LevelBlue
Secure What's Next.

CONFIGURATION GUIDE

Using MailMarshal Cloud with Exchange Server

Table of Contents

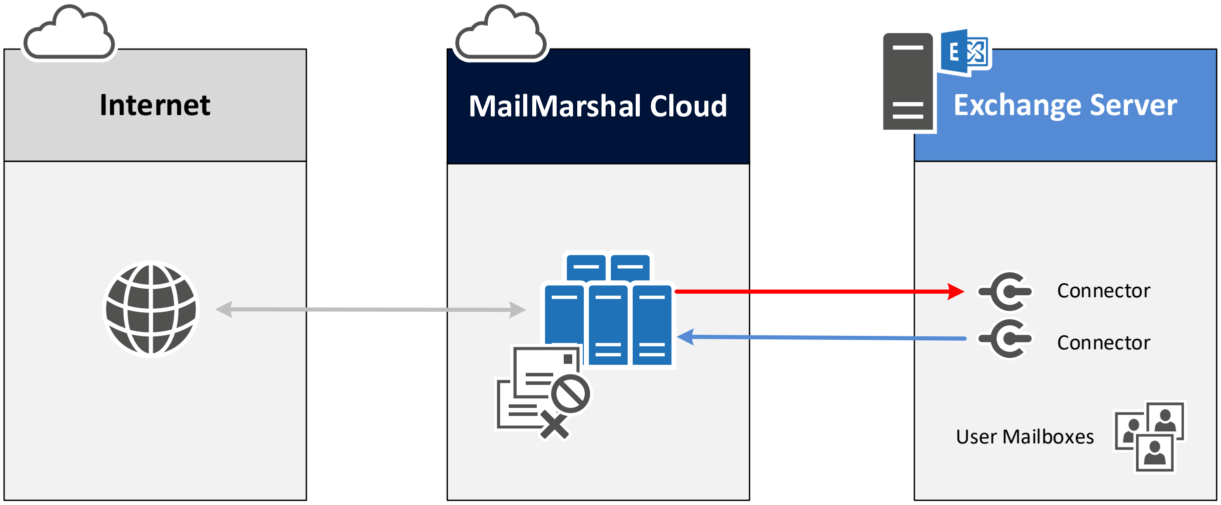
About This Document

This document is for the use of email administrators who are using MailMarshal Cloud to accept and filter messages from the Internet, and Microsoft Exchange to host user mailboxes.

The detailed procedures apply to Exchange 2016. The same ideas can be used to configure all versions of Microsoft Exchange, and other premises mail servers.

1 MailMarshal Cloud with Exchange Server

In this scenario, the organization hosts user mailboxes on a premises Microsoft Exchange server. The organization uses the 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

Note: The settings you enter in this step depend on the regional instance of MailMarshal Cloud configured for your customer account when provisioned. For details of the configuration data required, see MailMarshal Cloud Knowledgebase article Q21095, MailMarshal Cloud Connection Details (follow links for instances other than the US instance).

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

1. Configure MX records for all your local domains to point to the MailMarshal Cloud environment:
2. Add the MailMarshal Cloud server to your SPF record.
3. Ensure that any firewalls or SMTP proxy servers are configured to allow email traffic to and from MailMarshal Cloud.

3 Provisioning MailMarshal Cloud

The service provisioning team must configure MailMarshal Cloud to accept and deliver email for your domains, based on the information you provide.

1. MailMarshal Cloud will deliver email incoming for your managed domains to your local server. Provide the delivery details on the provisioning form.
2. MailMarshal Cloud will accept email relaying (messages sent to other domains “from” your managed domains) based on the configured inbound delivery addresses.

