Trend Micro™ Email Security

Administrator's Guide

Stop advanced email threats and spam before they reach your network

Document Part No.: APEM09974/250113

Release Date: May 20, 2025

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the service and/or provides installation instructions for a production environment. Read through the documentation before installing or using the service.

Detailed information about how to use specific features within the service may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Email Security collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Email Security collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Chapter 4: Managing domains

Chapter 5: Inbound and outbound protection

Chapter 6: Configuring policies

Chapter 7: Understanding quarantine

Chapter 8: Logs in Trend Micro Email Security

Chapter 9: Reports

Chapter 10: Configuring administration settings

Appendix A: FAQs and instructions

Appendix B: Technical support

Index

Pre-release disclaimer

In Trend Micro Email Security, some of the new features are released as "Pre-release"; therefore, the features are not an official release and are EXCLUDED from SLA warranties, if applicable. You acknowledge that the Pre-release features have not been released for production use, and as such, the Pre-release features may have errors or other operating deficiencies. The Pre-release features are provided “AS IS”, “WITH ALL FAULTS”, AND WITHOUT ANY WARRANTIES, GUARANTEES, OR CONDITIONS OF ANY KIND. YOUR USE OF PRE-RELEASE FEATURES ARE AT YOUR OWN RISK. Customers should review Pre-release features in a non-production environment. Customers can contact the Trend Micro Technical Support team while they are testing a Pre-release feature. We will review all customer feedback, requirements and scenarios in order to plan a proper enhancement in the future official general release. Furthermore, the Pre-release features may move from the "Pre-release" status to an official general release if certain improvements are made based on customers’ feedback or other internally-generated processes, but keep in mind that SOME or ALL Pre-release features may never be made available for general release by Trend Micro at its sole discretion.

There is no additional charge for pre-release features before official release, but features will not necessarily remain free after official release. If Trend Micro determines that such feature will be officially released, you may be required to pay to continue using the Trend Micro Email Security feature. We will notify you at least 30 days before official release or any upcoming charge. If you do not want to be charged, please discontinue use by opting out of the feature from Platform Directory before official release.

Chapter 1

About Trend Micro Email Security

Trend Micro Email Security is an enterprise-class solution that delivers continuously updated protection to stop phishing, ransomware, Business Email Compromise (BEC) scams, spam and other advanced email threats before they reach your network. It provides advanced protection for Microsoft™ Exchange Server, Microsoft 365, Google™ Gmail, and other cloud or on-premises email solutions.

Using Trend Micro Email Security, mail administrators set up policies to handle email messages based on the threats detected. For example, administrators can remove detected malware from incoming messages before they reach the corporate network or quarantine detected spam and other inappropriate messages.

Furthermore, Trend Micro Email Security delivers Email Continuity against planned or unplanned downtime events, which allows end users to continue sending and receiving email messages in the event of an outage.

What's new

The following new features are available in Trend Micro Email Security.

TABLE 1-1. New Features in This Release (Available on May 20, 2025)

FEATURE	DESCRIPTION
Enhanced Security Check Management for Approved Senders	Trend Micro Email Security extends its Bypass Checks for approved senders in Sender Filter Settings. In addition to the existing Connection Filtering and Spam Filtering criteria, this enhancement allows administrators to determine whether to apply security risks and anomalies scanning on emails from approved senders. This provides a more comprehensive and robust security framework, ensuring that even approved senders are subject to advanced threat detection and mitigation.
Enhanced File Scanning with Virtual Analyzer Nominated by Correlated Intelligence	Trend Micro Email Security allows administrators to decide whether to send files that are identified as suspicious by Correlated Intelligence to Virtual Analyzer for further analysis. Administrator can also specify the security level for configured actions based on Virtual Analyzer's scan results. This feature enhances file scanning robustness, ensuring more thorough threat detection and improved security. This feature is available only in the Trend Micro Email Security Advanced license.

TABLE 1-2. New Features Available on April 18, 2025

FEATURE	DESCRIPTION
Detection Signal Customization for Correlated Intelligence	In addition to predefined detection signals for Correlated Intelligence, Trend Micro Email Security allows administrators to define custom signals by using predefined conditions to meet specific security needs. These custom signals can then be incorporated into correlation rules, enhancing the detection capabilities of Trend Micro Email Security within the customer's unique environment.
Phishing Simulation Integration Available for the Japan Site	Trend Micro Email Security now supports phishing simulation integration for the Japan site, letting administrators decide whether to bypass inbound protection scans for Trend Micro phishing simulation emails.

TABLE 1-3. New Features Available on February 18, 2025

FEATURE	DESCRIPTION
Enhanced Domain Management for Reports	Trend Micro Email Security allows administrators to configure report settings and view generated reports only for the domains they have permission to manage. This enhancement ensures that email traffic and threat detection data in reports are accessible only to authorized administrators, providing better control and security.
New Tokens in Notifications and Stamps for Detections by Correlated Intelligence	Trend Micro Email Security includes two new tokens - %CI_RULE_NAME% and %CI_RULE_DESC%, that administrators can use in email notifications for policy matches and in stamps inserted into the message body. These tokens help identify which security risks or anomalies have been detected by Correlated Intelligence, providing clearer and more detailed information in your email security alerts.

TABLE 1-4. New Features Available on January 13, 2025

FEATURE	DESCRIPTION
Custom Correlation Rules for Anomaly Detection Available in Correlated Intelligence	Besides the Trend Micro predefined correlation rules, administrators can add custom correlation rules based on predefined detection signals to accommodate anomaly detection requirements in their environment. Administrators can apply custom correlation rules into the Correlated Intelligence policy and view details about detected anomalies in policy events logs. Furthermore, Trend Micro Email Security offers flexibility by enabling administrators to select all or specific predefined correlation rules to detect suspicious emails and possibly unwanted emails.

TABLE 1-5. New Features Available on December 9, 2024

FEATURE	DESCRIPTION
Boost Brand Visibility with BIMI	Trend Micro Email Security enhances your DMARC enforcement with Brand Indicators for Message Identification (BIMI), allowing you to display your brand's logo in recipient inboxes. Administrators can verify if their published BIMI records are correctly set up and active, or they can create a BIMI record and preview it in the administrator console before publishing it in DNS. This feature helps increase your brand visibility and builds customer trust.

TABLE 1-6. New Features Available on November 6, 2024

FEATURE	DESCRIPTION
Extended Audit Log Query Period	Trend Micro Email Security now allows administrators to query audit logs retained for up to 180 days, instead of the previous 30 days.

TABLE 1-7. New Features Available on October 21, 2024

FEATURE	DESCRIPTION
Quarantined Email Preview Enhancement in Quarantine Digest, End User Console, and Quarantine Query Details	Trend Micro Email Security now supports enabling quarantined email preview in quarantine digest templates. This feature allows administrators to decide whether end users can preview quarantined emails in quarantine digests. The quarantine digest preview supports inline actions for improved user interaction, including options to deliver emails or approve senders. Additionally, enhancements are also made to allow end users and administrators to view HTML-rendered email content in the End User Console or the Quarantine Query Details screen.

TABLE 1-8. New Features Available on September 18, 2024

FEATURE	DESCRIPTION
Anomaly Detection with Predefined Correlation Rules in Correlated Intelligence	In addition to detecting security risks, Correlated Intelligence in Trend Micro Email Security now supports detecting anomalies that deviate from normal behaviors and may require your attention. Based on the organization's security needs, administrators can enable all or partial predefined correlation rules at three levels of aggressiveness and apply the rules to detect anomalies in Correlated Intelligence policy.
Email Recovery for Deleted Emails	Trend Micro Email Security provides Email Recovery to retain emails marked for deletion for 14 days. This allows for restoration of emails that were mistakenly deleted before they are permanently purged, which helps ensure your business continuity and reduce the risk of data loss.
URL Information Available in Forwarded Syslog Messages	Trend Micro Email Security enhances syslog forwarding by including URLs embedded in emails within the mail tracking syslog messages.

TABLE 1-9. New Features Available on August 21, 2024

FEATURE	DESCRIPTION
Correlated Intelligence for Inbound Email Threat Detection	Trend Micro Email Security launches the Correlated Intelligence policy rules for Inbound Protection that can correlate the suspicious signals found across different scanning criteria (such as Virus Scan and Spam Filtering) to enrich threat detection for email services. With Correlated Intelligence capabilities, Trend Micro Email Security also provides the reasons why an email is detected as a threat.

TABLE 1-10. New Features Available on August 12, 2024

FEATURE	DESCRIPTION
Improved Inline Action Process in Quarantine Digest Notifications	When end users click an inline action link in the quarantine digest notification, they're prompted to confirm on a dedicated page. This extra step ensures that actions are only taken with end users' explicit consent, preventing unexpected access during notification transmission.
More Granular Security Checks for Approved Senders	Trend Micro Email Security adds Bypass Checks for approved senders in Sender Filter Settings. This allows you to determine which scanning criteria in Connection Filtering and Spam Filtering policies you want to apply on emails from approved senders.

TABLE 1-11. New Features Available on June 19, 2024

FEATURE	DESCRIPTION
More Granular Analysis Results for DMARC Reports	Trend Micro Email Security allows you to view your DMARC report data by sending source, including email service, hostname, and IP address. Besides, the solution now presents more details from raw DMARC reports in a readable format, enabling you to quickly drill down and identify the threats.
Notification Enhancement	Trend Micro Email Security now supports HTML format for system notifications. You can select either predefined or custom style for HTML notifications.

TABLE 1-12. New Features Available on May 20, 2024

FEATURE	DESCRIPTION
Descriptions Added to Email Addresses in Address Groups	Due to enhancements in policy object features, you may now add descriptions for email addresses in address groups. Use email address descriptions to help better identify and manage email addresses.
Threat Name Auto-Suggest for Policy Event Log Searches	To speed up your search for policy event logs using threat names, Trend Micro Email Security automatically displays the popular threats or top threats detected in your environment, such as quishing.

TABLE 1-13. New Features Available on April 19, 2024

FEATURE	DESCRIPTION
Support for Inserting an X-Header to Messages Matching Scan Exceptions	Trend Micro Email Security allows you to leverage the action "Insert X-Header" for messages matching scan exceptions in virus scan to meet your specific needs, for example, identify the specific scan exception for subsequent processing.
Granular Log Search for IP Block List Matching	When searching the mail tracking logs for mail traffic blocked due to IP block list matching, Trend Micro Email Security allows you to conduct more granular search by separately filtering for sender IPs found in the Blocked IP Address list and the Blocked Country/Region list.
Quishing Detection for PDF	In addition to detect quishing by scanning the QR code images attached or in the email body, Trend Micro Email Security now supports quishing detection for PDF attachments after you have enabled submission of suspicious files with QR codes to Virtual Analyzer.

TABLE 1-14. New Features Available on March 20, 2024

FEATURE	DESCRIPTION
DMARC Report Analysis	Trend Micro Email Security supports analyzing the DMARC reports for your managed domains. With the report analysis results, you can easily monitor trends and identify anomalies in emails sent on behalf of your managed domains.

TABLE 1-15. New Features Available on January 22, 2024

FEATURE	DESCRIPTION
DKIM Signatures in Email Notifications and Reports	To enhance DKIM email authentication, Trend Micro Email Security includes DKIM signatures in email notifications and reports for configured managed domains and all default system domains.

TABLE 1-16. New Features Available on January 8, 2024

FEATURE	DESCRIPTION
Search by Domain Name	Trend Micro Email Security supports searching for domains added to the Domain screen.

TABLE 1-17. New Features Available on December 11, 2023

FEATURE	DESCRIPTION
Enhancements on Data Loss Prevention	Trend Micro Email Security optimizes some data identifiers and compliance templates to provide more accurate detection of unauthorized data transmission.

TABLE 1-18. New Features Available on October 20, 2023

FEATURE	DESCRIPTION
DMARC Monitoring	Trend Micro Email Security provides you visibility of the DMARC record setup for your domains, including the SPF and DKIM record setup. You can easily identify missing configurations for implementing DMARC and understand the current DMARC policy setting for domains. For details, see *Monitoring DMARC setup on page 5-54*.

TABLE 1-19. New Features Available on September 18, 2023

FEATURE	DESCRIPTION
Sender Blocking Leveraging Suspicious Objects from Trend Vision One	In addition to files and URLs, Trend Micro Email Security can synchronize the sender addresses configured with the “Block/ Quarantine” action from the Suspicious Object List in Trend Vision One. Messages from the synchronized sender addresses are directly blocked. For details, see *Configuring suspicious object settings on page 10-100*.

Feature	Description
Detection of Email Messages with Unusual Signals	Trend Micro Email Security can identify and take action on email messages that show any unusual signal indicating possible threats, such as emails from unfamiliar senders with payment related information. For details, see *Configuring unusual signal criteria on page 6-31*.
Official launch of the new administrator console	Trend Micro Email Security officially launches its new administrator console to provide users a modern and improved experience, with all the existing features unchanged. You can click the icon  in the upper-right corner to go back to the old-style console.

Table 1-20. New Features Available on August 21, 2023

Feature	Description
Minimum TLS Version for Message Delivery	To further enhance the security of TLS-based communication with a peer, Trend Micro Email Security allows you to specify the minimum TLS version that the TLS peer must use for successful message delivery. For details, see *Adding domain TLS peers on page 5-14*.

Table 1-21. New Features Available on July 20, 2023

Feature	Description
Submission of Specified Files Types to Virtual Analyzer	Instead of submitting only suspicious files to Virtual Analyzer, Trend Micro Email Security allows you to submit all files of specified types so that possible risks contained in such file types can be caught by Virtual Analyzer. For details, see *Configuring virus scan criteria on page 6-18*.
More Granular DNS Record Statuses for DKIM Signing	For the DNS records published for DKIM signing, Trend Micro Email Security shows not only whether they have been published, but also whether the records have taken effect and are ready for signing. For details, see *Adding DKIM signing settings on page 5-43* and *Editing DKIM signing settings on page 5-45*.

TABLE 1-22. New Features Available on June 15, 2023

FEATURE	DESCRIPTION
Visibility of Email Risks Reported by End Users	In Mail Tracking logs, Trend Micro Email Security allows you to search for and view the messages that have been reported by end users as spam, phishing, or not a risk through the Email Reporting add-in. For details, see *Understanding mail tracking on page 8-2*. **Note** This feature is not available at the Japan site.

TABLE 1-23. New Features Available on May 18, 2023

FEATURE	DESCRIPTION
Suspicious Objects from Trend Vision One Available in Virus and Spam Scanning	Apart from the suspicious objects from Apex Central, Trend Micro Email Security allows you to leverage the suspicious objects synchronized from Trend Vision One to enhance the capability of detecting suspicious files during virus scanning and suspicious URLs during spam scanning. For details, see *Trend Vision One on page 10-100*.
Log Details Enhancements	In Mail Tracking and Policy Event log details, Trend Micro Email Security adds the email header Reply-To and can record the display name in addition to the email address for the headers From, To, and Reply-To.
Support for Returning Delivery Time and Antispam Engine Scan Report in Log-Related REST APIs	In the API for retrieving Mail Tracking logs, Trend Micro Email Security can return the `deliveryTime` parameter indicating the time at which it sent the email message to the next hop. Moreover, the API for retrieving Policy Event logs can return the `spamReport` parameter about Antispam Engine scan details. For details, see "Trend Micro Email Security REST API Online Help".

TABLE 1-24. New Features Available on March 20, 2023

FEATURE	DESCRIPTION
New Attachment-Based Criteria for Searching Mail Tracking Logs	Trend Micro Email Security allows you to query messages with attachments when searching mail tracking logs. In addition to the SHA256 hash and status of attachments, you can specify the filename and password analysis status of attachments as the search criteria. For details, see *Understanding mail tracking on page 8-2*.
Display of the Antispam Engine Scan Details in Logs	In the mail tracking logs and policy event logs, Trend Micro Email Security allows you to view the message scan result details from the Antispam Engine. For details, see *Understanding mail tracking on page 8-2* and *Understanding policy events on page 8-14*.
Visibility of Files Violating Content Filtering in Policy Event Logs	For messages matching the attachment-based scan criteria in content filtering, Trend Micro Email Security shows the specific files that triggered the policy in policy event logs. For details, see *Understanding policy events on page 8-14*.

TABLE 1-25. New Features Available on February 14, 2023

FEATURE	DESCRIPTION
IP Address-based Exceptions for DKIM Verification and DMARC Authentication	In addition to domain names, Trend Micro Email Security allows you to specify IP addresses and CIDR blocks as ignored peers to skip DKIM verification or DMARC authentication. For details, see *Adding DKIM verification settings on page 5-39* and *Adding DMARC settings on page 5-48*.
Password Configuration for Quarantined Message Download	To protect your download of quarantined messages with a password, Trend Micro Email Security allows you to use a random password or define your own custom password. For details, see *Querying the quarantine on page 7-3*.

Feature	Description
Audit Log Enhancements	In addition to a single account, Trend Micro Email Security allows you to use all accounts as a criterion to search audit logs. Moreover, audit logs now record administrators' logout from the administrator console and end users' logout from the End User Console. For details, see *Understanding audit log on page 8-27*.

