that malware or spam cannot bypass MailMarshal Cloud. You should only enable the connect AFTER you have updated MX records and confirmed email is flowing through MailMarshal Cloud to Exchange Online.

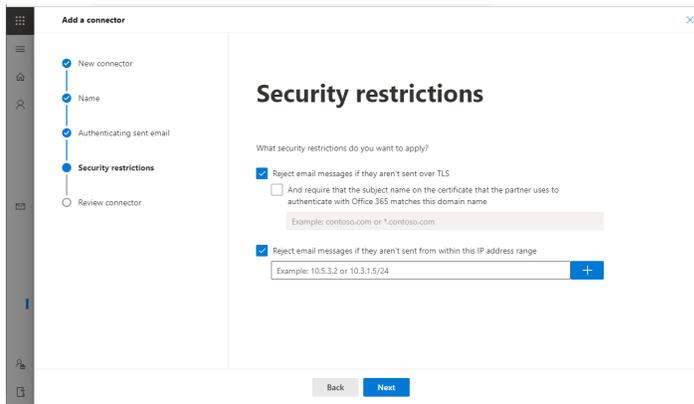
The steps to accept incoming messages are similar to those for outgoing messages.

1. To start the Connector wizard, click the plus symbol +.
2. On the first screen, choose a connector as follows (**note the direction**):

Connection from
Partner Organization
Connection to
Office 365

3. Give the connector a name and verbose description.
4. On the screen *Authenticating sent email*, select *By verifying that the sender domain matches one of the following domains*.
 - Enter * (to signify all domains), and then click + to add the entry.
5. On the Security restrictions screen, keep the entry *Reject email messages if they aren't sent over TLS*. **Do not require a subject name on the certificate.**
6. Select *Reject email messages if they aren't sent from within this IP address range*

- Type or paste each required range and then click + to add it. For details of the ranges required, see the connection details for your instance (US, Australia, or EU) linked from the [MailMarshal Cloud Information](#) page.



7. Repeat until you have added all required ranges for your instance.



Note: Some instances use ranges with CIDR /22. Because Exchange Online only allows ranges with /24 or higher, in this case you must enter four ranges to cover the required addresses.

8. Save the connector.

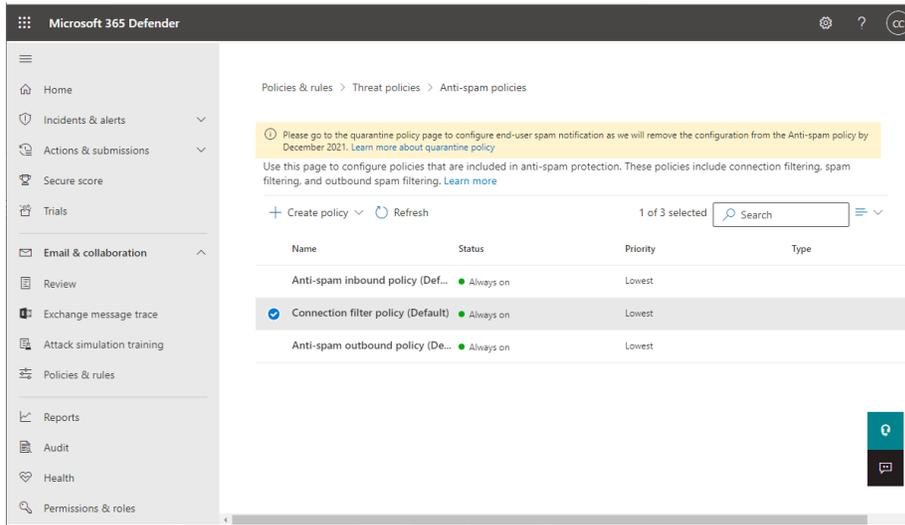
4.3 Set up Connection Filter Exclusions

Exchange Online includes a “connection filtering” function that limits the number of messages received from each IP address. You must exclude MailMarshal Cloud from this filtering to ensure that all incoming messages can be delivered.

To set up exclusions:

1. From the Office site, open the app menu and click **Security** (If you do not see Security, click **All apps**).

2. Navigate to **Policies & Rules > Threat policies > Anti-spam policies**. Edit the **Connection filter policy (default)**.

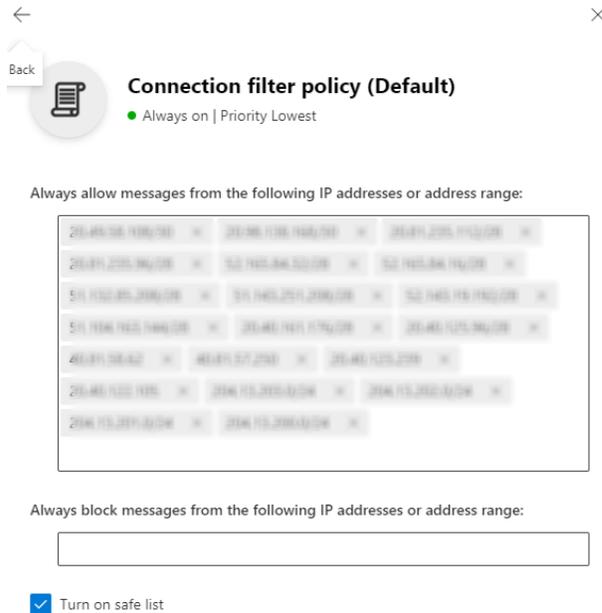


3. On the edit pane, in the Always Allow list, add the IP address ranges for MailMarshal Cloud, as in the connector setup.
4. Click **Save**.