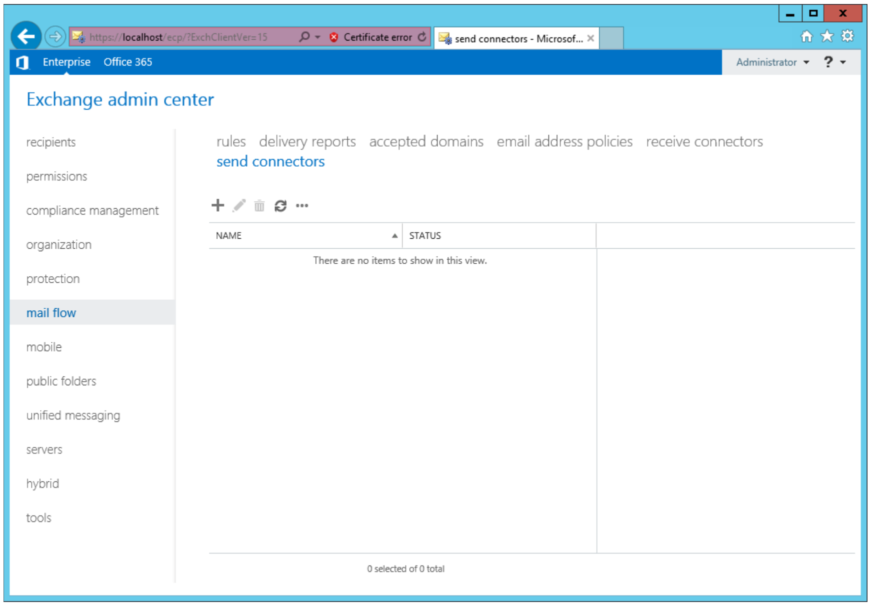
4 Configuring Exchange Server

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

To complete this step, you must have access to the Exchange Admin Center for the premises Exchange environment.

To create connectors in Exchange:

1. Log in to the Exchange Admin Center.
2. Click **mail flow**.



There are no items to show in this view.

0 selected of 0 total

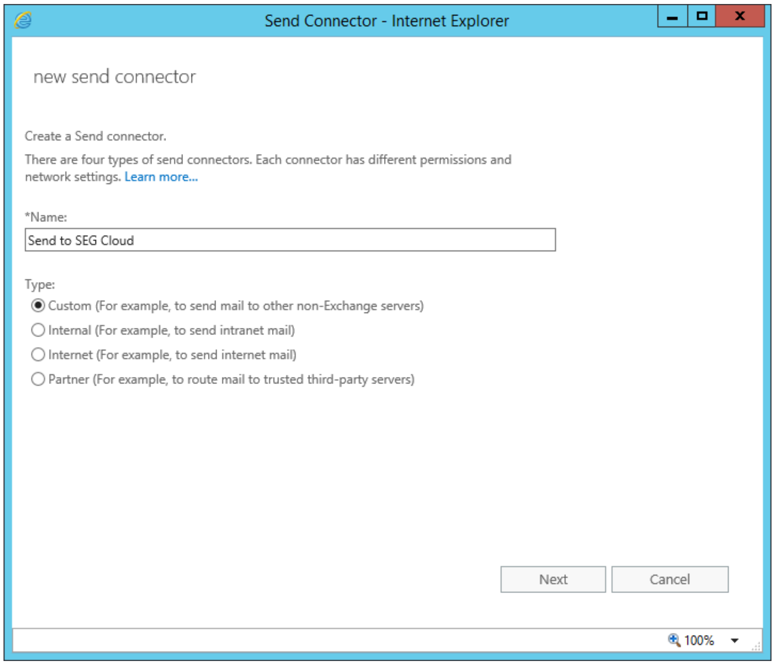
4.1 Set up a connector to send outgoing messages through MailMarshal Cloud

Note: These instructions assume that no Send connectors are configured in Exchange.

If you have configured a Send connector, you may prefer to edit the existing connector, or remove it and create a new one.

1. On the Mail Flow window, click **send connectors**.
2. To start the Connector wizard, click the plus symbol **+.**

3. Give the connector a name, and choose type **Custom**.



new send connector

Create a Send connector.

There are four types of send connectors. Each connector has different permissions and network settings. Learn more...

*Name:

Send to SEG Cloud

Type:

● Custom (For example, to send mail to other non-Exchange servers)

○ Internal (For example, to send intranet mail)