Table 1-26. New Features Available on December 13, 2022

Feature	Description
Outlook Add-in for Reporting Emails	Trend Micro Email Security launches an Outlook add-in that allows your users to report emails to Trend Micro as false positives and false negatives. The reporting helps Trend Micro Email Security provide you with more accurate detection. For details, see *Email reporting add-in for Outlook on page 10-103*. **Note** This feature is not available at the Japan site.
Scan Bypass for Trend Micro Phishing Simulations	Trend Micro Email Security provides an option to bypass all inbound protection scans for emails sent from the IP addresses of Trend Micro phishing simulation service. You can configure this feature under **Administration** > **Other Settings** > **Service Integration**. For details, see *Phishing simulation on page 10-102*. **Note** This feature is not available at the Japan site.

TABLE 1-27. New Features Available on November 28, 2022

FEATURE	DESCRIPTION
URLs Supported in the Web Reputation Approved List	In addition to domains and IP addresses, Trend Micro Email Security allows you to add URLs to the Web Reputation Approved List to bypass Web Reputation Services, Time-of-Click Protection, and Virtual Analyzer scanning. For details, see *Managing the Web Reputation approved list on page 10-6*.
Detailed Reasons for Actions Supported in Mail Tracking Log Retrieval	When you retrieve mail tracking logs through the REST API, Trend Micro Email Security returns the details about the reasons for specific actions taken on email messages. For details, see **Supported APIs** > **Logs** > **List Mail Tracking Logs** in the REST API Online Help.

TABLE 1-28. New Features Available on October 27, 2022

FEATURE	DESCRIPTION
Support for Using the Header Sender to Match Enforced Peers	In addition to envelope sender addresses, Trend Micro Email Security allows you to use the sender address in the message header for matching enforced peers in DKIM and DMARC verification for inbound messages. For details, see *Adding DMARC settings on page 5-48* and *Adding DKIM verification settings on page 5-39*.
Scanning Duration Visibility in Mail Tracking Logs	Trend Micro Email Security displays the time used for Virtual Analyzer scanning and file password analysis in mail tracking logs.

TABLE 1-29. New Features Available on September 22, 2022

FEATURE	DESCRIPTION
Time Zone Customization in Notifications and Stamps	Trend Micro Email Security allows you to customize the time zone for the %DATE&TIME% token used in notifications for rule match and stamps inserted into the message body. For details, see *Managing notifications on page 10-25* and *Managing stamps on page 10-27*.

TABLE 1-30. New Features Available on August 29, 2022

FEATURE	DESCRIPTION
Support for Multiple Entries in Log Search Boxes	Trend Micro Email Security allows you to specify multiple entries in the search criteria for mail tracking logs and policy event logs. For details, see *Understanding mail tracking on page 8-2* and *Understanding policy events on page 8-14*.
MTA-STS Support for Outgoing TLS Connections	Trend Micro Email Security supports Mail Transfer Agent - Strict Transport Security (MTA-STS) for outgoing TLS connections. For details, see *Transport Layer Security (TLS) peers on page 5-11*.
Display of File and URL Quota Usage	Trend Micro Email Security allows you to view the number of files and URLs successfully analyzed in the Virtual Analyzer Quota Usage Details chart on the dashboard and in reports. For details, see *Virtual Analyzer quota usage details on page 3-13*.

TABLE 1-31. New Features Available on July 26, 2022

FEATURE	DESCRIPTION
Support for EUC Local Account Management	Trend Micro Email Security allows you to manage EUC local accounts from a centralized location on the administrator console. For details, see *Local accounts on page 10-55*.
More Secure Password Reset for Administrators	Trend Micro Email Security uses verification codes in place of simple CAPTCHAs to verify administrators when they reset passwords on the administrator console. For details, see *Resetting local account passwords on page 2-7*.
More Secure Registration and Password Reset for End Users	Trend Micro Email Security uses verification codes in place of security questions and simple CAPTCHAs to verify end users during account registration and password reset on the End User Console. For details, see "Registering Your Account" and "Resetting Your Password" in the "Local Account Management" chapter of the End User Console Online Help.
Blank Message Body Detection	Trend Micro Email Security enhances content filtering policies to detect and take action on messages with a blank body. For details, see *Using body is blank criteria on page 6-52*.

TABLE 1-32. New Features Available on June 27, 2022

FEATURE	DESCRIPTION
Quarantined Message Download in Encrypted ZIP Package	In addition to the original email file, Trend Micro Email Security provides another option for downloading a quarantined message: a password-protected ZIP file. For details, see *Querying the quarantine on page 7-3*.
Removal of Mobile Number from Contact Information	Trend Micro Email Security removes the mobile number from the administrator's contact information on the administrator console. It's no longer necessary to provide your mobile number during provisioning and profile configuration.

TABLE 1-33. New Features Available on May 26, 2022

FEATURE	DESCRIPTION
Spoofing Detection Enhancement	As a supplement to the existing spoofing detection methods, Trend Micro Email Security adds anti-spoofing checks on the envelope sender and message header sender in content filtering. For details, see *Configuring content filtering criteria on page 6-38*.
Support for Multiple Entries in Quarantine Search Boxes	Trend Micro Email Security allows you to specify multiple senders, recipients, and reasons when searching for quarantined messages. For details, see *Querying the quarantine on page 7-3*.
More Granular Quarantine Permission Control	When you assign the read-only quarantine permissions to a subaccount, Trend Micro Email Security allows you to control whether to include the permissions for viewing quarantined message details and downloading quarantined messages. For details, see *Adding and configuring a subaccount on page 10-33*.

TABLE 1-34. New Features Available on April 25, 2022

FEATURE	DESCRIPTION
More Granular True File Type Detection for Microsoft Office Files	Trend Micro Email Security allows you to separately control true file type detection for Microsoft Office 97-2003 files (such as .doc, .ppt, .xls) and Microsoft Office files of later versions (such as .docx, .pptx, .xlsx). For details, see *Using attachment true file type criteria on page 6-49*.

TABLE 1-35. New Features Available on March 28, 2022

FEATURE	DESCRIPTION
Reverse DNS Validation	Trend Micro Email Security supports reverse DNS validation at the connection setup stage by performing PTR record lookup based on the email sending IP address. Besides, administrators can configure a list of blocked PTR domains to directly reject email messages from them. For details, see *Managing reverse DNS validation on page 5-24*.

TABLE 1-36. New Features Available on February 24, 2022

FEATURE	DESCRIPTION
Sender Filter Enhancement	Trend Micro Email Security redesigned the Sender Filter feature under Inbound Protection by providing the following enhancements: • Supporting more wildcard formats in approved or blocked sender addresses. • Allowing you to apply approved or blocked senders to all recipients in your organization. • Synchronizing approved or blocked sender lists between the administrator console and End User Console so that administrators can manage the approved or blocked senders added from the End User Console or quarantine digest mails. For details, see *Managing sender filter on page 5-2*.

TABLE 1-37. New Features Available on January 20, 2022

FEATURE	DESCRIPTION
New Account Type: Superadmin Account	Trend Micro Email Security introduces a new local account type, namely superadmin account, to ease the administrative burden of the Trend Micro Business Account. Superadmin accounts have all administrative permissions inherited from the Business Account and can perform actions on behalf of the Business Account when necessary. For details, see *Account management on page 10-29*.

Feature	Description
Support for Attaching the Original Message in Notifications for All Policy Violation Detections	In addition to writing style analysis detection, Trend Micro Email Security provides an option to attach the original message in notifications for all policy violation detections. For details, see *Managing notifications on page 10-25*.

Table 1-38. New Features Available on December 14, 2021

Feature	Description
Mail Tracking Log Enhancement	For deleted or delivered quarantined messages, Trend Micro Email Security enables you to check from mail tracking logs who took the action and the time when the action was completed.

Table 1-39. New Features Available on November 29, 2021

Feature	Description
Log Export Enhancement	Trend Micro Email Security now can export all queried mail tracking logs and policy event logs to CSV files from the log result page. For details, see *Understanding mail tracking on page 8-2* and *Understanding policy events on page 8-14*.
IP-based Control of Access to Trend Micro Email Security	IP-based access control is available to restrict access to Trend Micro Email Security. With this feature enabled, Trend Micro Email Security verifies the IP address from which the access request originates, and takes the preconfigured actions if the request originates from an unapproved IP address. For details, see *Logon access control on page 10-83*.

Table 1-40. New Features Available on October 28, 2021

Feature	Description
Quarantine Digest Template Enhancement	Trend Micro Email Security enhances its quarantine digest template by refining template text and providing a new token for your use. For details, see *Adding or editing a digest template on page 7-14*.

TABLE 1-41. New Features Available on September 9, 2021

FEATURE	DESCRIPTION
Support for Authenticated Received Chain (ARC)	Trend Micro Email Security adds support for ARC in DMARC authentication. If ARC is enabled and an ARC chain is present and validated, some legitimate messages that fail DMARC authentication due to intermediate processing will pass the authentication. For details, see *Domain-based message authentication, reporting & conformance (DMARC) on page 5-46*.
Policy Event Log Enhancement	Trend Micro Email Security enhances its policy event logs by providing more details about Virtual Analyzer scan exceptions.

TABLE 1-42. New Features Available on August 19, 2021

FEATURE	DESCRIPTION
Email Attachment Sanitizing	Trend Micro Email Security supports email attachment sanitizing for both incoming and outgoing messages. When configuring a content filtering policy, you can choose whether to set actions specifically for email messages that contain active content such as macros in Microsoft Office attachments. For details, see *Sanitizing attachments on page 6-66*.
Layout Optimization for Quarantine Digest Notifications	Trend Micro Email Security is optimized to make the layout for quarantine digest notifications more mobile-friendly.

TABLE 1-43. New Features Available on June 30, 2021

FEATURE	DESCRIPTION
Stamp Enhancement	Trend Micro Email Security further supports HTML stamps besides already supported plain text stamps. You can customize HTML stamps based on predefined styles, and view an automatic plain text version of the customized stamps in real time. For details, see *Managing stamps on page 10-27*.

TABLE 1-44. New Features Available on May 31, 2021

FEATURE	DESCRIPTION
Quarantined Message Management Enhancement	Trend Micro Email Security allows you to configure settings for end users to view quarantined messages and take action on the End User Console and in the quarantine digest notifications. In addition, quarantined message query is optimized to provide a reasonable and consistent user experience. For details, see *Configuring end user quarantine settings on page 7-8*.
Support for Wildcard Domain in Address Groups	Trend Micro Email Security supports wildcard domains for email addresses in hybrid address groups. In addition, when you search for address groups by email address, wildcard search is used instead of partial search. For details, see *Managing address groups on page 10-2*.
Keyword Expression Test Support	Trend Micro Email Security now enables you to test the keyword expression functionality when you add a new keyword expression. For details, see *Adding keyword expressions on page 10-23*
Log Search Enhancement	Trend Micro Email Security enhances its log search feature by allowing you to search mail tracking logs by sender IP address and destination IP address. For details, see *Understanding mail tracking on page 8-2*.

TABLE 1-45. New Features Available on May 14, 2021

FEATURE	DESCRIPTION
Keyword Expression Enhancement	Trend Micro Email Security is enhanced to add another match condition to the Keywords and Expressions feature under **Administration** > **Policy Objects**. With this enhancement, Trend Micro Email Security will trigger actions when the combined score of all matched keyword expressions reaches the specified threshold. For details, see *Adding keyword expressions on page 10-23*.

Feature	Description
Redirect Page Customization Support for Time-of-Click Protection	Trend Micro Email Security enhances Time-of-Click Protection settings by allowing you to customize redirect pages for suspicious, dangerous, and untested URLs in inbound messages. The redirect page customization settings apply to incoming messages of the entire organization. For details, see *Configuring time-of-click protection settings on page 5-84*.

Table 1-46. New Features Available on April 22, 2021

Feature	Description
High Profile Domains	Trend Micro Email Security allows you to add high profile domains, for example, your partners' domains or domains of famous brands, to leverage the improved Trend Micro Antispam Engine to detect cousin domains. A cousin domain looks deceptively similar to a legitimate target domain and is often used in phishing attacks to steal sensitive or confidential information from users. For details, see *High profile domains on page 5-79*.
Renaming from "Business Email Compromise (BEC)" to "High Profile Users"	With the launch of the High Profile Domains feature, Trend Micro Email Security renames the **Business Email Compromise (BEC)** menu under **Inbound Protection** to **High Profile Users** to provide a more accurate description of the feature.
Support for Enabling/ Disabling Log Retrieval	Trend Micro Email Security allows you to decide whether to retrieve policy event logs and mail tracking logs via REST APIs for third-party SIEM application integration. For details, see *Log retrieval on page 10-98*.
File Password Analysis Result Visibility in Mail Tracking Logs	Trend Micro Email Security shows the password analysis result of email attachments in mail tracking logs.
Support for %HEADERS%	Trend Micro Email Security now supports the %HEADERS% token, which will be replaced with message headers in stamps and notification body.

TABLE 1-47. New Features Available on March 30, 2021

FEATURE	DESCRIPTION
DNS-Based Authentication of Named Entities (DANE) Support for Outgoing TLS Connections	Trend Micro Email Security now supports DANE for outgoing TLS connections. For details, see *Transport Layer Security (TLS) peers on page 5-11*.
SPF Action Enhancement	Trend Micro Email Security enhances its SPF feature by allowing you to: • Tag the email subject and send a notification for email messages with a specific SPF check result (except Pass) • Use a new token in the notification template to represent the SPF check result For details, see *Adding SPF settings on page 5-33*.
License Information Optimization	Trend Micro Email Security is optimized to show all the licenses that you have purchased under **Administration** > **Other Settings** > **License Information**. In addition, a grace end date is provided in the license information.

TABLE 1-48. New Features Available on February 27, 2021

FEATURE	DESCRIPTION
Organization-Level Policy	Trend Micro Email Security is enhanced to allow you to create inbound and outbound protection policies at the organization level. These policies automatically apply to all domains in your organization including the new ones added in the future. Organization-level policies make policy management easier than otherwise. For details, see *Configuring policies on page 6-1*.
Predictive Machine Learning Support in Outbound Protection	Trend Micro Email Security adds support for Predictive Machine Learning in outbound protection, allowing you to specify Predictive Machine Learning settings in virus scan rules.
Syslog Enhancement	In addition to detection logs, audit logs and mail tracking logs, Trend Micro Email Security can now forward URL click tracking logs to syslog servers.

TABLE 1-49. New Features Available on January 28, 2021

FEATURE	DESCRIPTION
Quarantine Digest Template Enhancement	Trend Micro Email Security enhances its quarantine digest template by allowing you to: • Use two more actions: "Approve Sender Domain" and "Block Sender Domain" • Customize inline actions that are available in digest notifications • Send a test digest mail based on the configured digest template For details, see *Adding or editing a digest template on page 7-14*.
Log Search Enhancement	Trend Micro Email Security enhances its log search feature by allowing you to search policy event logs by message header address and threat name, and search mail tracking logs by message header address. For details, see *Understanding mail tracking on page 8-2* and *Understanding policy events on page 8-14*.

Service requirements

Trend Micro Email Security does not require hardware on your premises. All scanning is performed in the cloud. To access your web-based Trend Micro Email Security administrator console, you need a computer with access to the Internet.

The following are required before Trend Micro Email Security can be activated:

- An existing mail gateway or workgroup SMTP connection

  For example:

  - A local MTA or mail server
  - A cloud-based MTA solution

- Access to domain MX records (DNS mail exchanger host records) for repointing MX records to the Trend Micro Email Security MTA

  (Contact your service provider, if necessary, for more information or configuration help.)

If you have trouble accessing the site, confirm that you are using the correct web address. For details, see *Accessing the Trend Micro Email Security administrator console on page 2-2*.

If you have trouble using the site or with the way the website displays, confirm that you are using a supported browser with JavaScript enabled.

Supported browsers include:

- Microsoft Edge 91
- Mozilla Firefox 60.0 or later
- Google Chrome 67.0 or later

The Trend Micro Email Security administrator console and End User Console support the following languages. Change the locale in your browser according to your region.

Administrator Console	End User Console
• English • Japanese	• English • French • Spanish • German • Italian • Japanese • Portuguese

Features and benefits

Trend Micro Email Security provides the following features and benefits:

Sender Filter

Trend Micro Email Security allows you to filter senders of incoming email messages. You can specify the senders to allow or block using specific email addresses or entire domains and specify the type of sender addresses collected to match the approved and blocked sender lists.

For details, see *Managing sender filter on page 5-2*.

Email Reputation Services

Trend Micro Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service. Email Reputation Services use a standard IP reputation database and an advanced and dynamic IP reputation database (a database updated in real time). These databases have distinct entries, allowing Trend Micro to maintain a very efficient and effective system that can quickly respond to new sources of spam.

