WatchGuard Email Protection

Quick Start Guide

Content

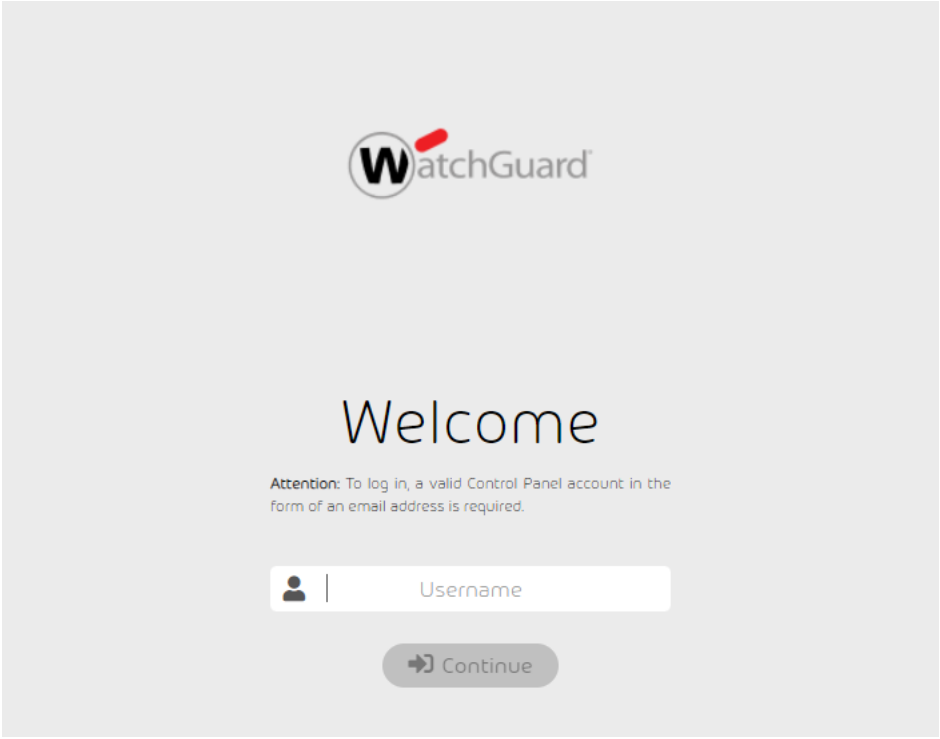
First Steps

Welcome to the WatchGuard Email Protection Quick Guide. In this document, you will be guided through the complete WatchGuard Email Protection onboarding process.

Log In to the Control Panel

You can access the Control Panel from Panda Cloud, Panda Partner Center, or by typing the URL of the Control Panel website into your browser: https://emailprotection.watchguard.com.

After you have accessed the website, the following login page appears:



Enter the credentials your received by email. Remember to change the password after the first login to the Control Panel.

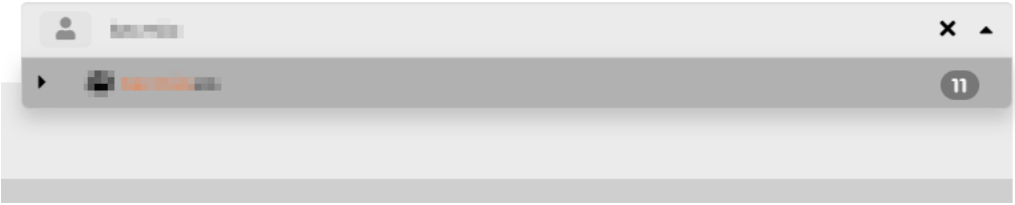
Click **Continue**.

Access Your Customer Account

These steps describe how to access your new customer account and set up filtering.

You can access the administration guides at any time from the Control Panel.