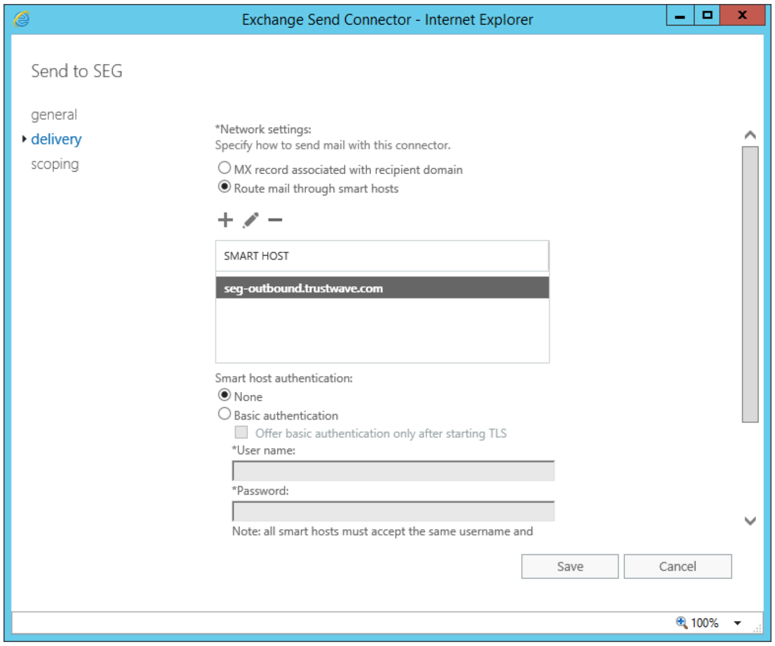
○ Internet (For example, to send internet mail)

○ Partner (For example, to route mail to trusted third-party servers)

4. Click **Next**.

5. Choose to **Route mail through smart hosts**.

6. Enter the MailMarshal Cloud FQDN. For details of the configuration data required, see MailMarshal Cloud Knowledgebase article Q21095, [MailMarshal Cloud Connection Details] (follow links for instances other than the US instance).



Send to SEG

*Network settings:

Specify how to send mail with this connector.

○ MX record associated with recipient domain

● Route mail through smart hosts

SMART HOST
seg-outbound.trustwave.com

Smart host authentication:

● None

○ Basic authentication

□ Offer basic authentication only after starting TLS

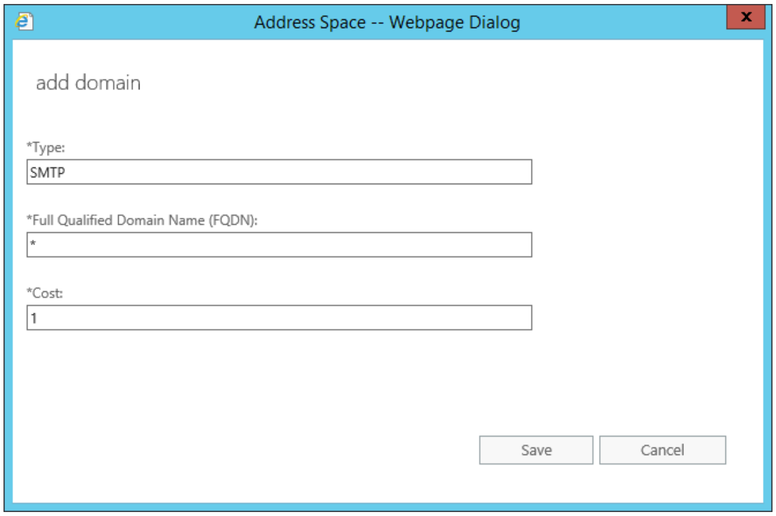
*User name:

*Password:

Note: all smart hosts must accept the same username and

7. Click **Next**.

8. On the **Authentication** window, select **None** and then click **Next**. Authentication is not required, because MailMarshal Cloud will only accept outgoing messages from the servers you specified in your provisioning request.
9. On the **Address Space** window, click + to add an entry. To deliver all outgoing mail through MailMarshal Cloud, enter * (all domains), and then click **Save**.