For details, see *Understanding IP reputation on page 5-17*.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

As an email validation system to detect and prevent email spoofing, Domain-based Message Authentication, Reporting and Conformance (DMARC) is intended to fight against certain techniques used in phishing and spam, such as email messages with forged sender addresses that appear to originate from legitimate organizations. DMARC fits into the inbound email authentication process of Trend Micro Email Security, allowing you to define DMARC policies, including the actions to take on messages that fail DMARC authentication.

For details, see *Domain-based message authentication, reporting & conformance (DMARC) on page 5-46*.

Multitiered Virus, Spam, Correlated Intelligence, and Content Filtering

Trend Micro Email Security leverages the Trend Micro Virus Scan Engine to compare the files with the patterns of known viruses and integrates Predictive Machine Learning to detect new, previously unidentified, or unknown malware through advanced file feature analysis. Trend Micro Email Security also supports integration with Virtual Analyzer, a cloud-based virtual environment designed for manage and analyze objects submitted by Trend Micro products.

To combat sophisticated attacks for enhanced inbound protection, Trend Micro Email Security leverages the Correlated Intelligence feature to correlate suspicious signals from various sources to detect phishing security risks and anomalies.

Furthermore, Trend Micro Email Security detects phishing, spam, Business Email Compromise (BEC) scams, graymail and social engineering attacks and examines the message contents to determine whether the message contains inappropriate content.

You can configure domain-level and organization-level policies to detect various security risks and anomalies by scanning email messages and then performing a specific action for each security risk detected.

For details, see *Configuring policies on page 6-1*.

Virtual Analyzer

Virtual Analyzer is a cloud sandbox designed for analyzing suspicious files and URLs. Sandbox images allow observation of files and URLs in an environment that simulates endpoints on your network without any risk of compromising the network.

Trend Micro Email Security sends suspicious files or URLs to Virtual Analyzer when a file or URL exhibits suspicious characteristics and signature-based scanning technologies cannot find a known threat. Virtual Analyzer performs static analysis and behavior simulation in various runtime environments to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings.

For details on Virtual Analyzer settings, see *Configuring virus scan criteria on page 6-18* and *Configuring Web Reputation criteria on page 6-26*.

Data Loss Prevention

Data Loss Prevention (DLP) safeguards an organization's digital assets against accidental or deliberate leakage. DLP evaluates data against a set of rules defined in policies to determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission. With DLP, Trend Micro Email Security allows you to manage your incoming email messages containing sensitive data and protects your organization against data loss by monitoring your outbound email messages.

For details, see *Data Loss Prevention on page 5-86*.

File Password Analysis

Based on user-defined passwords, Trend Micro Email Security can extract password-protected archive files and open password-protected document files in email messages to investigate any malicious or suspicious content in those messages.

For details, see *File password analysis on page 5-71*.

Suspicious Objects

Suspicious objects are objects with the potential to expose systems to danger or loss. After Trend Micro Email Security is registered to Trend Micro Apex Central, Apex Central synchronizes the suspicious object lists consolidated from its managed Trend Micro products with Trend Micro Email Security at a scheduled time interval.

For details, see *Apex Central on page 10-98*.

Email Continuity

Trend Micro Email Security provides protection against email loss if your email server goes down. If your server becomes unavailable due to a crash or network connectivity problem, Trend Micro Email Security automatically transfers inbound traffic to a backup server until your server is back online. This enables end users to read, forward, download and reply to email messages on the End User Console.

For details, see *Email Continuity on page 10-80*.

Logs and Reports

Trend Micro Email Security provides detailed logs to help you analyze system security and improve protection solutions. You can view and search logs to track messages for inbound and outbound traffic, and to track all messages for a specific sender, recipient, policy rule or detection. Trend Micro Email Security allows you to forward syslog messages to an external syslog server in a structured format, which allows third-party application integration.

For details, see *Logs in Trend Micro Email Security on page 8-1*.

Trend Micro Email Security provides reports to assist in mitigating threats and optimizing system settings. You can generate reports based on a daily, weekly, monthly or quarterly schedule.

For details, see *Reports on page 9-1*.

Message Quarantine

Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered on the administrator console. Furthermore, end users can view and manage their own quarantined messages on the End User Console.

For details, see *Understanding quarantine on page 7-1*.

Available license versions

Starting from October 31, 2019, Trend Micro Email Security Standard is available in addition to Trend Micro Email Security Advanced.

Trend Micro Email Security Standard includes a subset of features available in Trend Micro Email Security Advanced to deliver essential email protection for cloud or on-premises email solutions. Trend Micro Email Security Advanced includes all the features of the standard version and provides more advanced and enhanced functionality.

The following table summarizes the feature differences between the two license versions.

Note

The features that are common to both versions are not listed here.

TABLE 1-50. Feature differences

FEATURE	TREND MICRO EMAIL SECURITY STANDARD	TREND MICRO EMAIL SECURITY ADVANCED
Virtual Analyzer	No	Yes (both URL and file analysis)
Email continuity	No	Yes
Writing style analysis for Business Email Compromise (BEC) threat detection	No	Yes
File password analysis	No	Yes
Virtual Analyzer scan exceptions	No	Yes
Virtual Analyzer submission quota exceptions	No	Yes
DMARC Report Analysis	No	Yes
Sliding window for mail tracking log search	30 days	60 days
Sliding window for policy event log search	30 days	60 days
Message size limit	50 MB	150 MB
Suspicious file nomination by Correlated Intelligence to submit to Virtual Analyzer	No	Yes

The features of Trend Micro Email Security Standard and Trend Micro Email Security Advanced are controlled by the license applied. There are two ways to manage your license:

- From the Licensing Management Platform

  The Licensing Management Platform allows partners to self-provision and auto-renew licenses. Contact your reseller or MSP to add, renew or extend your licenses.

- From the Customer Licensing Portal

  Visit the Customer Licensing Portal website at https://clp.trendmicro.com and activate, register and manage your products on the portal. For details, see the supporting documentation at:

  http://docs.trendmicro.com/en-us/smb/customer-licensing-portal.aspx

If you have purchased the standard version and want to upgrade to Trend Micro Email Security Advanced, do the following:

1. Log on to the Customer Licensing Portal website (https://clp.trendmicro.com).
2. From the Customer Licensing Portal page, click **Provide Key**.
3. Provide your activation code and click **Continue**.

   Your version will then be upgraded to Trend Micro Email Security Advanced.

Data center geography

Trend Micro Email Security is hosted on Amazon AWS data centers, and its cloud sandbox service is hosted in different regions based on each Trend Micro Email Security serving site.

The following table lists the geographic location of data centers for each Trend Micro Email Security site.

Trend Micro Email Security Site	Amazon Data Center Location / Region	Cloud Sandbox Data Center Location / Region
North America, Latin America and Asia Pacific	Northern Virginia / US East	Northern Virginia / US East
Europe and Africa	Frankfurt / Germany	Frankfurt / Germany
Australia and New Zealand	Sydney / Australia	Northern Virginia / US East
Japan	Tokyo / Asia Pacific	Tokyo / Asia Pacific
Singapore	Singapore / Asia Pacific	Singapore / Asia Pacific

Trend Micro Email Security Site	Amazon Data Center Location / Region	Cloud Sandbox Data Center Location / Region
India	Mumbai / South Asia	Pune / Central India
Middle East (UAE)	UAE / Middle East	UAE / Middle East

Inbound message protection

Trend Micro Email Security provides inbound message protection by evaluating email messages in the following order:

- Connection filtering

  Provides the recipient filter, sender filter, Transport Layer Security (TLS) check, and IP Reputation settings.

- Domain-based authentication

  Provides authentication methods such as Sender IP Match, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect against email spoofing.

- Virus scan

  Allows you to configure virus policies and scan exceptions.

- Spam filtering

  Allows you to configure spam policies, high profile users for BEC policies and Time-of-Click Protection settings.

- Correlated Intelligence

  Allows you to configure Correlated Intelligence policies to detect phishing security risks and anomalies by correlating signals across different sources.

- Content filtering

  Allows you to configure content filtering policies to take actions on messages based on the conditions matched.

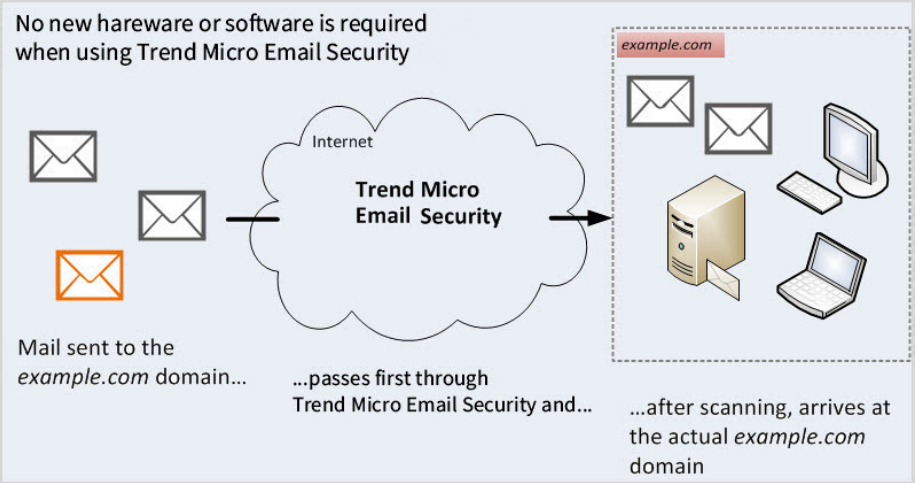
- Data Loss Prevention

  Allows you to create Data Loss Prevention (DLP) policies to manage your incoming email messages containing sensitive data.

Inbound message flow

Trend Micro Email Security will first scan incoming email messages before final delivery to the “example.com” Inbound Server.

The flow of messaging traffic from the Internet, through the Trend Micro Email Security, and then to the “example.com” Inbound Server, or local MTA.



Evaluation is done in the following order:

1. The originating MTA performs a Domain Name Service (DNS) lookup of the MX record for “example.com” to determine the location of the “example.com” domain.

   The MX record for “example.com” points to the IP address of the Trend Micro Email Security instead of the original “example.com” Inbound Server.

2. The originating MTA routes messages to Trend Micro Email Security.
3. The Trend Micro Email Security accepts the connection from the originating mail server.
4. Trend Micro Email Security performs connection-based filtering at the MTA connection level to decide on an action to take. Actions include the following:
    - Trend Micro Email Security terminates the connection, rejecting the messages.
    - Trend Micro Email Security accepts the messages and filters them using content-based policy filtering.
5. Trend Micro Email Security examines the message contents to determine whether the message contains malware or any other threats.
6. Assuming that a message is slated for delivery according to the policies, the Trend Micro Email Security routes the message to the original "example.com" Inbound Server.

Outbound message protection

Trend Micro Email Security scans outgoing email messages before delivery if outbound filtering is enabled. Trend Micro Email Security applies the following policies for filtering:

- Malware (viruses, spyware, and so on)
- Spam and phishing
- Web reputation
- Data Loss Prevention (DLP)
- Transport Layer Security (TLS) check
- DomainKeys Identified Mail (DKIM) signing

In addition, outbound encryption is seamlessly integrated with the content-filtering capabilities of Trend Micro Email Security, using policy-based encryption to secure email messages. The service does not automatically encrypt email messages. When outbound filtering is enabled, outbound

encryption appears as a policy option within the Trend Micro Email Security administrator console. You will need to configure policy rules that apply encryption as a rule action.

To learn about the policy rule used to encrypt outbound messages, see *Encrypting outbound messages on page 6-73*. To learn more about how to enable outbound protection for a managed domain, see step 5 in *Adding a domain on page 4-4*.

Trend Micro Email Security evaluates outgoing messages against regulatory compliance templates defined in DLP policies to prevent data leakage. For details about DLP, see *Data Loss Prevention on page 5-86*.

Integration with Trend Micro products

For seamless integration, make sure that the Trend Micro products or services that integrate with Trend Micro Email Security run the required or recommended versions.

TABLE 1-51. Trend Micro Products that Integrate with Trend Micro Email Security

PRODUCT/SERVICE	VERSION
Apex Central	2019
Control Manager	7.0 with hot fix HF2964

Apex Central

Apex Central™ is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Apex Central web-based management console provides a single monitoring point for managed products and services throughout the network.

Apex Central allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Apex Central allows both manual and pre-scheduled updates, and the

configuration and administration of products as groups or as individuals for added flexibility.

If Trend Micro Email Security is managed from Apex Central, you can use single sign-on to access the Trend Micro Email Security administrator console and check the connection status of registered Trend Micro Email Security servers.

Registering to Apex Central

Make sure you have a Customer Licensing Portal account and your account has been bound both with Trend Micro Email Security and Apex Central.

Procedure

1. Open the Apex Central management console.
2. Go to **Administration** > **Managed Servers** > **Server Registration**.
3. On the screen that appears, select **Trend Micro Email Security** as **Server Type**.
4. Click **Cloud Service Settings**.
5. Specify your Customer Licensing Portal account credentials and click **OK**.

   The Trend Micro Email Security server appears in the server list.

   You can click the server address to single sign-on to the Trend Micro Email Security administrator console.

Checking Trend Micro Email Security server status

Procedure

1. Go to **Dashboard**.
2. Click the **Summary** tab.
3. Scroll down and find the **Product Connection Status** widget.

You can check the status of any Trend Micro Email Security server registered with Apex Central.

Unregistering from Apex Central

Procedure

1. Go to **Administration** > **Managed Servers** > **Server Registration**.
2. Click **Cloud Service Settings**.
3. Click **Stop managing services with Apex Central**.
4. In the dialog box that appears, click **Yes**.

   The Trend Micro Email Security server disappears from the server list.

Remote Manager

Trend Micro Remote Manager is a robust console that works in parallel with the Customer Licensing Portal and the Licensing Management Platform to provide managed security services to small and medium businesses.

Remote Manager enables you to monitor the health of multiple managed networks through multiple, managed products and services. Remote Manager allows reseller administrators to issue commands to manage critical aspects of network security.

Trend Micro Email Security is one of the products that Remote Manager monitors and manages.

- If you are using Licensing Management Platform accounts, contact your reseller to connect to or disconnect from Remote Manager.
- If you are using Customer Licensing Portal accounts, you can connect to or disconnect from Remote Manager on the Trend Micro Email Security administrator console.

  For details, see *Remote Manager on page 10-102*.

Chapter 2

Getting started with Trend Micro Email Security

Accessing the Trend Micro Email Security administrator console

Choose the proper way to access the Trend Micro Email Security administrator console based on your licensing agreement with Trend Micro.

TABLE 2-1. Accessing the Trend Micro Email Security administrator console

ACCOUNT TYPE	LOGON METHOD
Customer Licensing Portal account	Log on directly to your administrator console at the following web address for your region: • North America, Latin America and Asia Pacific: https://tm.tmes.trendmicro.com • Europe and Africa: https://tm.tmes.trendmicro.eu • Australia and New Zealand: https://tm.tmes-anz.trendmicro.com • Japan: https://tm.tmems-jp.trendmicro.com • Singapore: https://tm.tmes-sg.trendmicro.com • India: https://tm.tmes-in.trendmicro.com • Middle East (UAE): https://tm.tmes-uae.trendmicro.com

Account Type	Logon Method
	 **Note** Customer Licensing Portal helps you manage your accounts, customer information, and subscriptions. You can directly access the web consoles of Trend Micro solutions including Trend Micro Email Security. For details about how to log on to, register and manage Trend Micro Email Security using Customer Licensing Portal, see the Customer Licensing Portal documentation at http://docs.trendmicro.com/en-us/smb/customer-licensing-portal.aspx.

Account Type	Logon Method

Licensing Management Platform account	For Licensing Management Platform resellers, substitute your Tenant ID for `<tenant-id>` in the following web address for your region:
	• North America, Latin America and Asia Pacific:
	`https://<tenant-id>.tmes.trendmicro.com`
	• Europe and Africa:
	`https://<tenant-id>.tmes.trendmicro.eu`
	• Australia and New Zealand:
	`https://<tenant-id>.tmes-anz.trendmicro.com`
	• Japan:
	`https://<tenant-id>.tmems-jp.trendmicro.com`
	• Singapore:
	`https://<tenant-id>.tmes-sg.trendmicro.com`
	• India:
	`https://<tenant-id>.tmes-in.trendmicro.com`
	• Middle East (UAE):
	`https://<tenant-id>.tmes-uae.trendmicro.com`

Account Type	Logon Method
Local accounts added by the administrator	• North America, Latin America and Asia Pacific: https://ui.tmes.trendmicro.com • Europe and Africa: https://ui.tmes.trendmicro.eu • Australia and New Zealand: https://ui.tmes-anz.trendmicro.com • Japan: https://ui.tmems-jp.trendmicro.com • Singapore: https://ui.tmes-sg.trendmicro.com • India: https://ui.tmes-in.trendmicro.com • Middle East (UAE): https://ui.tmes-uae.trendmicro.com **Note** If you forget your local account password, reset the password by referring to *Resetting local account passwords on page 2-7*.
SSO accounts	Log on to the administrator console at the URL generated in Step 4 in *Configuring single sign-on on page 10-42*.