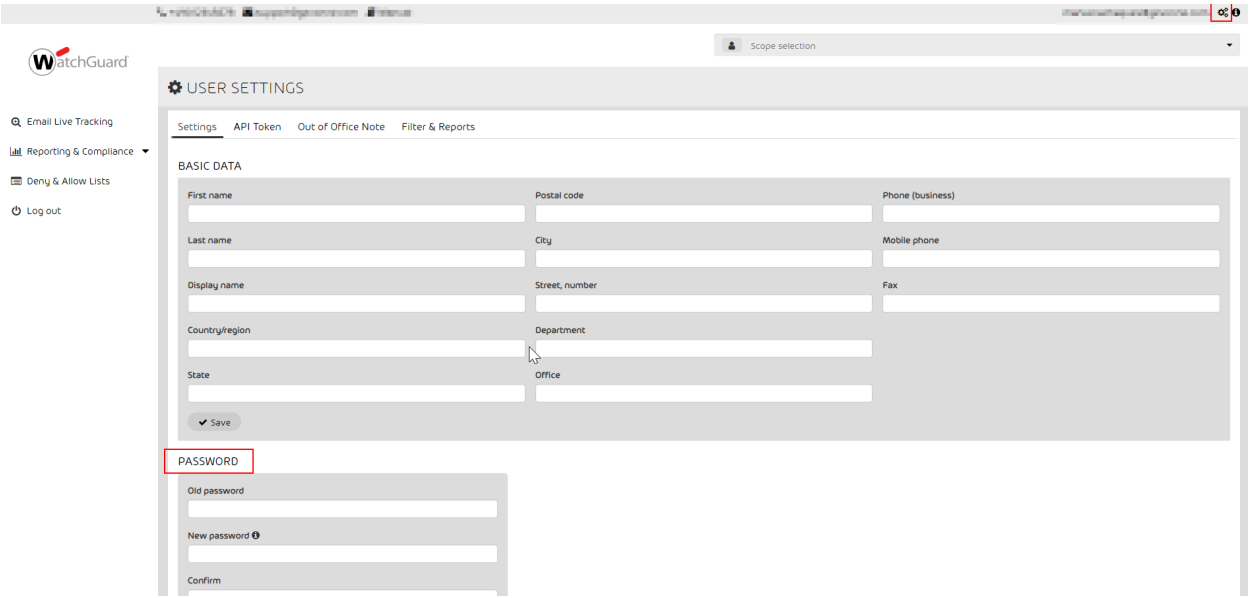
1. Navigate to the domain selection option in the upper-right corner.



2. Select your customer account.

Reset the Password

To reset the password after the first login to the Control Panel, click the **Personal Settings** button in the upper-right corner. Go to the **Password** section.

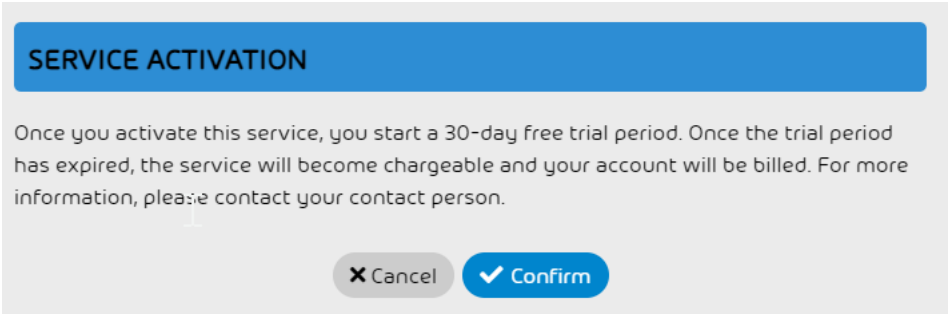


Set Up Spam and Malware Protection

To enable and set up filtering for the newly created domain, follow these steps.

1. Navigate to **Security Settings** on the left side.
2. Select the Spam and Malware Protection service. A page opens. Configure filtering for your new domain. You can adjust it here at any time later.
3. Click **Activate Spam and Malware Protection** under **Primary Environment Settings**.

A dialog box opens. Select **Confirm**.



Enabling this feature unlocks **Primary Environment Settings** and **Email Filter Settings**.

After you enable **Spam and Malware Protection**, further settings are made available under **Primary Environment Settings**.

Primary Environment Settings

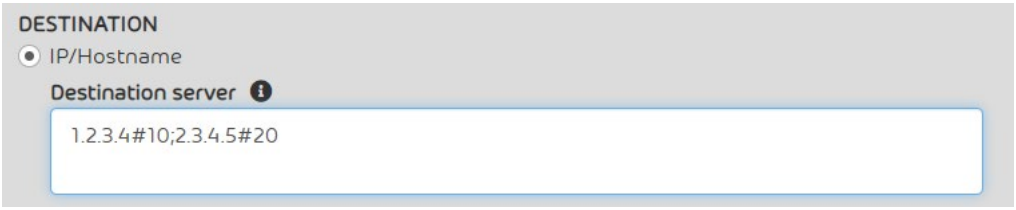
Under **Primary Environment Settings**, you can specify the destination of incoming email messages, define relay IP addresses to filter outgoing email, activate bounce management, and set up user check.