Note: Be sure to enter the correct IP ranges to allow inbound for your instance (US, Australia, or EU) linked from the [MailMarshal Cloud Information](#) page.

The filtering information may appear as below:



4.4 Set up the MailMarshal Connector Agent for Azure AD

The Connector Agent is an optional module of MailMarshal Cloud that allows you to retrieve information about local user groups and email addresses from your Active Directory server or LDAP server, for use in MailMarshal Cloud policy.

You can use the Connector Agent with Azure AD.



Tip: For full instructions about how to download, install, and configure the Connector Agent, refer to the MailMarshal Cloud Customer Guide.

- If you have a workstation or server available on premises that is a domain member, you can install and configure the Connector Agent in the same way as for a premises AD installation. Refer to the MailMarshal Cloud Customer Guide.
- You can also use the Connector Agent to synchronize information from Azure AD using LDAPS.

To use the Connector Agent with Azure AD LDAPS:

1. Configure Secure LDAP (LDAPS) in Azure AD Domain Services. See the [Microsoft documentation for this task](#).

2. Once secure LDAP access to your managed domain over the internet is successfully enabled, the Azure AD Domain Services management site shows the external IP address that can be used to access your directory over LDAPS in the field **EXTERNAL IP ADDRESS FOR LDAPS ACCESS**.

domain services PREVIEW

ENABLE DOMAIN SERVICES FOR THIS DIRECTORY YES NO ?

Users will not be able to login to the domain using their credentials until you [enable password synchronization](#).

DNS DOMAIN NAME OF DOMAIN SERVICES ?

CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK ?

IP ADDRESS ?

SECURE LDAP (LDAPS) ?

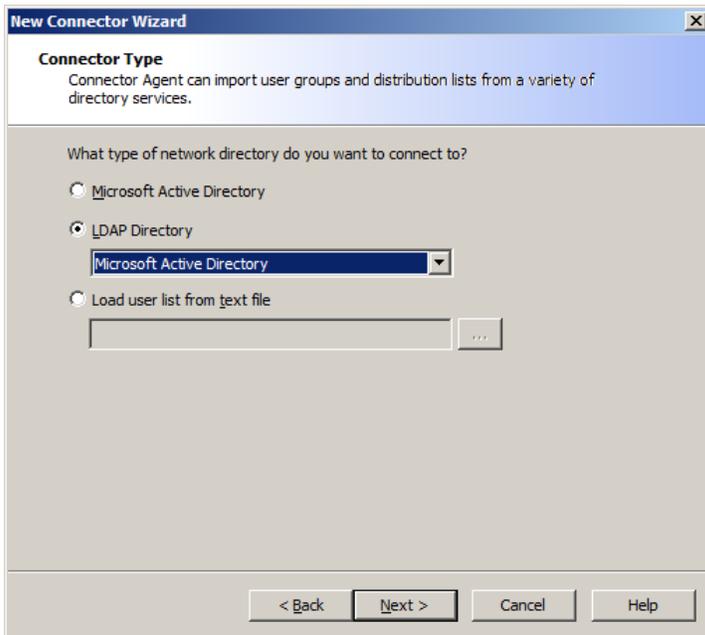
SECURE LDAP CERTIFICATE ?

ENABLE SECURE LDAP ACCESS OVER THE INTERNET YES NO ?

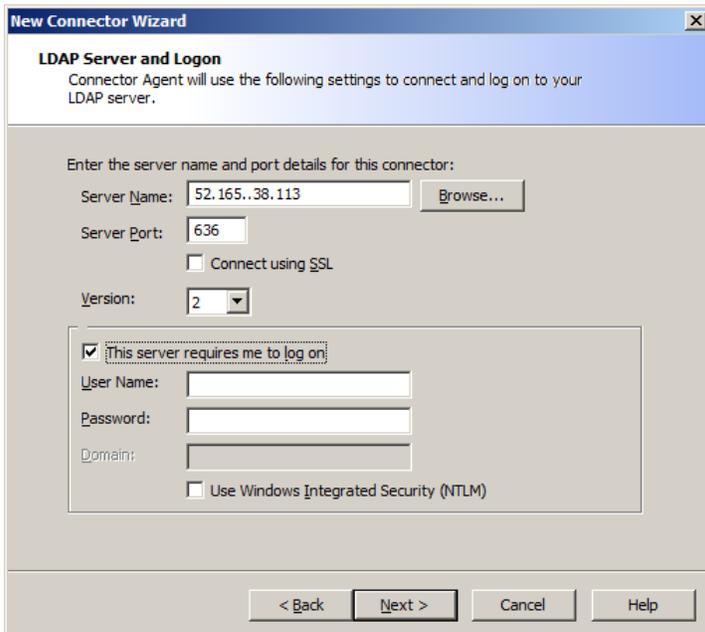
?

3. Install the Connector Agent on any computer that has Internet access (HTTPS access to MailMarshal Cloud, and port 636 for LDAPS access to the Azure LDAPS IP address).

4. Create a new connector, and specify a **LDAP directory** of type "Microsoft Active Directory".



5. Enter the Azure LDAPS IP address. Specify port 636 and select **Connect using SSL**. Enter logon credentials.



6. Click **Next**. The Agent tests the connection.
7. When the connection is successfully tested, continue the Wizard as described in the MailMarshal Cloud Customer Guide.
8. When the connector has been successfully created, you can proceed to select groups for synchronization.

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 TrustKeeper® 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>.