From the Trend Micro Email Security administrator console, administrators can create reports, view logs, perform administrative tasks, and configure security policies against different types of threats.

The Trend Micro Email Security administrator console provides the following features:

- Chart-based dashboard
- Domain management
- Inbound and outbound protection settings
- Quarantined message query and quarantine digest settings
- Mail tracking, policy event, URL click tracking and syslog settings
- Daily, weekly, monthly and quarterly reports
- Centralized administration settings, including:
  - Policy objects
  - Suspicious objects
  - Email continuity settings
  - Administrator management
  - End user management
  - Directory management
  - License information

Resetting local account passwords

Procedure

1. Access the administrator console.

   The logon screen for the Trend Micro Email Security administrator console appears.

2. Click **Forgot your Password**.

   The **Reset Password** screen appears.

3. Type the user name and email address of your local account.

4. Click **Send verification code**.

   A verification code is sent to the above specified email address.

5. Specify the verification code.

6. Specify and confirm your new password.

7. Click **Finish**.

   You can use the new password to log on to the administrator console.

Selecting a serving site for first time use

For the customers who use Trend Micro Email Security for the first time, Trend Micro Email Security allows you to choose a serving site, regardless of the registration key or activation code you have purchased. A serving site is the geographical location where Trend Micro Email Security provides you services and stores your service data.

Note

This feature is available for customers from the Customer Licensing Portal. Customers from the Licensing Management Platform cannot select a serving site for first time use, because their serving site has been specified during registration.

You cannot modify the serving site setting after the initial configuration completes. Your Trend Micro Email Security service data will always stay within your selected site and will not be transferred to other sites for data privacy and sovereignty considerations.

The steps outlined below detail how to select a Trend Micro Email Security serving site from the Customer Licensing Portal during first time use.

Procedure

1. Log on to the Customer Licensing Portal management console.

2. Go to **Products/Services**, locate **Trend Micro Email Security**, and then click **Open console** under **Action**.

   The **Initial Configuration** screen appears.

3. Select a site, click **OK** after confirming your selection, and click **Save**.

   Trend Micro Email Security uses an Amazon AWS data center to host your data at each serving site. For more information, see *Data center geography on page 1-28*.

   The Trend Micro Email Security management console opens after the initial configuration is complete.

   Check the URL of your Trend Micro Email Security management console logon page in the address bar, which is determined based on your selected serving site. For example, if you are at the Europe and Africa site, the URL of your Trend Micro Email Security management console logon page is `https://tm.tmes.trendmicro.eu`.

Provisioning a Trend Micro Business Account

After you have selected a serving site on the administrator console, Trend Micro Email Security launches a provisioning wizard for you to provision your Trend Micro Business Account.

Procedure

1. Provide your administrator profile information.

   Keep your information current because Trend Micro will send you important maintenance plans, urgent incidents and new features.

   a. Type your first name and last name.

   b. Specify your email address.

   c. Click **Next**.

      An email message will be sent to your registered email address. Check your mailbox and click the verification link in the message to verify your email address. Verifying the email address proves

that you own it and ensures that you will receive important system notifications from Trend Micro Email Security.

2. Set your company identifier.

Note

Trend Micro generates a custom subdomain for your company based on the company identifier you set. For example, if your company identifier is "example", your MX record for incoming email messages will be generated based on your location.

- North America, Latin America and Asia Pacific:

  example.in.tmes.trendmicro.com

- Europe and Africa:

  example.in.tmes.trendmicro.eu

- Australia and New Zealand:

  example.in.tmes-anz.trendmicro.com

- Japan:

  example.in.tmems-jp.trendmicro.com

- Singapore:

  example.in.tmes-sg.trendmicro.com

- India:

  example.in.tmes-in.trendmicro.com

- Middle East (UAE):

  example.in.tmes-uae.trendmicro.com

3. Add a domain you want to manage through Trend Micro Email Security.

Note

For details about adding domains, see *Adding a domain on page 4-4*.

You still need to perform further setup tasks to get Trend Micro Email Security up and running. For details, see *Setting up Trend Micro Email Security on page 2-11*.

Setting up Trend Micro Email Security

To ensure your organization achieves effective email security protection, Trend Micro recommends you perform the following tasks:

1. Configure the domain you added and add additional domains if needed.

   Check the status of the domain you added for provisioning and make sure the domain has been configured properly. Add more domains if necessary.

   For details, see *Managing domains on page 4-1*.

2. Import user directories that will be applied by policies.

   Trend Micro Email Security provides multiple ways to import user directories. Choose the proper way that suits your organization.

   For details, see *Directory management on page 10-86*.

3. Configure policies to design your organizational protection solution.

   Trend Micro Email Security provides robust email management options, enabling you to customize your email security protection and configure policies to meet the needs of your organization. Trend Micro Email Security is preconfigured with several default domain-level policies (if configured) and default organization-level policies to provide immediate protection upon deployment.

   For details, see *Configuring policies on page 6-1*.

Chapter 3

Working with the dashboard

The **Dashboard** screen displays charts for email traffic relayed through Trend Micro Email Security.

Note

The time zone of the browser accessing Trend Micro Email Security is used.

Select the data shown in charts and their corresponding thumbnail charts on the **Threats**, **Top Statistics**, or **Other Statistics** tab of **Dashboard** using the following controls and settings.

TABLE 3-1. Controls and settings

CONTROL	SETTINGS
Domain and direction of traffic	Select a domain and mail traffic direction using specific controls. **Tip** To select all domains, select **all my domains** from the **Managed domain** drop-down list.
Settings	Click the settings icon on the right of the tabs to select widgets to show on each tab as needed.

Control	Settings
Time periods	Select a time period at the top of each chart. The following are the definitions of time periods: • **Date**: The most recent eight (8) days. Days are split into hours from 0:00 to 23:59. Because days start at midnight, charts with a time period of the current day will never show a full 24 hours of data. • **Week**: The most recent eight (8) weeks. Weeks are the days from Sunday to Saturday. Because weeks start on Sunday, charts with a time period of the current week will never show a full seven (7) days of data. • **Month**: The most recent two (2) months. Months are days from the first to the last day of the calendar month. Because months start on the first, charts with a time period of the current month will never show the full month of data. • **Last 12 months**: The data for the last twelve months plus all days of the current month. Always shows more than one year of data. **Note** The specified time period only affects the data shown on the current chart and its corresponding thumbnail chart on the **Summary** tab. Changing the selection on a chart does not affect other charts.

TABLE 3-2. Specific Charts

CHART	SETTINGS
Ransomware Details **Threats** **Threats Details** **Virtual Analyzer File Analysis Details** **Virtual Analyzer URL Analysis Details** **Virtual Analyzer Quota Usage Details** **Domain-based Authentication Details**	Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

Chart	Settings
Top Business Email Compromise (BEC) Threats **Top Analyzed Advanced Threats (Files)** **Top Analyzed Advanced Threats (URLs)** **Top Malware Detected by Predictive Machine Learning** **Top Malware Detected by Pattern-based Scanning** **Top Spam** **Top Data Loss Prevention (DLP) Incidents**	Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show the total percentage of messages by value for the selected time period. Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.
Volume **Bandwidth** **Time-of-Click Protection**	Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

Threats tab

The **Threats** tab of **Dashboard** provides the information about the threats processed by Trend Micro Email Security.

Ransomware details chart

The **Ransomware Details** chart on the **Threats** tab of **Dashboard** displays the number of messages detected as ransomware by different components of Trend Micro Email Security.

Hover over **Malware Scanning** detections above the chart to view the number of threats detected by Predictive Machine Learning and the number of threats detected by pattern-based scanning.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Threats chart

The **Threats** chart on the **Threats** tab of **Dashboard** displays the total percentage of messages detected as threats.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show the total percentage of messages by value for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

TABLE 3-3. Detected Values on Charts

DETECTED VALUES	FOR INCOMING MAIL	FOR OUTGOING MAIL
Ransomware	The number of email messages containing attachments that are detected as ransomware or the URL of sites that directly or indirectly facilitate the distribution of ransomware	The number of email messages containing attachments that are detected as ransomware or the URL of sites that directly or indirectly facilitate the distribution of ransomware
Malware (Pattern-based)	The number of email messages that pattern-based scanning detected as containing a malware threat	The number of email messages that pattern-based scanning detected as containing a malware threat
Malware (PML Detected)	The number of email messages that Predictive Machine Learning detected as containing a malware threat	The number of email messages that Predictive Machine Learning detected as containing a malware threat
Suspicious Files	The number of suspicious files detected during spam scanning	The number of suspicious files detected during spam scanning
Analyzed Advanced Threats (Files)	The number of email messages containing suspected file threats detected as high risk by the Advanced Threat Scan Engine or analyzed by Virtual Analyzer as security risks	Not available
Analyzed Advanced Threats (URLs)	The number of email messages containing suspected URL threats detected as high risk by the Advanced Threat Scan Engine or analyzed by Virtual Analyzer as security risks	Not available
Probable Advanced Threats	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine but not analyzed by Virtual Analyzer	Not available

Detected Values	For Incoming Mail	For Outgoing Mail
BEC	The number of email messages detected as Business Email Compromise (BEC) attacks	Not available
Phishing	The number of email messages that Trend Micro Email Security content-based filtering detected as phishing threats	The number of email messages that Trend Micro Email Security content-based filtering detected as phishing threats
Suspicious URLs	The number of suspicious URLs detected during spam scanning	The number of suspicious URLs detected during spam scanning
Web Reputation	The number of email messages containing URLs that pose security risks	The number of email messages containing URLs that pose security risks
Spam	The number of email messages that Trend Micro Email Security content-based filtering detected as spam	The number of email messages that Trend Micro Email Security content-based filtering detected as spam
Domain-based Authentication	The number of messages that failed Sender IP Match, SPF, DKIM, and DMARC authentication	Not available
Graymail	The number of email messages detected as graymail	Not available
Data Loss Prevention	The number of email messages that triggered Data Loss Prevention incidents regardless of the action taken (block or pass)	The number of email messages that triggered Data Loss Prevention incidents regardless of the action taken (block or pass).
Anomaly	The number of email messages that Trend Micro Email Security Correlated Intelligence filtering detected as anomaly.	No applicable
Other	The number of email messages detected as virus scan exceptions or containing content filtering violations	The number of email messages detected as virus scan exceptions or containing content filtering violations

Detected Values	For Incoming Mail	For Outgoing Mail
Total	The total number of email messages processed	

Threats details chart

The **Threat Details** chart on the **Threats** tab of **Dashboard** displays the number of messages detected as threats and the total percentage of blocked messages.

The **Threat Details** table allows you to drill down from overall metrics into policy event logs for more granular data. The drill-down actions are available only for threats detected within the past 30 days.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

Table 3-4. Detected Values on Charts

Detected Values	For Incoming Mail	For Outgoing Mail
Ransomware	The number of email messages containing attachments that are detected as ransomware or the URL of sites that directly or indirectly facilitate the distribution of ransomware	The number of email messages containing attachments that are detected as ransomware or the URL of sites that directly or indirectly facilitate the distribution of ransomware
Malware (Pattern-based)	The number of email messages that pattern-based scanning detected as containing a malware threat	The number of email messages that pattern-based scanning detected as containing a malware threat

Detected Values	For Incoming Mail	For Outgoing Mail
Malware (PML Detected)	The number of email messages that Predictive Machine Learning detected as containing a malware threat	The number of email messages that Predictive Machine Learning detected as containing a malware threat
Suspicious Files	The number of suspicious files detected during spam scanning	The number of suspicious files detected during spam scanning
Analyzed Advanced Threats (Files)	The number of email messages containing suspected file threats detected as high risk by the Advanced Threat Scan Engine or analyzed by Virtual Analyzer as security risks	Not available
Analyzed Advanced Threats (URLs)	The number of email messages containing suspected URL threats detected as high risk by the Advanced Threat Scan Engine or analyzed by Virtual Analyzer as security risks	Not available
Probable Advanced Threats	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine but not analyzed by Virtual Analyzer	Not available
BEC	The number of email messages detected as Business Email Compromise (BEC) attacks	Not available
Phishing	The number of email messages that Trend Micro Email Security content-based filtering detected as phishing threats	The number of email messages that Trend Micro Email Security content-based filtering detected as phishing threats
Suspicious URLs	The number of suspicious URLs detected during spam scanning	The number of suspicious URLs detected during spam scanning

Detected Values	For Incoming Mail	For Outgoing Mail
Web Reputation	The number of email messages containing URLs that pose security risks	The number of email messages containing URLs that pose security risks
Spam	The number of email messages that Trend Micro Email Security content-based filtering detected as spam	The number of email messages that Trend Micro Email Security content-based filtering detected as spam
Domain-based Authentication	The number of messages that failed Sender IP Match, SPF, DKIM, and DMARC authentication	Not available
Graymail	The number of email messages detected as graymail	Not available
Data Loss Prevention	The number of email messages that triggered Data Loss Prevention incidents regardless of the action taken (block or pass)	The number of email messages that triggered Data Loss Prevention incidents regardless of the action taken (block or pass).
Anomaly	The number of email messages that Trend Micro Email Security Correlated Intelligence filtering detected as anomaly.	No applicable
Other	The number of email messages detected as virus scan exceptions or containing content filtering violations	The number of email messages detected as virus scan exceptions or containing content filtering violations
Total	The total number of email messages processed	

Virtual Analyzer file analysis details chart

The **Virtual Analyzer File Analysis Details** chart on the **Threat** tab of **Dashboard** displays the number and level of file threats detected by Virtual Analyzer based on the selected mail traffic direction.

Note

The data on this tab is displayed for incoming mail traffic only.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

TABLE 3-5. Detected Values on Charts

DETECTED VALUES	FOR INCOMING MAIL	FOR OUTGOING MAIL
High risk	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine and detected as high risk by Virtual Analyzer	Not available
Medium risk	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine and detected as medium risk by Virtual Analyzer	Not available
Low risk	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine and detected as low risk by Virtual Analyzer	Not available
No risk detected	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine and detected as safe by Virtual Analyzer	Not available

Detected Values	For Incoming Mail	For Outgoing Mail
Risk rating unavailable	The number of email messages containing suspected file threats detected by the Advanced Threat Scan Engine but not analyzed by Virtual Analyzer	Not available
Total	The total number of email messages processed	

Virtual Analyzer URL analysis details chart

The **Virtual Analyzer URL Analysis Details** chart on the **Threat** tab of **Dashboard** displays the number and level of URL threats detected by Virtual Analyzer based on the selected mail traffic direction.

Note

The data on this tab is displayed for incoming mail traffic only.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

Table 3-6. Detected Values on Charts

Detected Values	For Incoming Mail	For Outgoing Mail
High risk	The number of email messages containing suspected URL threats detected during spam scanning and rated as high risk by Virtual Analyzer	Not available

Detected Values	For Incoming Mail	For Outgoing Mail
Medium risk	The number of email messages containing suspected URL threats detected during spam scanning and rated as medium risk by Virtual Analyzer	Not available
Low risk	The number of email messages containing suspected URL threats detected during spam scanning and rated as low risk by Virtual Analyzer	Not available
No risk detected	The number of email messages containing suspected URL threats detected during spam scanning and rated as safe by Virtual Analyzer	Not available
Risk rating unavailable	The number of email messages containing suspected URL threats detected during spam scanning but not analyzed by Virtual Analyzer	Not available
Total	The total number of email messages processed	

Virtual Analyzer quota usage details

The **Virtual Analyzer Quota Usage Details** chart on the **Threats** tab of **Dashboard** displays the usage of the Virtual Analyzer submission quota.

Note

The data on this tab is displayed for incoming mail traffic only.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

TABLE 3-7. Values on Charts

VALUE	FOR INCOMING MAIL	FOR OUTGOING MAIL
File submission quota	The total number of file submissions to Virtual Analyzer allowed by the allocated quota	Not available
URL submission quota	The total number of URL submissions to Virtual Analyzer allowed by the allocated quota	Not available
Files analyzed	The number of files successfully analyzed by Virtual Analyzer	Not available
Files over quota	The number of file submissions over quota	Not available
URLs analyzed	The number of URLs successfully analyzed by Virtual Analyzer	Not available
URLs over quota	The number of URL submissions over quota	Not available
Submissions	The total number of file or URL submissions	

Domain-based authentication details chart

The **Domain-based Authentication Details** chart on the **Threat** tab of **Dashboard** displays the number of messages that failed Sender IP Match, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) authentication based on the selected mail traffic direction.

Sender IP Match is a way that readily enables you to simultaneously allow all inbound email traffic from a particular domain while equally preventing spoofing by manually defining the allowed IP ranges. SPF, DKIM and DMARC are three email authentication systems to protect against email spoofing.

Note

The data on this tab is displayed for incoming mail traffic only.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

TABLE 3-8. Detected Values on Charts

DETECTED VALUES	FOR INCOMING MAIL
Sender IP Match	The total number of messages that failed the Sender IP Match check.
SPF	The total number of messages that failed SPF check.
DKIM	The total number of messages that failed DKIM verification.
DMARC	The total number of messages that failed DMARC authentication.
DMARC - SPF	The total number of messages that failed SPF check of DMARC authentication.
DMARC - DKIM	The total number of messages that failed DKIM signature check of DMARC authentication.
DMARC - Alignment	The total number of messages that failed alignment check of DMARC authentication.
DMARC - Availability	The total number of messages that failed availability check of DMARC authentication because the sending domain does not have any DMARC record.