For a detailed description of these steps, see section Primary Environment Settings in the manual.

Specify the Destination of Incoming Email Messages

Under **Destination**, define the IP address or host name of the server to which email messages are to be transferred after filtering.

Several IP addresses or host names can be entered. Pay attention to the specified syntax.

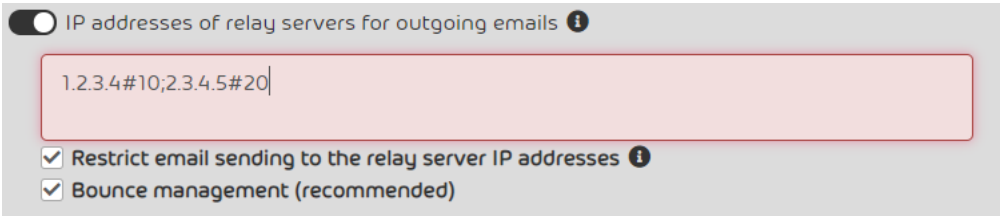


The next step is to configure the outgoing email traffic.

Define Relay IP Addresses for Outgoing Email Messages

Under **IP addresses of relay servers for outgoing emails**, enable filtering of outgoing email messages.

1. Enter one or more IP addresses. You must enter all sending IP addresses. Pay attention to the syntax.

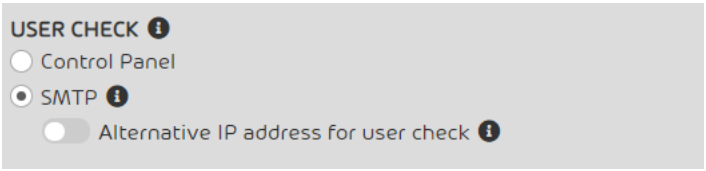


2. Enable **Bounce Management**.

Set Up User Check

During user check, the system checks whether the recipient address of an incoming email message exists and is valid.

This option is selected under the **User Check** section.



- **Control Panel**: If you select this check box, Spam and Malware Protection checks whether the recipient address is listed in the Control Panel user list.
- **LDAP**: If you select this check box, Spam and Malware Protection checks whether the recipient address is listed in your directory service.
- **SMTP**: If you select this check box, Spam and Malware Protection checks the recipient address by using an SMTP callback. To do this, Spam and Malware Protection asks the destination server of the recipient address whether the recipient address is valid. Usually, the destination server is determined based on the domain part. If you want to use other destination servers for the user check with SMTP, enable **Alternative IP address for user check** and enter the IP address in the text box.

Select one of the options. Click **Save.**

Email Authentication

Email Authentication provides different methods to authenticate email senders. You can authenticate email senders using the following methods:

- SPF (Sender Policy Framework) check (see SPF Check)
- DKIM (DomainKeys Identified Mail) validation and DKIM signing (see DKIM Validation and DKIM Signing)
- DMARC (Domain-based Message Authentication, Reporting and Conformance) validation (see DMARC Validation)

Before you set up these methods, check whether the DNS settings of your domains are correctly configured (see Check the DNS Settings of Your Own Domains).

We strongly recommend that you enable SPF check after setting up an SPF record in your DNS.

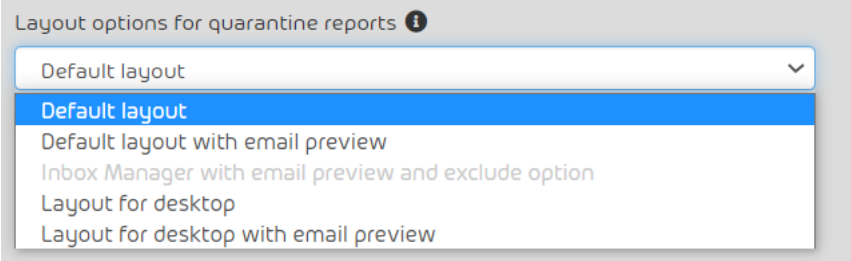
Add Quarantine Report

The Quarantine Report is an email message that is sent to users of the WatchGuard Email Protection filtering systems at different times.