Address Space -- Webpage Dialog

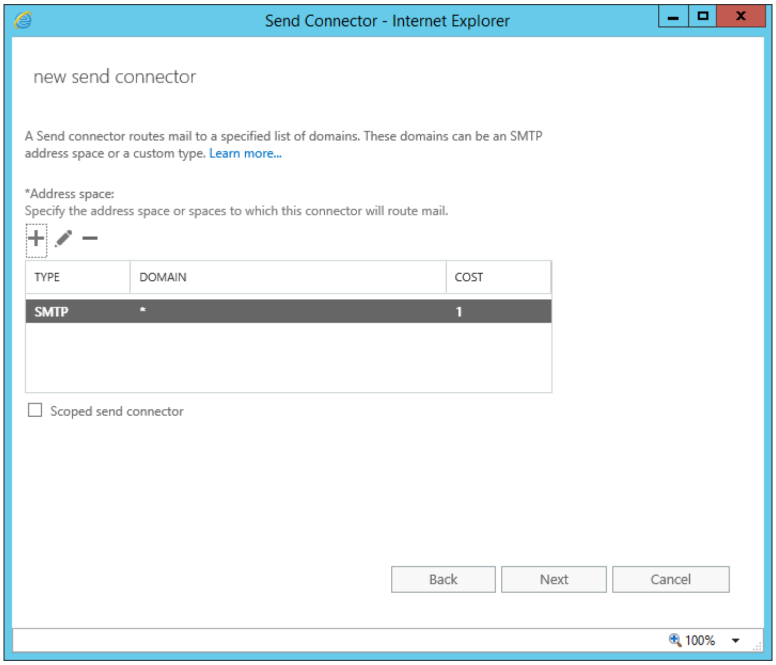
add domain

*Type: SMTP

*Full Qualified Domain Name (FQDN): *

*Cost: 1

10. The result displays on the parent window.



Send Connector - Internet Explorer

new send connector

A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. Learn more...

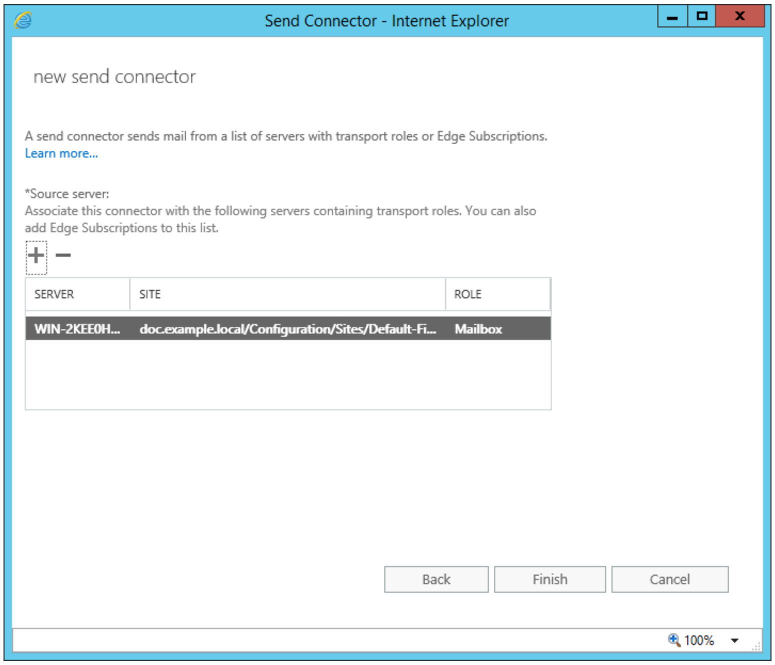
*Address space:
Specify the address space or spaces to which this connector will route mail.

TYPE	DOMAIN	COST
SMTP	*	1

☐ Scoped send connector

11. Click **Next**.

12. On the **Source Server** window, add the servers you want to send outbound mail through MailMarshal Cloud (generally all eligible servers in the environment).



Send Connector - Internet Explorer

new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions.
Learn more...

*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.

SERVER	SITE	ROLE
WIN-2KEE0H...	doc.example.local/Configuration/Sites/Default-Fi...	Mailbox

13. Click **Finish**.

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

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

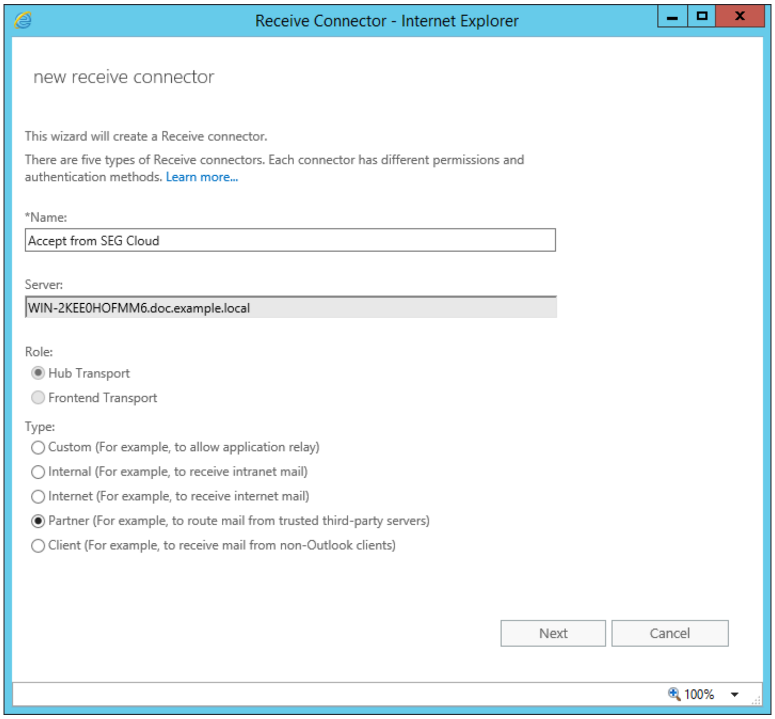
Note: These instructions assume that no Receive Connectors are configured in Exchange.