Blocked message details

The **Blocked Message Details** chart on the **Threats** tab of **Dashboard** displays the number of messages blocked for different reasons.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

TABLE 3-9. Values on Charts

VALUE	DESCRIPTION
Sender IP found in QIL	The number of messages blocked because the sender IP address was detected in the Quick IP List (QIL)
Sender IP found in KSSL	The number of messages blocked because the sender IP address was found in the Known Spam Source List (KSSL)
Sender IP found in DUL	The number of messages blocked because the sender IP address was found in the Dynamic User List (DUL)
Sender IP found in ETL	The number of messages blocked because the sender IP address was found in the Emerging Threat List (ETL)
Sender IP found in block list	The number of messages blocked because the sender IP address was found in the Blocked IP Address list or Blocked Country/Region list
Sender IP blocked	The number of messages blocked because the sender IP address was found in the internal global block list
Sender IP not allowed	The number of messages blocked because the sender IP address was not in the Outbound Servers under **Domain Management**
Sender blocked (block list)	The number of messages blocked because the sender email address was found in the blocked sender list or the internal global block list
Sender blocked (Suspicious Object List)	The number of messages blocked because the sender email address was found in the Suspicious Object List synchronized from Trend Vision One

Value	Description
Sender domain not found	The number of messages blocked because the sender domain was not found in the public DNS system
Sender domain malformed	The number of messages blocked because the sender's DNS record was found malformed
Recipient blocked	The number of messages blocked because the recipient email address was found in the internal global block list
Recipient invalid	The number of messages blocked because the recipient was not in the Valid Recipient list when Recipient Directory Management is enabled
Recipient domain not found	The number of messages blocked because the recipient domain was not found in the public DNS system
Recipient domain malformed	The number of messages blocked because the recipient's DNS record was found malformed
Message count limit reached (by IP address)	The number of messages blocked because the total number of messages sent from a single IP address exceeded the maximum limit in a certain period
Message count limit reached (by email address)	The number of messages blocked because the total number of messages sent from or to a single email address exceeded the maximum limit in a certain period
Data size limit reached (by IP address)	The number of messages blocked because the accumulated data size from a single IP address exceeded the maximum limit in a certain period
Data size limit reached (by email address)	The number of messages blocked because the accumulated data size from or to a single email address exceeded the maximum limit in a certain period
Data size limit reached (by domain)	The number of messages blocked because the accumulated data size from or to a single domain exceeded the maximum limit in a certain period
TLS not available	The number of messages blocked because the email client did not use TLS or the TLS version used by the peer was lower than the minimum version required to communicate with Trend Micro Email Security

Value	Description
Reverse DNS validation failed	The number of messages blocked because the message failed reverse DNS validation
Message too big	The number of messages blocked because the message size exceeded the maximum
Policy matching error	The number of messages blocked because an error occurred during policy matching
Other	The number of messages blocked due to other reasons
Total	The total number of email messages blocked

Top statistics tab

The **Top Statistics** tab of **Dashboard** provides the top 20 recipients of spam, malware, Business Email Compromise threats, and analyzed advanced threats.

Top bec attacks detected by antispam engine chart

The **Top BEC Attacks Detected by Antispam Engine** chart on the **Top Statistics** tab of **Dashboard** displays the email recipients that received the most messages containing Business Email Compromise (BEC) attacks as detected by the Antispam Engine based on the selected mail traffic direction.

Note

The data on this tab is displayed for incoming mail traffic only.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top BEC attacks detected by Writing Style Analysis chart

The **Top BEC Attacks Detected by Writing Style Analysis** chart on the **Top Statistics** tab of **Dashboard** displays the email recipients that received the most messages containing Business Email Compromise (BEC) attacks as detected by writing style analysis based on the selected mail traffic direction.

Note

For details about writing style analysis, see *Configuring Business Email Compromise criteria on page 6-23*.

The data on this tab is displayed for incoming mail traffic only.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top targeted high profile users

The **Top Targeted High Profile Users** chart on the **Top Statistics** tab of **Dashboard** displays the high profile users that were most frequently targeted for BEC attacks through email and detected by writing style analysis during selected time period.

Note

For details about high profile users, see *Configuring high profile users on page 5-82*.

The data on this tab is displayed for incoming mail traffic only.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top analyzed advanced threats (files) chart

The **Top Analyzed Advanced Threats (Files)** chart on the **Top Statistics** tab of **Dashboard** displays the email addresses that received the most messages containing advanced file threats based on the selected mail traffic direction.

Note

The data on this tab is displayed for incoming mail traffic only.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top analyzed advanced threats (URLs) chart

The **Top Analyzed Advanced Threats (URLs)** chart on the **Top Statistics** tab of **Dashboard** displays the email addresses that received the most messages containing advanced URL threats based on the selected mail traffic direction.

Note

The data on this tab is displayed for incoming mail traffic only.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top malware detected by Predictive Machine Learning chart

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. For details, see *About Predictive Machine Learning on page 6-22*.

The **Top Malware Detected by Predictive Machine Learning** chart on the **Top Statistics** tab of **Dashboard** displays the email addresses that sent or received the most messages containing malware threats, as detected by Predictive Machine Learning.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top malware detected by pattern-based scanning chart

The **Top Malware Detected by Pattern-based Scanning** chart on the **Top Statistics** tab of **Dashboard** displays the email addresses that sent or received the most messages containing malware threats based on the selected mail traffic direction, as detected by traditional pattern-based scanning.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top spam chart

The **Top Spam** chart on the **Top Statistics** tab of **Dashboard** displays the email addresses that sent or received the most spam messages based on the selected mail traffic direction.

Hover over a bar to see details.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Top Data Loss Prevention (DLP) incidents chart

The **Top Data Loss Prevention (DLP) Incidents** chart on the **Top Statistics** tab of **Dashboard** displays the email addresses that sent or received the most messages triggering DLP incidents regardless of the action taken (block or pass) based on the selected mail traffic direction.

Select a time period by **Date**, **Week**, or **Month** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Use the **Top violators** drop-down list to select the number of email addresses that display on the chart.

Other statistics tab

The **Other Statistics** tab of **Dashboard** provides volume and bandwidth of messages processed by Trend Micro Email Security.

Volume chart

The **Volume** chart on the **Summary** tab of **Dashboard** displays the total number of accepted and blocked messages and the total percentage of blocked messages.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The following is the specific data displayed:

TABLE 3-10. Detected Values on Charts

DETECTED VALUES	FOR INCOMING MAIL	FOR OUTGOING MAIL
Blocked	The number of email messages blocked by connection-based filtering at the MTA connection level or by Trend Micro Email Security incoming security filtering **Note** This value does not include messages blocked by content-based filtering.	The number of messages blocked using Trend Micro Email Security relay mail service filtering Possible reasons for blocking include: • Recipient address is not resolvable (such as `someone@???.com`). • Spammers forged the mail sender address so the message appears to be coming from the customer domain. • The customer's MTA is compromised and is sending spam messages (for example, it is an open relay).
Accepted	The number of email messages passed by connection-based filtering at the MTA connection level or by Trend Micro Email Security incoming security filtering	The number of messages passed by Trend Micro Email Security relay mail service filtering
Blocked %	The percentage of email messages blocked by connection-based filtering at the MTA connection level or by Trend Micro Email Security incoming security filtering	The percentage of messages blocked by Trend Micro Email Security relay mail service filtering
Total	The total number of email messages processed	

Bandwidth chart

The **Bandwidth** chart on the **Other Statistics** tab of **Dashboard** displays the total size of email messages scanned by Trend Micro Email Security.

Select a time period by **Date**, **Week**, **Month**, or **Last 12 months** to show data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

The traffic direction does not change the data displayed on charts. The following is the specific data displayed:

TABLE 3-11. Detected Values on Charts

DETECTED VALUES	FOR INCOMING MAIL	FOR OUTGOING MAIL
Not Quarantined	The total size of email messages that Trend Micro Email Security did not quarantine	
Quarantined	The total size of email messages that Trend Micro Email Security quarantined **Note** By default, no messages are quarantined. To begin using the quarantine, select a quarantine action for one or more policy rules.	
Total Size	The total size of email messages scanned by Trend Micro Email Security	

Time-of-click protection chart

The **Time-of-Click Protection** chart on the **Other Statistics** tab of **Dashboard** displays the total number of URL clicks, number of clicks allowed and blocked, number of clicks warned and stopped, and number of clicks warned but clicked through.

Select a time period by **Date**, **Week** or **Month** to show daily, weekly or monthly data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Note

If you select **Outgoing** from **Direction**, this chart will be hidden because Time-of-Click Protection applies only to incoming messages.

The following is the specific data displayed:

TABLE 3-12. Detected Values on Charts

DETECTED VALUES	FOR INCOMING MAIL
Blocked	The total number of URL clicks analyzed and blocked by Trend Micro Email Security at the time of click.
Allowed	The total number of URL clicks analyzed and allowed by Trend Micro Email Security at the time of click.
Warned and stopped	The total number of URL clicks collected where Trend Micro Email Security warned users and users stopped their access to the URLs.
Warned but accessed	The total number of URL clicks collected where Trend Micro Email Security warned users but users continued to access the URLs.
Total	The total number of URL clicks collected where Trend Micro Email Security provides Time-of-Click Protection.

DMARC compliance chart

The **DMARC Compliance** chart on the **Other Statistics** tab of **Dashboard** displays the total number of messages that have been checked for DMARC compliance, number of compliant messages, number of non-compliant messages, and the DMARC compliance rate. The statistics are based on the DMARC reports that Trend Micro Email Security has received.

Select a time period by **Week** or **Month** to show weekly or monthly data for the selected time period.

The specified time period only affects the data shown on this chart and its corresponding thumbnail chart on the **Threats** tab. Changing these selections does not affect other charts.

Note

The data in this chart is displayed for outgoing mail traffic only.

The following is the specific data displayed:

TABLE 3-13. Detected Values on Charts

DETECTED VALUES	FOR OUTGOING MAIL
Total messages	The total number of email messages that have been checked for DMARC compliance.
Compliant	The number of email messages that pass the DMARC compliance check.
Non-compliant	The number of email messages that fail the DMARC compliance check.
Compliance rate	The percentage of email messages that pass the DMARC compliance check.

Chapter 4

Managing domains

Use the **Domains** screen to add, modify, or delete domains.

TABLE 4-1. Fields on the Domains screen

FIELD	DESCRIPTION
Domain name	Name of a domain you added.

Field	Description
Inbound Servers	Recipient: Recipient can be a wildcard (*) or an exact email address. IP address or FQDN: Fully qualified domain name (FQDN) is a unique name, which includes both host name and domain name, and resolves to a single IP address. • For example: `hostmaster1.example.com` or `mailhost.example.com` • Not valid: `example.com` Port: Port is a number from 1 to 65535 that an inbound server listens on. These ports vary based on server configuration. Preference: Preference, sometimes referred to as distance, is a value from 1 to 100. The lower the preference value, the higher the priority. **Note** If more than one mail server is available, delivery is prioritized to servers with lower values. Using the same value will balance delivery to each server.
Outbound Servers	If outbound protection is enabled, this is the information for the MTA(s) that Trend Micro Email Security relays your outbound messages from. The following options are available: **Microsoft 365**: Relays your outbound messages from your Microsoft 365 solution. **Google Workspace**: Relays your outbound messages from your Google Workspace solution. **User-defined mail servers**: Relays your outbound messages from the mail servers you specified for your managed domain.
Time Added	Time when a domain was added.

Field	Description
Status	Status of a domain, which can be one of the following: • **Completed**: All required information and operations have been completed. The domain is successfully added. • **Configuration Required**: Certain required information or configurations are missing or incorrect.

Adding a domain

Procedure

1. Click **Domains**.
2. On the **Domains** screen, click **Add**.

   The **Add Domain** screen appears.
3. In the **General** section, specify the following:

   - **Domain name**: Includes everything to the right of the at sign (@) in email addresses managed by the server(s) being added.
   - **Skip default domain-level policy creation**: By default, this check box is selected.

     Trend Micro recommends that you skip creating default domain-level policy rules. The preconfigured default organization-level policy rules have the same rule scanning criteria as the default domain-level policy rules and will automatically apply to the new domain.

     If your account was provisioned before the release of the organization-level policy feature, no default organization-level policy rules were available. Trend Micro recommends that you manually create organization-level policy rules to provide organization-level protection.
4. In the **Inbound Servers** section, specify the following:

   - Recipient: Recipient can be a wildcard (*) or an exact email address. Specify the local part of an email address.
   - IP address or FQDN: Fully qualified domain name (FQDN) is a unique name, which includes both host name and domain name, and resolves to a single IP address.
   - Port: Port is a number from 1 to 65535 that an inbound server listens on. These ports vary based on server configuration.

- Preference: Preference, sometimes referred to as distance, is a value from 1 to 100. The lower the preference value, the higher the priority.

  If more than one mail server is available, delivery is prioritized to servers with lower values. Using the same value will balance delivery to each server.

Note

You can specify up to 100 inbound servers and 100 outbound servers.

Use the add + and the remove - buttons to manage additional entries.

Here is an example to explain how messages are routed to inbound servers based on preference values.

TABLE 4-2. Message routing example

RECIPIENT	IP ADDRESS OR FQDN	PREFERENCE
*@test.com	1.2.3.4	10
recipient1@test.com	1.2.3.5	11
recipient2@test.com	1.2.3.6	9

If a message is sent to recipient1@test.com, Trend Micro Email Security routes the message to the server (IP address: 1.2.3.4) with lower preference value (10), and then the server (IP address: 1.2.3.5) if the first server is unavailable.

If a message is sent to recipient2@test.com, Trend Micro Email Security routes the message to the server (IP address: 1.2.3.6) with lower preference value (9), and then the server (IP address: 1.2.3.4) if the first server is unavailable.

- **Send test message to**: (optional) Email address used to confirm email delivery from Trend Micro Email Security.

5. In the **Outbound Servers** section, specify the following:

Note

Outbound protection is disabled for trial users. To enable this feature, purchase a full license or contact technical support.

- Select **Enable outbound protection**.

WARNING!

Enabling outbound protection without specifying outbound servers will prevent the delivery of any outbound traffic routed through the service.

- Configure outbound servers using the following options:
  - **Microsoft 365**: Relays your outbound messages from your Microsoft 365 solution.
  - **Google Workspace**: Relays your outbound messages from your Google Workspace solution.
  - **User-defined mail servers**: Relays your outbound messages from the mail servers you specified for your managed domain.

6. Click **Add Domain**.

   If the domain is valid and an MX record for the domain exists, the domain appears on the **Domains** screen.

   After adding a domain, Trend Micro sends a welcome message to the administrative email address on record.

Configuring a domain

After adding a domain, perform required configurations to finish provisioning the domain. On the **Domains** screen, any domain missing required configurations is in the “Configuration required” status, and a red exclamation mark will be shown next to the field that requires your

operation or reports any problem. You can hover over the exclamation mark to view the detailed error message.

After you finish all required operations, the status of the domain will change from “Configuration required” into “Completed.”

Procedure

1. In the **General** section, verify your domain.

   a. Add the TXT record provided on the console to your domain's DNS configuration to prove that you own the domain.

   b. Click **Verify**.

      The message “Domain verified” appears if the domain verification is successful.

   If your domain does not pass verification, the built-in policy rule "Global Anti-Virus Rule (Enforced on Unverified Domains)" will be forcibly applied to incoming messages sent to the domain.

   If you have difficulty adding the TXT record, you can add an MX record for your domain instead:

   Add an MX record for the Trend Micro Email Security server with the highest preference value.

   - North America, Latin America and Asia Pacific:

     ```
     <your_domain> MX preference = 20, mail exchanger =
     <your_domain_mta>
     ```

     ```
     <your_domain> MX preference = 32767, mail exchanger =
     <company_identifier>.in.tmes.trendmicro.com
     ```

   - Europe and Africa:

     ```
     <your_domain> MX preference = 20, mail exchanger =
     <your_domain_mta>
     ```

     ```
     <your_domain> MX preference = 32767, mail exchanger =
     <company_identifier>.in.tmes.trendmicro.eu
     ```

- Australia and New Zealand:

  ```
  <your_domain> MX preference = 20, mail exchanger =
  <your_domain_mta>
  ```

  ```
  <your_domain> MX preference = 32767, mail exchanger =
  <company_identifier>.in.tmes-anz.trendmicro.com
  ```

- Japan:

  ```
  <your_domain> MX preference = 20, mail exchanger =
  <your_domain_mta>
  ```

  ```
  <your_domain> MX preference = 32767, mail exchanger =
  <company_identifier>.in.tmems-jp.trendmicro.com
  ```

- Singapore:

  ```
  <your_domain> MX preference = 20, mail exchanger =
  <your_domain_mta>
  ```

  ```
  <your_domain> MX preference = 32767, mail exchanger =
  <company_identifier>.in.tmes-sg.trendmicro.com
  ```

- India:

  ```
  <your_domain> MX preference = 20, mail exchanger
  =<your_domain_mta>
  ```

  ```
  <your_domain> MX preference = 32767, mail exchanger
  =<company_identifier>.in.tmes-in.trendmicro.com
  ```

- Middle East (UAE):

  ```
  <your_domain> MX preference = 20, mail exchanger
  =<your_domain_mta>
  ```

  ```
  <your_domain> MX preference = 32767, mail exchanger
  =<company_identifier>.in.tmes-uae.trendmicro.com
  ```

Note

In the preceding MX record, the second preference value `32767` is only used as an example. When setting the second preference value, make sure it is larger than the first preference value, which means this route has lower priority than the first one.