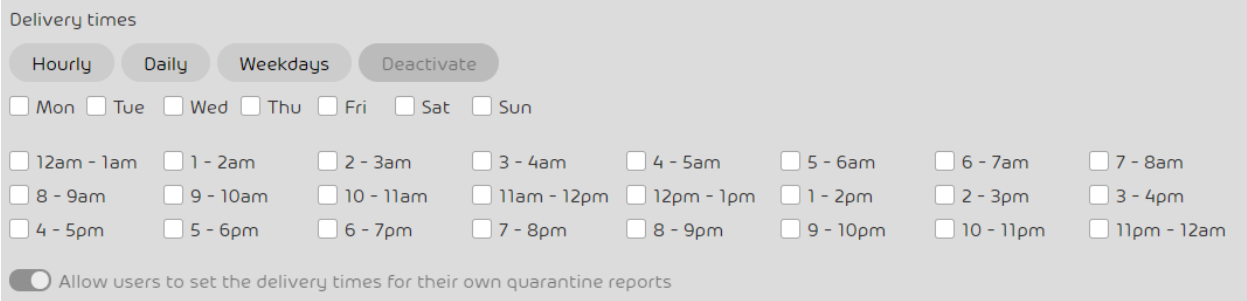
This report contains a list of email messages that have been quarantined since the last Quarantine Report.

1. Select **Security Settings**. Select **Quarantine Report**.
2. Click the **Activate Quarantine Report** button.

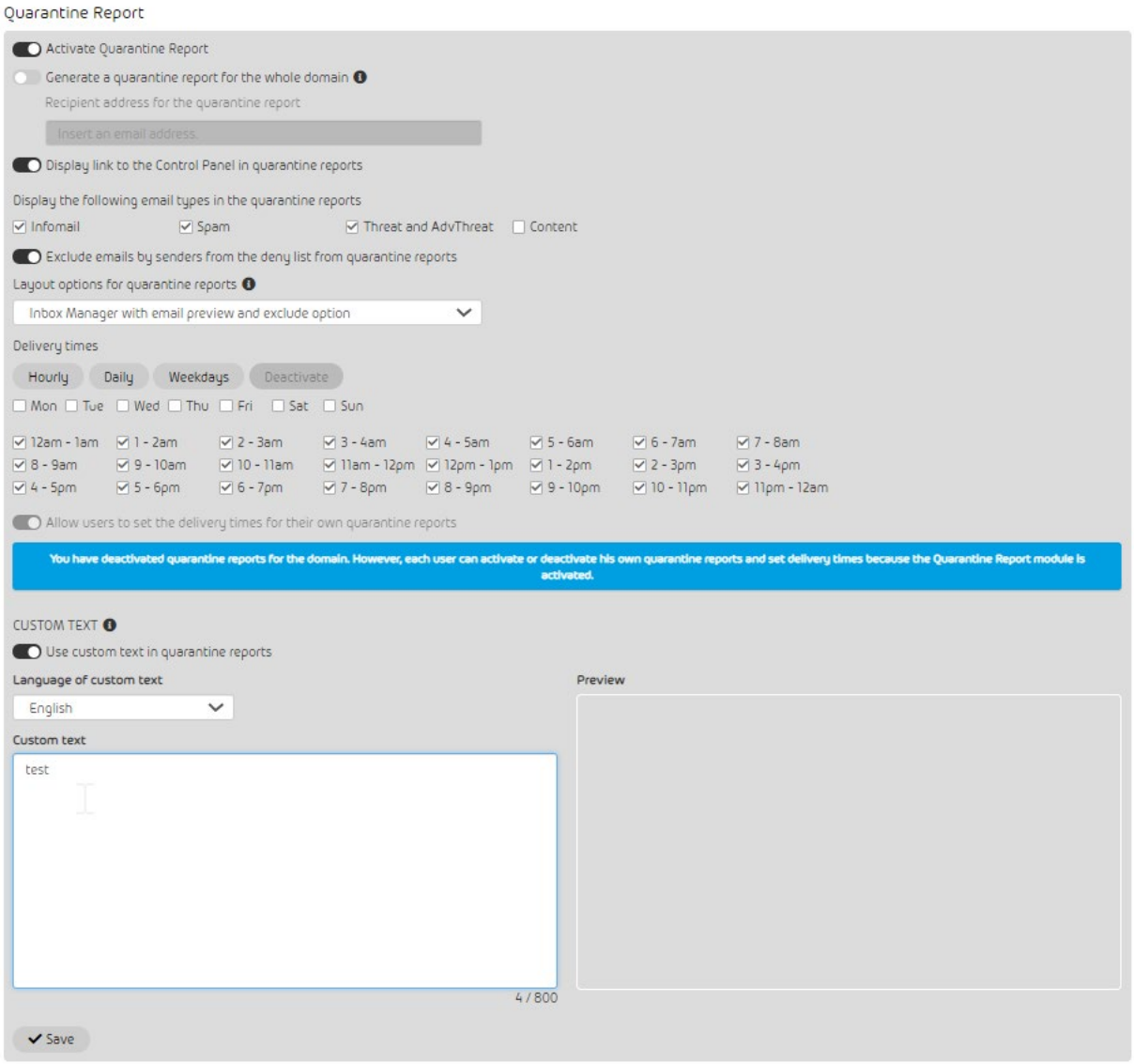
3. OPTIONAL: Select the corresponding check box if you want to **Generate a Quarantine Report for the whole domain**. Under **Recipient address for the Quarantine Report**, enter the email address that should receive the report.
4. 4. Under **Layout options for quarantine reports**, select a quarantine report layout.