In many cases a “Default Frontend” connector will be configured and bound to all IPv4 addresses. You will not be able to create a new connector bound to the same IP addresses as an existing connector. You might prefer to edit the existing connector to use the Remote Address Settings, or remove it and create a new one.

When you set up a connector as described in this section, Exchange Server 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 is the correct setup to ensure all incoming traffic is scanned.

1. On the Mail Flow window, click **receive connectors**.
2. To start the Connector wizard, click the plus symbol **+.**

3. On the Name window, enter a name and choose **Partner** connector. Click Next.



new receive connector

This wizard will create a Receive connector.

There are five types of Receive connectors. Each connector has different permissions and authentication methods. Learn more...

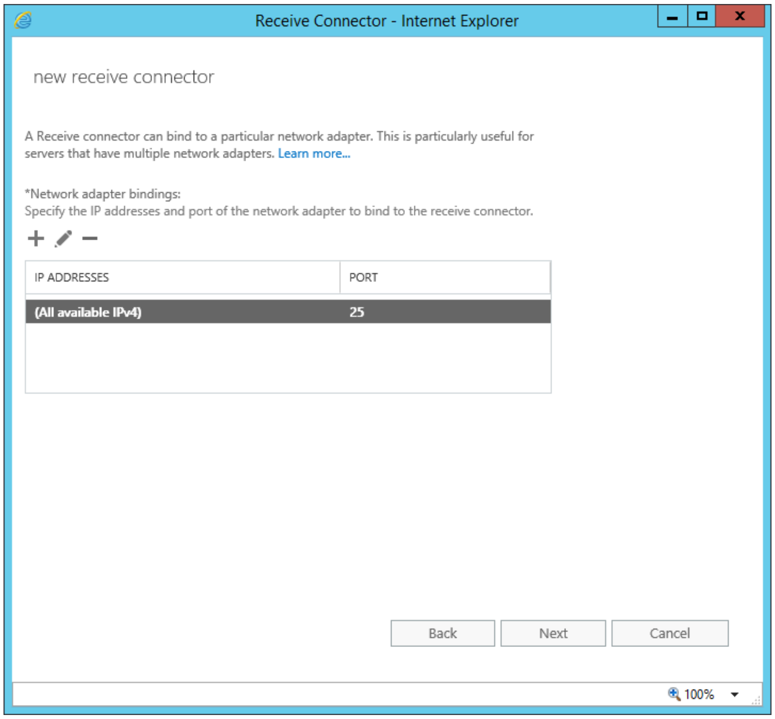
*Name: Accept from SEG Cloud

Server: WIN-2KEE0HOFMM6.doc.example.local

Role:
● Hub Transport
○ Frontend Transport

Type:
○ Custom (For example, to allow application relay)
○ Internal (For example, to receive intranet mail)
○ Internet (For example, to receive internet mail)
● Partner (For example, to route mail from trusted third-party servers)
○ Client (For example, to receive mail from non-Outlook clients)

4. On the Network adapter bindings window, specify the IPv4 addresses where you want to accept mail from MailMarshal Cloud. In most cases you can select **All available IPv4** and port **25**. Click **Next**.