To learn more about MX records, see *About mx records and Trend Micro Email Security on page A-13*.

Tip

DNS propagation can take up to 48 hours. The status of the domain you are adding does not change until DNS propagation is complete. During this period, do not turn off any on-premises security. While waiting for DNS propagation, you can use the administrator console to customize the domain settings for features such as **Policy**, **Recipient Filter**, **Sender Filter**, **Policy Objects**, **BEC**, and **IP Reputation**.

If the domain stays as unverified for more than 48 hours, confirm that the TXT record or MX record for the domain is correct.

- For Linux, run one of the following commands:

```
dig txt <domain_name>
```

```
dig mx <domain_name>
```

- For Windows, run one of the following commands:

```
nslookup -q=txt <domain_name>
```

```
nslookup -q=mx <domain_name>
```

2. In the **Inbound Servers** section, complete the following configurations:

   a. Configure your firewall to accept email messages from the following Trend Micro Email Security IP addresses or CIDR blocks:

      - North America, Latin America and Asia Pacific:

18.208.22.64/26

18.208.22.128/25

18.188.9.192/26

18.188.239.128/26

- Europe and Africa:

  18.185.115.0/25

  18.185.115.128/26

  34.253.238.128/26

  34.253.238.192/26

- Australia and New Zealand:

  13.238.202.0/25

  13.238.202.128/26

- Japan:

  18.176.203.128/26

  18.176.203.192/26

  18.177.156.0/26

  18.177.156.64/26

  15.168.56.0/25

  15.168.49.64/26

  15.168.56.128/26

- Singapore:

  13.213.174.128/25

  13.213.220.0/26

- India:

  `3.110.59.128/25`

  `3.110.71.192/26`

- Middle East (UAE):

  `3.29.202.0/25`

  `3.29.194.192/26`

Note

If you are using a third-party IP reputation service, add the preceding Trend Micro Email Security IP addresses or CIDR blocks to the approved list of the IP reputation service, or disable the third-party service and enable Trend Micro Email Security to perform IP reputation-based filtering for you.

b. Click **Test Connection**.

c. Point the MX record of your domain to the Trend Micro Email Security server with the lowest preference value.

- North America, Latin America and Asia Pacific:

  `<your_domain> MX preference = 20, mail exchanger = <your_domain_mta>`

  `<your_domain> MX preference = 10, mail exchanger = <company_identifier>.in.tmes.trendmicro.com`

- Europe and Africa:

  `<your_domain> MX preference = 20, mail exchanger = <your_domain_mta>`

  `<your_domain> MX preference = 10, mail exchanger = <company_identifier>.in.tmes.trendmicro.eu`

- Australia and New Zealand:

```
<your_domain> MX preference = 20, mail exchanger =
<your_domain_mta>

<your_domain> MX preference = 10, mail exchanger =
<company_identifier>.in.tmes-anz.trendmicro.com
```

- Japan:

```
<your_domain> MX preference = 20, mail exchanger =
<your_domain_mta>

<your_domain> MX preference = 10, mail exchanger =
<company_identifier>.in.tmems-jp.trendmicro.com
```

- Singapore:

```
<your_domain> MX preference = 20, mail exchanger =
<your_domain_mta>

<your_domain> MX preference = 10, mail exchanger =
<company_identifier>.in.tmes-sg.trendmicro.com
```

- India:

```
<your_domain> MX preference = 20, mail exchanger
=<your_domain_mta>

<your_domain> MX preference = 10, mail exchanger
=<company_identifier>.in.tmes-in.trendmicro.com
```

- Middle East (UAE):

```
<your_domain> MX preference = 20, mail exchanger
=<your_domain_mta>

<your_domain> MX preference = 10, mail exchanger
=<company_identifier>.in.tmes-uae.trendmicro.com
```

To learn more about MX records, see *About mx records and Trend Micro Email Security on page A-13*.

d. Click **Verify** to verify the inbound servers you added.

The message “Inbound servers verified” appears if the inbound server verification is successful.

e. Type an email address next to **Send test message to** to verify that messages are being delivered from Trend Micro Email Security.

3. In the **Outbound Servers** section, complete the following configurations:

a. If your domain has SPF records, make sure the SPF record under the **Outbound Servers** section is also included.

For details about adding SPF records, see *Adding SPF records on page 4-14*.

b. Click **Verify**.

c. Route your outbound mail server to the following Trend Micro Email Security MTA for your region:

- North America, Latin America and Asia Pacific:

  `<company_identifier>.relay.tmes.trendmicro.com`

- Europe and Africa:

  `<company_identifier>.relay.tmes.trendmicro.eu`

- Australia and New Zealand:

  `<company_identifier>.relay.tmes-anz.trendmicro.com`

- Japan:

  `<company_identifier>.relay.tmems-jp.trendmicro.com`

- Singapore:

  `<company_identifier>.relay.tmes-sg.trendmicro.com`

- India:

  `<company_identifier>.relay.tmes-in.trendmicro.com`

- Middle East (UAE):

```
<company_identifier>.relay.tmes-uae.trendmicro.com
```

4. If you currently use Microsoft 365, configure Microsoft 365 connectors to allow email traffic to or from Trend Micro Email Security MTAs.

   See *Adding Microsoft 365 inbound connectors on page 4-16*.

   See *Adding Microsoft 365 outbound connectors on page 4-19*.

Adding SPF records

Sender Policy Framework (SPF) is an open standard to prevent sender address forgery. An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email messages on behalf of your domain. The purpose of an SPF record is to prevent spammers from sending messages with forged addresses at your domain.

Procedure

1. Access your DNS hosting provider's website.
2. Edit the existing SPF record or create a new TXT record for SPF.

   If you have an SPF record for your domain, add required values to the current record for Trend Micro. For example, change the following TXT record:

   ```
   v=spf1 ip4:x.x.x.x include:spf.example.com ~all
   ```

   Into:

   ```
   v=spf1 ip4:x.x.x.x include:<SPF record for Trend Micro
   Email Security server> include:spf.example.com ~all
   ```

   The *SPF record for Trend Micro Email Security server* is as follows for each serving:

Serving Site	SPF Record
North America, Latin America and Asia Pacific	spf-us.tmes.trendmicro.com
Europe and Africa	spf.tmes.trendmicro.eu
Australia and New Zealand	spf.tmes-anz.trendmicro.com
Japan	spf.tmems-jp.trendmicro.com
Singapore	spf.tmes-sg.trendmicro.com
India	spf.tmes-in.trendmicro.com
Middle East (UAE)	spf.tmes-uae.trendmicro.com

Note

If you are using the "spf.tmes.trendmicro.com" record for your serving site, Trend Micro recommends that you change it to the above SPF record that is reserved specifically for your site.

You can also find the *SPF record for Trend Micro Email Security server* in **Domains** > *Domain name* > **Outbound Servers** on the Trend Micro Email Security console.

Important

A domain cannot have more than one TXT record for SPF. If your domain has more than one SPF record, a message delivery or spam classification issue may occur.

Adding Microsoft 365 inbound connectors

Before you begin

Before integrating your Microsoft 365 managed domain name with Trend Micro Email Security, perform all steps recommended by Microsoft to complete configuration of Microsoft 365 email management for your domain.

To configure inbound connectors, ensure that you have an Microsoft 365 administrator account.

Some organizations use Microsoft 365 to remotely host their email architecture, allowing Microsoft to manage the day-to-day aspects of maintaining their email servers. Trend Micro Email Security integrates with Microsoft 365 to provide additional security and benefits.

Configure Microsoft 365 connectors to allow email traffic to and from Trend Micro Email Security MTAs.

Important

Consult the Microsoft 365 help for information about adding connectors. Some Microsoft 365 plans do not offer connectors.

Configure mail flow using connectors in Exchange Online

Procedure

1. Log on to your Microsoft 365 administration center.
2. In the navigation on the left, go to **Admin** > **Admin centers** > **Exchange**

   The **Exchange admin center** screen appears.
3. In the navigation on the left, go to **mail flow**, and then click **connectors** in the top navigation.
4. Do the following to add an Inbound Connector to Microsoft 365:

Note

By adding an inbound connector, you can configure Microsoft 365 to accept mail filtered by Trend Micro Email Security for delivery to email accounts in your Microsoft 365 managed domain.

a. Click the plus (+) icon.

A new connector configuration screen appears.

b. In the **From** field, select **Partner organization**.

c. In the **To** field, select **Microsoft 365**.

d. Click **Next**.

e. In the **Name** field, type a descriptive name for the connector.

For example, type `Trend Micro Email Security (Inbound)`.

f. Select the **Turn it on** check box.

g. Click **Next**.

h. Select **Use the sender's IP address**, and then click **Next**.

i. In the **Specify the sender IP address range.** field, add the following Trend Micro Email Security IP addresses:

- North America, Latin America and Asia Pacific:

  `18.208.22.64/26`

  `18.208.22.128/25`

  `18.188.9.192/26`

  `18.188.239.128/26`

- Europe and Africa:

  `18.185.115.0/25`

  `18.185.115.128/26`

  `34.253.238.128/26`

```
34.253.238.192/26
```

- Australia and New Zealand:

```
13.238.202.0/25
```

```
13.238.202.128/26
```

- Japan:

```
18.176.203.128/26
```

```
18.176.203.192/26
```

```
18.177.156.0/26
```

```
18.177.156.64/26
```

```
15.168.56.0/25
```

```
15.168.49.64/26
```

```
15.168.56.128/26
```

- Singapore:

```
13.213.174.128/25
```

```
13.213.220.0/26
```

- India:

```
3.110.59.128/25
```

```
3.110.71.192/26
```

- Middle East (UAE):

```
3.29.202.0/25
```

```
3.29.194.192/26
```

j. Click **Next**.

k. Select **Reject email messages if they aren't sent over TLS**, and then click **Next**.

The **New connector** confirmation screen appears, displaying all the settings that you have configured.

l. Click **Save**.

Adding Microsoft 365 outbound connectors

Before you begin

To configure outbound connectors, ensure that you have an Microsoft 365 administrator account.

Some organizations use Microsoft 365 to remotely host their email architecture, allowing Microsoft to manage the day-to-day aspects of maintaining their email servers. Trend Micro Email Security integrates with Microsoft 365 to provide additional security and benefits.

Configure Microsoft 365 connectors to allow email traffic to and from Trend Micro Email Security MTAs.

Important

Consult the Microsoft 365 help for information about adding connectors. Some Microsoft 365 plans do not offer connectors.

Configure mail flow using connectors in Exchange Online

Procedure

1. Log on to your Microsoft 365 administration center.
2. In the navigation on the left, go to **Admin** > **Admin centers** > **Exchange**

   The **Exchange admin center** screen appears.
3. In the navigation on the left, go to **mail flow**, and then click **connectors** in the top navigation.
4. Do the following to add an Outbound Connector to Microsoft 365:

Note

By adding an outbound connector, you can configure Microsoft 365 to relay outbound mail to Trend Micro Email Security for filtering and delivery to recipients outside of your Microsoft 365 managed domain.

a. Click the plus (+) icon.

A new connector configuration screen appears.

b. In the **From** field, select **Microsoft 365**.

c. In the **To** field, select **Partner organization**.

d. Click **Next**.

e. In the **Name** field, type a descriptive name for the connector.

For example, type `Trend Micro Email Security (Outbound)`.

f. Select the **Turn it on** check box.

g. Click **Next**.

h. Select **Only when I have a transport rule set up that redirects messages to this connector**, and then click **Next**.

i. Select **Route email through these smart hosts**, click the plus (+) icon, and then add the following host to the list:

`<company_identifier>.relay.<domain_name>`

Note

In the preceding information, replace <*company_identifier*> and <*domain_name*> with actual values. The value of <*domain_name*> varies according to your location:

- North America, Latin America and Asia Pacific:

  `tmes.trendmicro.com`

- Europe and Africa:

  `tmes.trendmicro.eu`

- Australia and New Zealand:

  `tmes-anz.trendmicro.com`

- Japan:

  `tmems-jp.trendmicro.com`

- Singapore:

  `tmes-sg.trendmicro.com`

- India:

  `tmes-in.trendmicro.com`

- Middle East (UAE):

  `tmes-uae.trendmicro.com`

j. Click **Next**.

k. Keep the default settings on the screen that appears, and click **Next**.

The **New connector** confirmation screen appears, displaying all the settings that you have configured.

l. Click **Next**.

m. Add an email address to the field provided, and then click **Validate**.

After the validation process completes, the **Validation Result** screen displays.

n. Click **Save**.

5. Add an email flow rule to use the outbound connector you created.

   a. In the navigation on the left, go to **mail flow**, and then click **rules** in the top navigation.

   b. Click the plus (+) icon and click **Create a new rule**.

   c. In the **Name** field, type a name for the rule, for example, `Trend Micro Email Security (Outbound)`.

   d. Under **Apply this rule if...**, select **The recipient is located** and then **Outside the organization** and click **OK**.

   e. Click **More Options** at the bottom to show more settings.

   f. Under **Do the following...**, select **Redirect the message to** and then **the following connector** and choose the outbound connector you created for message redirection.

   g. Configure the remaining fields if necessary; otherwise, keep the default settings for them.

   h. Click **Save**.

Editing or deleting domains

Procedure

1. On the **Domains** screen, select domains by doing one of the following:

   - To select one or more domains, select the check box to the left of each entry.
   - To select all domains, select the check box to the left of the **Domain Name** column title.

2. To edit information for a domain, do the following:

a. Click the domain name in the **Domain Name** column.

The **Edit Domain** screen appears, with fields pre-filled with the information on record for that domain.

b. Modify the fields as needed.

3. To delete domains, select one or multiple domain records and click **Delete**.

After you delete the domain(s), related quarantined emails will be removed and can no longer be released. Make sure you check the quarantined items before deleting the domain(s).

Chapter 5

Inbound and outbound protection

Managing recipient filter

The **Recipient Filter** screen displays the list of available domains. You can enable or disable these domains to check valid recipients and export the domain recipient lists to local storage.

TABLE 5-1. Recipient Filter Tasks

TASKS	STEPS
Enable All Filters	On the **Recipient Filter** screen, click **Enable All** to enable all filters in all domains.
Disable All Filters	On the **Recipient Filter** screen, click **Disable All** to disable all filters in all domains.
Export All	On the **Recipient Filter** screen, click **Export All** to export all filters in all domains to the local storage.
Export A Filter List	On the **Recipient Filter** screen, click the  icon under the **Export** column to export the filter list in a domain.

Managing sender filter

Trend Micro Email Security allows you to configure the following to filter senders of incoming messages for the entire organization, a managed domain, or a specific recipient address in your managed domains:

- Approved senders

  Specifies the senders to allow using specific email addresses or entire domains.

- Blocked senders

  Specifies the senders to block using specific email addresses or entire domains.

- Sender filter settings

  - Specifies the type of sender addresses collected to match the approved and blocked sender lists.

- Specifies whether to insert an X-Header in the message header for email messages matching approved senders.
- Specifies whether to skip certain security checks on email messages from approved senders.

Trend Micro Email Security achieves a two-way synchronization between the following data:

- Senders configured for a specific end user on the administrator console
- Senders added by that user through the End User Console or quarantine digest notifications

Any changes made to the approved or blocked senders of an end user either on the administrator console or End User Console should be reflected to the other location.

Configuring approved and blocked sender lists

Configure the **Approved Senders** and **Blocked Senders** lists to control which email messages Trend Micro Email Security scans. Specify the senders to allow or block using specific email addresses or entire domains.

For example, `*@example.com` specifies all senders from the `example.com` domain.

Evaluation is done in the following order:

1. Blocked sender list of an end user's email address
2. Blocked sender list of managed domains or the entire organization
3. Approved sender list of an end user's email address
4. Approved sender list of managed domains or the entire organization

Note

Approved senders of an end user's email address will not override blocked senders for the corresponding domain or organization. For example, assume that `*@example.com` is in the blocked sender list of the administrator console, and `john@example.com` is in the approved sender list of an end user. Messages from `john@example.com` will still be blocked.

IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

Lists of approved or blocked senders are managed using the following tabs on the **Inbound Protection** > **Connection Filtering** > **Sender Filter** screen:

- **Approved Senders**

  Trend Micro Email Security performs connection filtering and spam filtering checks on emails from approved senders according to what you specify on the *Sender Filter Settings on page 5-9* tab.