5. Under **Delivery Times**, set the times at which the Quarantine Report should be delivered.



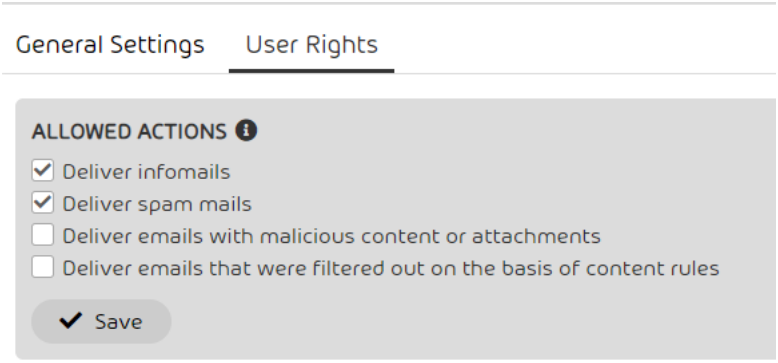
If you are satisfied with your selections, go to **Check the Control Panel Settings.**



Allow and Deny User Actions

In the **Email Live Tracking** module and in **Quarantine Reports**, users have actions available to have email messages delivered to them that have been intercepted by Spam and Malware Protection.
You can allow or deny these actions.

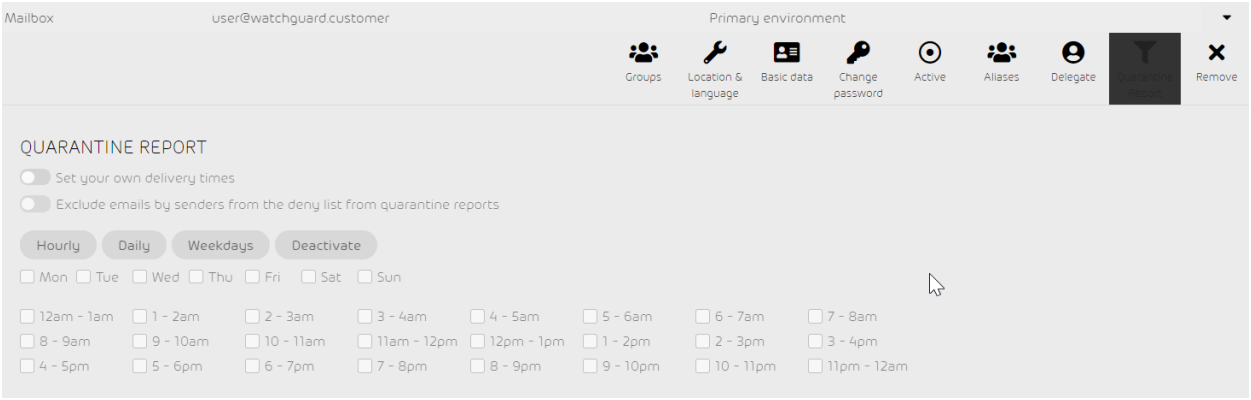
1. Select the **User Rights** tab.