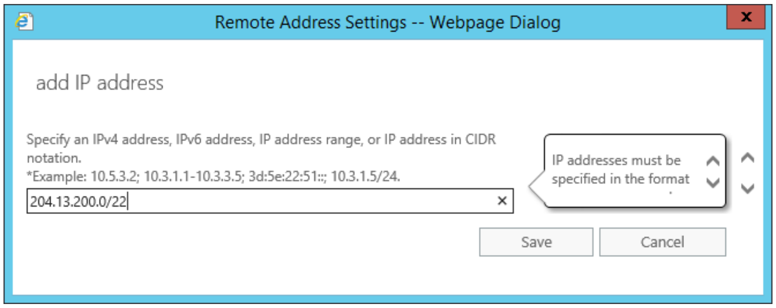
new receive connector

A Receive connector can bind to a particular network adapter. This is particularly useful for servers that have multiple network adapters. Learn more...

*Network adapter bindings:
Specify the IP addresses and port of the network adapter to bind to the receive connector.

IP ADDRESSES	PORT
(All available IPv4)	25

5. On the **Remote network** settings window, select the default entry and then click the – symbol to remove it. Click **+** to add an IP address.
6. On the **Remote Address Settings** window, enter the IP address range of the MailMarshal Cloud servers and then click **Save**. For details of the configuration data required, see MailMarshal Cloud Knowledgebase article Q21095, [MailMarshal Cloud Connection Details]() (follow links for instances other than the US instance).



Remote Address Settings -- Webpage Dialog

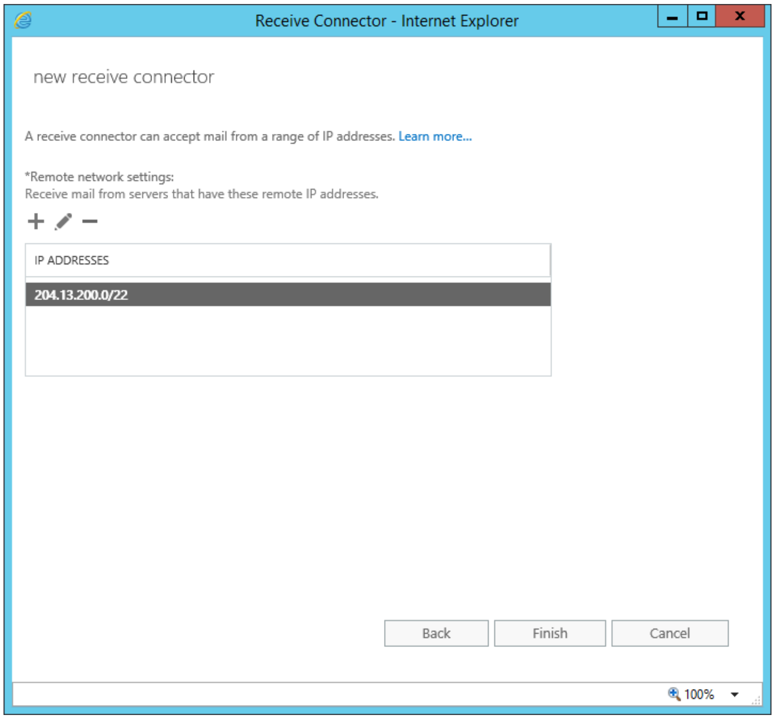
add IP address

Specify an IPv4 address, IPv6 address, IP address range, or IP address in CIDR notation.
*Example: 10.5.3.2; 10.3.1.1-10.3.3.5; 3d:5e:22:51::; 10.3.1.5/24.

204.13.200.0/22

IP addresses must be specified in the format

7. Repeat until you have added all required ranges for your instance.
8. Click **Finish** to save the connector.



Receive Connector - Internet Explorer

new receive connector

A receive connector can accept mail from a range of IP addresses. Learn more...

*Remote network settings:
Receive mail from servers that have these remote IP addresses.

IP ADDRESSES
204.13.200.0/22

5 Set up the MailMarshal Connector Agent for your Active Directory

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.

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

Tip: You can also use the Connector Agent with Azure AD. For details, see the document *Using MailMarshal Cloud with Exchange Online*.

About LevelBlue

LevelBlue reduces risk and builds lasting resilience so organizations can innovate and advance their mission with confidence. As the world's most analyst-recognized and largest pure-play managed security services provider, LevelBlue elevates client outcomes that matter: stronger defense, faster response, and sustained business continuity. LevelBlue combines AI-powered security operations, advanced threat intelligence, and elite human expertise to provide the most comprehensive portfolio of strategic advisory, managed security, offensive security, and incident response services