  Trend Micro Email Security performs virus scanning and content filtering on all emails received and takes the action configured in policy rules once detecting any virus or content filtering violation.

- **Blocked Senders**

  Trend Micro Email Security automatically blocks messages sent from addresses or domains added to the blocked list without submitting the messages to any scanning.

The **Approved Senders** and **Blocked Senders** tables display the following information:

- **Status**: Specifies whether the senders added to a recipient are enabled
- **Recipient**: The recipient for which you approved or blocked the specified sender. The options include the entire organization, a managed domain, or a specific recipient address in a managed domain.

Note

To view the approved or blocked senders added to the **Recipient**, click the recipient name.

- **Modified**: The date and time that you last modified the senders of the recipient

Adding senders

Trend Micro Email Security approves or blocks email messages from the specified sender for the entire organization, a managed domain, or a specific recipient address in your managed domains.

For example, after adding `spammerbob@examplespamdomain.com` to the blocked list for your managed domain `mydomain.com`, Trend Micro Email Security only blocks the email messages sent from `spammerbob@examplespamdomain.com` to addresses in the `mydomain.com` domain. Trend Micro Email Security still scans and possibly passes email messages sent from `spammerbob@examplespamdomain.com` to your other managed domains.

Procedure

1. Click the **Approved Senders** or **Blocked Senders** tab, and click **Add**.
2. On the **Specify Target Recipient** dialog box that appears, specify the target recipient of the sender you want to add and click **Next**.
   - **My organization**
   - **Managed domain**
   - **Email address**
3. In the **Add Approved Senders** dialog box, type a sender in the second field. A sender can be a specific email address or all addresses from a specific domain or subdomain.
   - Filter a specific email address by typing that email address.

- Filter all addresses from a domain by using an asterisk (*) to the left of the at sign (@) in the email address. For example, `*@example.com` will filter all email addresses in the `example.com` domain.
- Filter all addresses from a subdomain by using an asterisk (*) to the left of the at sign (@) and also using an asterisk (*) in place of the subdomain in the email address. For example, `*@*.example.com` will filter all email addresses in all subdomains of the `example.com` domain.

The following table displays format examples that are valid or not valid:

TABLE 5-2. Format Examples for Approved Senders and Blocked Senders

VALID	NOT VALID
`name@example.com`	`name@info.*.example.com`
`name@info.example.com`	`name@example.com.*`
`name@*.example.com`	`*name@info.example.com`
`name@*`	`*@*`
`*@example.com`	
`*@server.example.com`	
`*@*.example.com`	

4. Click **Add**.

   Trend Micro Email Security validates the sender address and adds it to the list.

Editing senders

Procedure

1. On the **Approved Senders** or **Blocked Senders** tab, click the recipient name for which you want to edit the senders.

2. Optionally type a sender address and click **Search** to search for specific senders.
3. Click the email address of a sender.

   The email address becomes editable, and buttons labeled **Save** or **Cancel** appear.
4. Make and confirm your changes or corrections.

   - Filter a specific email address by typing that email address.
   - Filter all addresses from a domain by using an asterisk (*) to the left of the at sign (@) in the email address. For example, `*@example.com` will filter all email addresses in the `example.com` domain.
   - Filter all addresses from a subdomain by using an asterisk (*) to the left of the at sign (@) and also using an asterisk (*) in place of the subdomain in the email address. For example, `*@*.example.com` will filter all email addresses in all subdomains of the `example.com` domain.

   The following table displays format examples that are valid or not valid:

TABLE 5-3. Format Examples for Approved Senders and Blocked Senders

VALID	NOT VALID
`name@example.com`	`name@info.*.example.com`
`name@info.example.com`	`name@example.com.*`
`name@*.example.com`	`*name@info.example.com`
`name@*`	`*@*`
`*@example.com`	
`*@server.example.com`	
`*@*.example.com`	

Importing senders

Trend Micro Email Security allows you to import approved and blocked senders in batches from a properly-formatted CSV file.

Procedure

1. Click the **Approved Senders** or **Blocked Senders** tab.
2. Display the import dialog box by using either of the following methods:
   - To import senders and recipients in pairs, click **Import** on the tab.
   - To import senders for a specific recipient, click a recipient name, and click **Import** in the dialog box that appears.
3. From the import dialog box, click **Choose File** to locate the file to import.
4. Select one of the following import options:
   - **Merge**: append the sender email addresses or domains to the existing list.
   - **Overwrite**: replace the existing list with the sender email addresses or domains in the file.

   You can click **Download sample file** to view a sample of a properly formatted file.

   Trend Micro Email Security checks all the entries in the selected file to identify any invalid, duplicate, conflict, excessive email addresses or email addresses from unmanaged domains.
5. Click **Preview**.
6. After you confirm all the entries to be imported, click **Import**.

Exporting senders

Trend Micro Email Security allows you to export the existing approved and blocked senders to the local storage.

Procedure

1. Click the **Approved Senders** or **Blocked Senders** tab.
2. Export senders by using either of the following methods:
   - To export senders and recipients in pairs, select one or more recipient records, and click **Export**.
   - To export all senders of a specific recipient, click the recipient name, and click **Export All** in the dialog box that appears.

   The selected senders are exported to the local storage.

Sender filter settings

Just like physical letters, an email message has two sets of addresses: the envelope address and the message header address. The envelope address, like the address on the outside of an envelope, is used by the MTA to route and deliver the email message; the message header address, which is part of the message header, is similar to the address attached to a salutation at the start of a physical letter.

The **Settings** tab on the **Sender Filter** screen enables you to choose the type of sender addresses Trend Micro Email Security uses to match the approved or blocked sender list.

The following options are available:

- **Envelope addresses**
- **Message header addresses**

By default, both options are selected. Trend Micro Email Security uses both addresses for matching. The **Message header addresses** option can be modified while the **Envelope addresses** option cannot.

Note

If **Message header addresses** is selected on the **Quarantine** > **End User Quarantine Settings** screen, Trend Micro recommends you also select it on the **Sender Filter Settings** screen. Otherwise, the approved or blocked senders added by end users will not work as expected.

Trend Micro Email Security provides the capability of inserting an X-Header in the message header for email messages matching approved senders. If you select the **Insert an X-Header in the message header if an approved sender matches** check box, you can do extra actions based on the message header on your own MTA or mail server.

- The following X-Header is inserted in the message header once an approved sender's envelope address matches:

  ```
  X-TM-Approved-Sender: envelope-sender
  ```

- The following X-Header is inserted in the message header if an approved sender's envelope address does not match but the message header address matches:

  ```
  X-TM-Approved-Sender: header-sender
  ```

Trend Micro Email Security also allows you to specify which of the following scanning criteria should not be applied to emails from approved senders:

- IP reputation-based filtering
- Unknown sender domain check
- Spam
- BEC
- Phishing and other suspicious content
- Graymail
- Web Reputation
- Social engineering attack

- Unusual signal
- Security risks

Note

When this option is selected, suspicious files identified by Correlated Intelligence will not be sent to Virtual Analyzer for further observation.

- Anomalies

Note

Unless specified otherwise, Trend Micro Email Security considers the envelope address as the common sender address.

Regardless of your sender address settings, IP reputation-based filtering and unknown sender domain check will always use **Envelope addresses** rather than **Message header addresses** to match the approved or blocked sender list. Unknown sender domain check refers to the check that verifies if the sender's envelop address has a valid DNS A or MX record.

Transport Layer Security (TLS) peers

Transport Layer Security (TLS) is a protocol that helps to secure data and ensure communication privacy between endpoints. Trend Micro Email Security allows you to configure TLS encryption policies between Trend Micro Email Security and specified TLS peers. Trend Micro Email Security supports the following TLS protocols in descending order of priority: TLS 1.3, TLS 1.2, TLS 1.1 and TLS 1.0.

To prevent against man-in-the-middle attacks on TLS connections, Trend Micro Email Security introduces DNS-based Authentication of Named Entities (DANE) and Mail Transfer Agent - Strict Transport Security (MTA-STS) to verify the identity of the destination servers.

Note

You can enable DANE or MTA-STS authentication between Trend Micro Email Security and specified TLS peers during outbound mail delivery.

For inbound mails, Trend Micro Email Security inherently supports MTA-STS after you have set up a DNS record and a policy for your domain. For details, see *About mta-sts records for inbound protection on page A-14*.

The **Transport Layer Security (TLS) Peers** screen uses the following important terms:

TERM	DETAILS
Managed Domain list	
Status (Managed Domain)	• **Enabled**: Domain is enabled • **Disabled**: Domain is disabled
Default (for unspecified domains)	This configuration applies to all domains that are not in the managed domain list
Domain TLS Peers list	
Status (TLS Peer)	• **Enabled**: Trend Micro Email Security applies your specified TLS configuration to the peer • **Disabled**: Trend Micro Email Security does not apply your specified TLS configuration to the peer Instead, the "Default (for unspecified peers)" TLS configuration applies.
TLS peer	Trend Micro Email Security can apply your specified TLS configuration with this peer during network communications.
Minimum TLS version	Minimum TLS version that the TLS peer must use to communicate with Trend Micro Email Security through the TLS protocol. • **TLS 1.3**: The TLS peer must use TLS 1.3. • **TLS 1.2**: The TLS peer must use TLS 1.2 or later.

Term	Details
	• **No restriction**: The TLS peer can use any TLS protocol.

Security level	• **Opportunistic TLS**:
	  • Communicates using encryption if the peer supports and elects to use TLS
	  • Communicates without encryption if the peer does not support TLS
	  • Communicates without encryption if the peer supports TLS but elects not to use TLS
	• **Mandatory TLS**:
	  • Communicates using encryption if the peer supports and elects to use TLS
	  • Does not communicate if the peer does not support TLS
	  • Does not communicate if the peer supports TLS but elects not to use TLS
	• **Opportunistic DANE TLS** (Outbound protection only)
	  • Communicates using encryption only if remote SMTP server has usable DANE TLSA record(s) and the peer DANE authentication succeeds
	  • Downgrades to **Mandatory TLS** if all TLSA record(s) are unusable due to unsupported parameters or malformed data
	  • In other cases, downgrades to **Opportunistic TLS**
	• **Mandatory DANE TLS** (Outbound protection only)
	  • Communicates using encryption if the peer DANE authentication succeeds
	  • Does not communicate if the peer does not pass DANE authentication
	• **MTA-STS** (Outbound protection only)
	  • Delivers the message using encryption when the TLS peer uses the policy mode **enforce** or **testing** and passes MTA-STS validation

TERM	DETAILS
	• Does not deliver the message when the TLS peer uses the policy mode **enforce** but fails the MTA-STS validation • Uses **Opportunistic TLS** to deliver the message when the policy of the TLS peer cannot be obtained, the TLS peer uses the policy mode **none**, or the TLS peer uses the policy mode **testing** but fails the MTA-STS validation **Note** When a TLS peer supports both DANE and MTA-STS, Trend Micro recommends that you select DANE for communicating with the peer. DANE is considered more secure than MTA-STS for protecting SMTP connections.
Default (for unspecified peers)	This configuration applies to all peers that meet any of the following criteria: • Peer is not in the peer list • Peer is in the peer list, but is not enabled

Adding domain TLS peers

Procedure

1. Go to **Inbound Protection** > **Connection Filtering** > **Transport Layer Security (TLS) Peers** or **Outbound Protection** > **Connection Filtering** > **Transport Layer Security (TLS) Peers**.
2. Click **Add**.
3. On the **Add Domain TLS Peers** screen, configure TLS peers for a managed domain.
   a. In the **Basic Information** section, select a managed domain.
   b. In the **Domain TLS Peers** section, click **Add** to add a TLS peer for the selected domain.
   c. Set **Status** to **Enabled** to have Trend Micro Email Security apply your specified TLS security level to the new peer.

d. For inbound protection, specify a sender domain, IP address, or CIDR block as **TLS Peer**. For outbound protection, specify a recipient domain as **TLS Peer**.

e. Specify **Minimum TLS Version** that the TLS peer must use when communicating with Trend Micro Email Security through the TLS protocol.

To determine which TLS version to set as the minimum, you can view the number of messages sent with TLS versions lower than the selected version in the last 7 days.

f. Set the **Security level**.

Note

The security levels **Opportunistic DANE TLS**, **Mandatory DANE TLS**, and **MTA-STS** are available only for outbound delivery.

To ensure messages can be received from the Trend Micro Email Security MTA, configure your firewall to accept email messages from the following Trend Micro Email Security IP address / CIDR blocks:

- North America, Latin America and Asia Pacific:

  `18.208.22.64/26`

  `18.208.22.128/25`

  `18.188.9.192/26`

  `18.188.239.128/26`

- Europe and Africa:

  `18.185.115.0/25`

  `18.185.115.128/26`

  `34.253.238.128/26`

  `34.253.238.192/26`

- Australia and New Zealand:

  `13.238.202.0/25`

  `13.238.202.128/26`

- Japan:

  `18.176.203.128/26`

  `18.176.203.192/26`

  `18.177.156.0/26`

  `18.177.156.64/26`

  `15.168.56.0/25`

  `15.168.49.64/26`

  `15.168.56.128/26`

- Singapore:

  `13.213.174.128/25`

  `13.213.220.0/26`

- India:

  `3.110.59.128/25`

  `3.110.71.192/26`

- Middle East (UAE):

  `3.29.202.0/25`

  `3.29.194.192/26`

g. (Optional) Select **Deliver daily reports to TLS peer**.

This option is available when you select **Mandatory DANE TLS**, **Opportunistic DANE TLS**, or **MTA-STS**.

The reports share success or failure statistics about TLS connections with DANE or MTA-STS support to the specified TLS peer.

h. (Optional) Test the connection to the TLS peer.

- For inbound protection, type an email address local part for TLS test.
- For outbound protection, type a domain name for DANE test or MTA-STS test if you set **Security level** to **Opportunistic DANE TLS** / **Mandatory DANE TLS** or **MTA-STS**.

4. Click **Save**.
5. Click **Submit**.

Editing domain TLS peers

Procedure

1. Go to **Inbound Protection** > **Connection Filtering** > **Transport Layer Security (TLS) Peers** or **Outbound Protection** > **Connection Filtering** > **Transport Layer Security (TLS) Peers**.
2. Click the name of a managed domain.
3. Find the TLS peer that you want to edit, and click the peer name.
4. Edit the peer information as required.
5. Click **Save**.

Understanding IP reputation

Trend Micro Email Security offers two tiers of protection. Connection-based filtering at the MTA connection level, including IP reputation-based filtering provided by Trend Micro Email Reputation Services (ERS), is the first tier. The second is content-based filtering at the message level.

Tip

IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

See *IP reputation order of evaluation on page 5-22*.

Trend Micro Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service. Email Reputation Services use a standard IP reputation database and an advanced, dynamic IP reputation database (a database updated in real time). These databases have distinct entries, allowing Trend Micro to maintain a very efficient and effective system that can quickly respond to new sources of spam.

Configure the following settings on the **Settings** tab of the **IP Reputation** screen:

- **Quick IP List**, which is also known as dynamic IP reputation settings, controls how Trend Micro Email Security uses the dynamic IP reputation database from Email Reputation Services Advanced Service.
- **Standard IP Reputation Settings** control how Trend Micro Email Security uses the standard IP reputation database from Email Reputation Services Standard Service.

The other tabs of the **IP Reputation** screen are as follows:

- **Approved IP Address**
- **Blocked IP Address**
- **Approved Country/Region**
- **Blocked Country/Region**

About quick IP list

Trend Micro Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service.

Quick IP List uses Trend Micro Email Reputation Services Advanced Service, a real-time antispam solution. The Trend Micro network of automated expert systems, along with Trend Micro spam experts, continuously monitor network and traffic patterns and immediately update the dynamic IP reputation database as new spam sources emerge, often within minutes. As evidence of spam activity increases or decreases, the dynamic IP reputation database is updated accordingly.

The dynamic IP reputation database includes the following blocking levels:

- **Level 0: Off**

  Queries the dynamic reputation database but does not block any IP addresses.

- **Level 1: Least aggressive**

  Trend Micro Email Security allows the same amount of spam from a sender with a good rating as in Level 2. The length of time that the IP address stays in the database is generally shorter than for more aggressive settings.

- **Level 2:** (the default setting)

  Trend Micro Email Security allows a larger volume of spam from a sender with a good rating than more aggressive settings. However, if an increase in spam above the allowable threshold is detected, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database is generally shorter than for more aggressive settings.

- **Level 3:**

  Trend Micro Email Security allows a small volume of spam from senders with a good rating. However, if an increase in spam beyond the allowable threshold is detected, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database depends on whether additional spam from the sender is detected.

- **Level 4: Most aggressive**

If even a single spam message from a sender IP address is detected, Email Reputation Services adds the sender to the dynamic reputation database and Trend Micro Email Security blocks all messages from the sender. The length of time that the IP address stays in the database depends on whether additional spam from the sender is detected.