2. Under **Allowed Actions**, select the check boxes of the actions you want to allow domain users to perform.
   Click **Apply changes**.
3. Click **Save**.

If you want to apply these settings to a user or a mailbox, follow these steps.

1. Navigate to **Customer Settings**. Navigate to **Mailboxes**.
2. Click the menu arrow next to the mailbox you want to edit.
3. Click the **Filter & Reports** button.



4. Select when you want to send the Quarantine Report to the user or mailbox.
5. Click the **Save** button.

Check the Control Panel Settings

Before you configure the firewall settings and change the MX records, it is very important that you check the following Control Panel settings.
Check the following settings once again:

- Alias domain settings
- Target IP address or host name
- Relay IP address
- Mailboxes
- User check

Please note that an incorrect configuration of the listed items can lead to the rejection of email messages.

After all these settings have been configured, you can configure the firewall and MX records.

Firewall Configuration

Your firewall should be tested to check whether email delivery is actually possible.
A correctly configured firewall also prevents the delivery of spam directly from the Internet. The following IP ranges must be allowed for mail traffic:

1. Range: **83.246.65.0/24** with subnet mask **255.255.255.0**, corresponding to addresses between **83.246.65.1** and **83.246.65.255**.
2. Range: **94.100.128.0/20** with subnet mask **255.255.240.0**, corresponding to addresses between **94.100.128.1** and **94.100.143.255**.
3. Range: **173.45.18.0/24** with subnet mask **255.255.255.0**, corresponding to addresses between **173.45.18.1** and **173.45.18.255**.
4. Range: **185.140.204.0/22** with subnet mask **255.255.252.0**, corresponding to addresses between **185.140.204.1** and **185.140.207.255**.

If you have set up the firewall correctly, you can now adjust the MX records.

MX Record Conversion

In this step, the MX records are converted to those of WatchGuard Email Protection.
With this change, all email messages to your domain are forwarded to the WatchGuard Email Protection platform.

Make sure to completely remove the MX records that have been stored in your domain so far!
The WatchGuard Email Protection MX records for EMEA customers are:

MX 10 mx01.hornetsecurity.com

MX 20 mx02.hornetsecurity.com

MX 30 mx03.hornetsecurity.com

MX 40 mx04.hornetsecurity.com

The WatchGuard Email Protection MX records for US customers are:

MX 10 mx-cluster-usa01.hornetsecurity.com

MX 20 mx-cluster-usa02.hornetsecurity.com

MX 30 mx-cluster-usa03.hornetsecurity.com

MX 40 mx-cluster-usa04.hornetsecurity.com

If you cannot configure this yourself, we recommend that you contact the corresponding DNS provider.

Set Up Email Relay

The prerequisite for setting up email relay is that the corresponding option has been enabled in the Control Panel and one or more IP addresses have been stored there.
For relaying, WatchGuard Email Protection uses a host name cluster with various connected load balancers.
The address to be used for EMEA customers is:

relay-cluster-eu01.hornetsecurity.com

The address to be used for US customers is:

relay-cluster-usa01.hornetsecurity.com

Set Up the SPF Record

We recommend that you store a TXT entry in your DNS settings, thus configuring an SPF record.
With such an entry, you can prevent deception attempts such as spoofing.

Part 1:
The SPF record to be stored is
v=spf1 include:spf.hornetsecurity.com ~all
Part 2:
For additional protection, we recommend you enable the SPF filter.

1. Go to **Security Settings**->**Email Authentication** and enable SPF check. Enable the recommended SPF version1 for your domains.

For information about other versions, click this link.

After configuring the SPF record, you have finished setting up your domain.

Completion of Onboarding

You have now finished setting up your customer domain.

Inbound and outbound email messages are now checked by WatchGuard Email Protection and your domain is protected.

With the configurations you have performed, you have fulfilled the prerequisites to activate more services from WatchGuard Email Protection.

After activating **WatchGuard Email Protection**, now you can activate the following services as well:

- Content Control
- Compliance Filter
- Primary Environment Settings
- Continuity Service (ignore the 30-day trial pop-up message, as this service is included in your license)

We hope you found this onboarding guide useful. Thank you for implementing the service.