If legitimate email is being blocked, select a less aggressive setting. If too much spam is reaching your network, select a more aggressive setting. However, this setting might increase false positives by blocking connections from legitimate email senders.

Note

To avoid false positives from a trusted partner company, go to **Inbound Protection** > **Connection Filtering** > **IP Reputation**, and add the IP address for their MTA to the **Approved IP Address** list.

The IP addresses in the approved lists bypass other IP reputation-based filtering. This list is useful for ensuring all messages from a partner company or other MTA are allowed, no matter their status with the standard IP reputation databases or with the Trend Micro Email Reputation Services (ERS) dynamic IP reputation database. When using the IP reputation approved lists, you may experience lower overall spam catch rates.

About standard IP reputation settings

Trend Micro Email Security makes use of Trend Micro Email Reputation Services (ERS) Standard Service and Advanced Service.

Standard IP Reputation Settings use Trend Micro Email Reputation Services Standard Service, which helps block spam by validating requested IP addresses against the Trend Micro standard IP reputation database, powered by the Trend Micro Threat Prevention Network. This ever-expanding database currently contains over a billion IP addresses with reputation ratings based on spamming activity. Trend Micro spam investigators continuously review and update these ratings to ensure accuracy.

Trend Micro Email Security makes a query to the standard IP reputation database server whenever it receives an email message from an unknown

host. If the host is listed in the standard IP reputation database, that message is reported as spam.

You can choose which lists to enable from the standard IP reputation database. By default, all lists are enabled. The default setting is the most effective for reducing spam levels, and it meets the needs of most customers.

Note

If you disable some portions of the standard IP reputation database, you may see an increase in the amount of spam messages that reach your internal mail server for additional content filtering.

The standard IP reputation database includes the following lists:

- **Known Spam Source List**: The Known Spam Source List (KSSL) is a list of IP addresses of mail servers that are known to be sources of spam.
- **Dynamic User List**: The Dynamic User List (DUL) is a list of dynamically assigned IP addresses, or those with an acceptable use policy that prohibits public mail servers. Most entries are maintained in cooperation with the ISP owning the network space. IP addresses in this list should not be sending email directly but should be using the mail servers of their ISP.
- **Emerging Threat List**: The Emerging Threat List (ETL) is a list of IP addresses identified as involved in active ransomware, malware, or other email threat campaigns.

Note

To avoid false positives from a trusted partner company, go to **Inbound Protection** > **Connection Filtering** > **IP Reputation**, and add the IP address for their MTA to the **Approved IP Address** list.

About approved and blocked IP addresses

To manually override IP reputation-based filtering at the MTA connection level:

- Configure the **Approved IP Address** list
- Configure the **Blocked IP Address** list
- Configure the **Approved Country/Region** list
- Configure the **Blocked Country/Region** list

Tip

The **Approved IP Address** and **Blocked IP Address** lists support both IP addresses and Classless Inter-Domain Routing (CIDR) blocks.

To add a CIDR block to the list, type the IPv4 address / CIDR block. The following is the only valid format: `x.x.x.x/z`

These lists override the **Quick IP List** and **Standard IP Reputation Settings** and allow for customization of which addresses are subjected to IP reputation-based filtering.

The IP addresses in the approved lists bypass other IP reputation-based filtering as well as reverse DNS validation. This list is useful for ensuring all messages from a partner company or other MTA are allowed, no matter their status with the standard IP reputation databases or with the Trend Micro Email Reputation Services (ERS) dynamic IP reputation database. When using the IP reputation approved lists, you may experience lower overall spam catch rates.

The IP addresses in the blocked lists are not subject to other IP reputation-based filtering. Trend Micro Email Security permanently rejects connection attempts from such IP addresses by responding with a 550 error (a rejection of the requested connection).

IP reputation order of evaluation

Message sender IP addresses go through IP reputation-based filtering. IP addresses are evaluated until the first match is found.

Messages from approved sender IP addresses bypass IP reputation-based filtering at the MTA connection level. Messages from blocked sender IP addresses are blocked.

Evaluation is done in the following order:

1. IP addresses
    a. In the **Approved IP Address** list
    b. In the **Blocked IP Address** list
2. Countries/regions
    a. In the **Approved Country/Region** list
    b. In the **Blocked Country/Region** list
3. The Emerging Threat List (ETL) in the IP Reputation settings
4. The Known Spam Source (KSS) in the IP Reputation settings
5. The Dynamic User List (DUL) in the IP Reputation settings
6. The Quick IP List (QIL) in the IP Reputation settings

An IP address added to the **Approved IP Address** list will not be blocked even if that IP address is also in a CIDR block listed in the **Blocked IP Address** list. Furthermore, that IP address will not be blocked even if it is also in the **Known Spam Source** standard IP reputation database list.

Important

IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

See *Managing sender filter on page 5-2*.

Troubleshooting issues

If you encounter unexpected errors while trying to save your settings on the **IP Reputation** screen, you may be able to resolve the issue on your own. Consult the following table for guidance on resolving the problem before contacting technical support.

TABLE 5-4. IP Reputation Settings: Issues and Solutions

ISSUE	POSSIBLE CAUSE	POSSIBLE SOLUTION
The **Save** button is disabled.	You do not have a valid Activation Code.	Obtain a valid Activation Code from your vendor.
	You have applied for an Activation Code, but it has not yet been added to the Trend Micro Email Security system.	Try again later.
	A temporary network issue is preventing Trend Micro Email Security from validating the Activation Code.	Try again later.
I cannot save my IP Reputation settings.	There is a temporary network issue.	Try again later.
		Log off, log on, and try again.
	There is more than one browser window open to the Trend Micro Email Security administrator console, and the session in one of the other windows has expired.	Close the other windows and try again.
		Log off, log on, and try again.

Managing reverse DNS validation

Trend Micro Email Security adds a layer of protection by validating the reverse DNS (rDNS) records for inbound email messages.

With the reverse DNS validation feature, an administrator can configure the following:

- Validation settings: whether to reject an email message when the corresponding PTR record is missing or invalid
- Block list: a list of PTR domains for message blocking

During the SMTP connection setup stage, Trend Micro Email Security uses the email sending IP address to perform rDNS lookup. If the query result matches the criteria in any rDNS validation settings or the PTR domain

block list, Trend Micro Email Security rejects the email message before the message body is sent over.

Note

If the IP address sending an email message matches the Approved IP address list of IP reputation, the email message bypasses revere DNS validation.

Configuring reverse DNS validation settings

Trend Micro Email Security allows you to configure rules for reverse DNS validation based on the sender domain, namely the domain in the **envelope address** of the email sender.

For each rule, Trend Micro Email Security supports two levels of reverse DNS validation:

- Whether there is a PTR record for the email sending IP address
- If a PTR record exists, whether the PTR record for the email sending IP address has a matching Address record (A record)

If the sender domain of an incoming message meets multiple rules, Trend Micro Email Security uses the most matched rule. For example, if you have configured the following three rules:

- Rule 1 for subdomain.example.com
- Rule 2 for *.example.com
- Rule 3 for *.subdomain.example.com

The match results for different incoming sender domains are as follows:

Incoming Sender Domain	Matched Rule
subdomain.example.com	Rule 1
a.example.com	Rule 2
a.subdomain.example.com	Rule 3
a.b.com	Default rule

Adding reverse DNS validation settings

Trend Micro Email Security allows you to add reverse DNS validation for sender domains.

Procedure

1. Go to **Inbound Protection** > **Connection Filtering** > **Reverse DNS Validation**.
2. Click the **Settings** tab, and click **Add** to configure reverse DNS validation rules for sender domains.

   Two rules are pre-configured:

   - Default (for unspecified domains): applies to all sender domains, except those for which you have configured a new reverse DNS validation rule.
   - Empty sender: applies to email messages with no envelope address specified.
3. On the **Add Reverse DNS Validation Settings** screen, specify a sender domain in one of the following formats:

   - example.com
   - subdomain.example.com
   - *.example.com

     This format matches all the subdomains under the example.com domain, for example, a.example.com, a.b.example.com.
4. Select **Reject for missing PTR** and/or **Reject for invalid PTR**.

   - **Reject for missing PTR**: Reject a message when its sending IP address has no PTR record.
   - **Reject for invalid PTR**: Reject a message when its sending IP address has a PTR record, but for the PTR record, there is no mapping A record, or the IP address in the A record does not match the sending IP address.

5. Click **Save**.

   The reverse DNS validation rule appears in the list on the **Settings** tab.

What to do next

To remove a rule, select a rule and click **Delete**. You can also select the checkbox in the table heading row to select all rules except the default rule and **Empty sender** rule, which you cannot delete.

Editing reverse DNS validation settings

Procedure

1. Go to **Inbound Protection** > **Connection Filtering** > **Reverse DNS Validation**.
2. Click the **Settings** tab.
3. From the list of reverse DNS validation domains, click a sender domain that you want to edit.
4. Modify the reverse DNS validation settings as required.

   Note

   For details about the settings, see *Adding reverse DNS validation settings on page 5-26*.

5. Click **Save**.

Configuring the blocked PTR domain list

When the domain in the PTR record of a sending IP address matches the blocked PTR domain list, Trend Micro Email Security rejects email messages from this IP address.

Adding PTR domains

Procedure

1. Go to **Inbound Protection** > **Connection Filtering** > **Reverse DNS Validation**.
2. Click the **Blocked PTR Domains** tab and click **Add**.
3. On the **Add Blocked PTR Domain** screen, configure information about the PTR domain from which you want to block messages.
   a. Specify a domain name in one of the following formats:
      - example.com
      - subdomain.example.com
      - *.example.com

        This format matches all the subdomains under the example.com domain, for example, a.example.com, a.b.example.com.

   b. Type a description for the domain.
   c. In the **Exception(s)** section, specify exceptions to the blocked PTR domain and click **Add**.

      The domains in the exception list must be subdomains of the blocked PTR domain. Trend Micro Email Security does not block messages from these subdomains.

      To delete an exception, select the exception item and click **Delete**.
   d. Click **Save**.

      The blocked PTR domain appears in the blocked PTR domain list.

What to do next

To remove a blocked PTR domain, select a PTR domain and click **Delete**. You can also select the checkbox in the table heading row to select all rules.

Editing PTR domains

Procedure

1. Go to **Inbound Protection** > **Connection Filtering** > **Reverse DNS Validation**.
2. Click the **Blocked PTR Domains** tab.
3. From the list of PTR domains, click a PTR domain that you want to edit.

   You can type the PTR domain name in the search box to find a PTR domain.
4. Modify the PTR domain settings as required.

   Note

   For details about the settings, see *Adding PTR domains on page 5-28*.
5. Click **Save**.

Domain-based authentication

Trend Micro Email Security provides authentication methods such as Sender IP Match, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) verification, and Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect against email spoofing.

If all these methods are enabled, Trend Micro Email Security evaluates email messages in the following order:

1. Sender IP Match
2. SPF check
3. DKIM verification
4. DMARC authentication

Trend Micro Email Security keeps evaluating and scanning an email message in the preceding order until encountering an “Intercept” action. If an email

message passes the Sender IP Match check, Trend Micro Email Security skips its own SPF check as well as the SPF check of DMARC authentication for this message.

Note

For details about intercept actions, see *"intercept" actions on page 6-59*.

Sender IP match

Trend Micro Email Security allows you to specify an IP address or a range of addresses within a sender domain identified by the **message header address** to allow email messages only from those addresses. Sender IP Match is a way that readily enables you to simultaneously allow all inbound email traffic from a particular domain while equally preventing spoofing by manually defining the allowed IP ranges.

If an email message passes the Sender IP Match check, Trend Micro Email Security skips its own SPF check as well as the SPF check of DMARC authentication for this message.

Adding sender IP match settings

To prevent sender forgery, you can specify a sender domain within the **message header address** and the allowed IP addresses for the domain.

Note

Trend Micro Email Security provides a built-in default rule that has the lowest priority to ensure you receive a baseline level of protection. The default rule cannot be deleted.

You can create only one single rule for each "Managed Domain". The default rule will be applied if no other rules are matched based on the "Managed Domain".

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **Sender IP Match**.
2. Click **Add**.

   The **Add Sender IP Match Settings** screen appears.
3. Select a specific recipient domain from the **Managed domain** drop-down list.
4. Select **Enable Sender IP Match**.
5. Under **Sender Domain-IP Paris**, add one or multiple domain-IP pairs.
   a. Specify a sender domain using one of the following formats:
      - example.com
      - subdomain.example.com
      - *.example.com

   b. Specify one or multiple IP addresses or IP/CIDR blocks to pair with the domain.

   c. Click **Add**.
6. Under **Intercept**, specify the action to take if the sender IP address does not match the sender domain as you specified.
   - **Delete entire message**
   - **Quarantine**
7. Under **Notify**, choose to send notifications and select at least one notification template.
8. Click **Add**.

Editing sender IP match settings

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **Sender IP Match**
2. From the list of sender IP match rules, click a managed domain to edit its settings.
3. Modify the sender IP match settings as required.

Note

For details about the settings, see *Adding sender IP match settings on page 5-30*.

4. Click **Save**.

Sender policy framework (SPF)

Sender Policy Framework (SPF) is an open standard to prevent sender address forgery. SPF protects the **envelope address** of a sender, which is used for the delivery of email messages. Trend Micro Email Security allows you to verify the sender's authenticity using SPF settings.

SPF requires the owner of a domain to publish the email sending policy (for example, which email servers are used to send email messages from that domain) in an SPF record in the Domain Name System (DNS).

When Trend Micro Email Security receives an email message claiming to come from that domain, Trend Micro Email Security checks the SPF record to verify whether the email message complies with the domain's stated policy. For example, if the message comes from an unknown server, the email message can be considered as fake.

Evaluation of an SPF record can return any of the following results.

RESULT	EXPLANATION	DEFAULT ACTION
Pass	The SPF record designates the host to be allowed to send.	Accept (reserved)
Fail	The SPF record has designated the host as not being allowed to send.	Delete (customizable)
SoftFail	The SPF record has designated the host as not being allowed to send but is in transition.	Accept (customizable)
Neutral	The SPF record specifies explicitly that nothing can be said about validity.	Accept (customizable)
None	The domain does not have an SPF record or the SPF record does not evaluate to a result.	Accept (customizable)
PermError	A permanent error has occurred (for example, badly formatted SPF record).	Accept (customizable)
TempError	A transient error has occurred.	Accept (customizable)

Note

By default, if an email message gets a "Pass" result, Trend Micro Email Security will bypass the SPF check and skip the remaining SPF settings for the message. Trend Micro Email Security will then continue scanning the message according to policy rules.

If an email message passes the Sender IP Match check, the message is also considered as passing its own SPF check.

Adding SPF settings

Trend Micro Email Security allows you to add SPF settings to validate an inbound message comes from the authorized IP address stated in the DNS record for the sender domain within the **envelope address**.

Note

Trend Micro Email Security provides a built-in default rule that has the lowest priority to ensure you receive a baseline level of protection. The default rule cannot be deleted.

You can create only one single rule for each “Managed Domain”. The default rule will be applied if no other rules are matched based on the “Managed Domain”.

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **Sender Policy Framework (SPF)**.
2. Click **Add**.

   The **Add SPF Settings** screen appears.
3. Select a specific recipient domain from the **Managed domain** drop-down list.
4. Select **Enable SPF** to enable SPF check in Trend Micro Email Security.
5. Optionally select **Insert an X-Header into email messages** to add the SPF check result into the email message's X-Header.

   Trend Micro Email Security adds messages similar to the following in email message's X-Header named **X-TM-Received-SPF**:

Status	X-Header
Pass	`X-TM-Received-SPF: Pass (domain of example_address@example.com designates 10.64.72.206 as permitted sender) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`

Status	X-Header
Fail	`X-TM-Received-SPF: Fail (domain of example_address@example.com does not designates 10.64.72.206 as permitted sender) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`
SoftFail	`X-TM-Received-SPF: SoftFail (domain of transitioning example_address@example.com discourages use of 10.64.72.206 as permitted sender) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`
Neutral	`X-TM-Received-SPF: Neutral (10.64.72.206 is neither permitted nor denied by domain of example_address@example.com) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`
None	`X-TM-Received-SPF: None (domain of example_address@example.com does not designate permitted sender hosts) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`
PermError	`X-TM-Received-SPF: PermError (domain of example_address@example.com uses mechanism not recognized by this client) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`

Status	X-Header
TempError	`X-TM-Received-SPF: TempError (error in processing during lookup of example_address@example.com) client-ip=10.64.72.206; envelope-from=example_address@example.com; helo=mailserver.example.com`

Note

If the value of `envelope-from` is blank, the value of `helo` will be used instead for the SPF check.

6. Under **Actions**, specify the action to take based on the SPF check result and select whether to tag the subject or send a notification for the message that fails SPF check.
7. Under **Tag and Notify**, customize the tag and select **Do not tag digitally signed messages** if necessary.

Note

The **Tag subject** action may destroy the existing DKIM signatures in email messages, leading to a DKIM verification failure by the downstream mail server. To prevent tags from breaking digital signatures, select **Do not tag digitally signed messages**.

8. Under **Ignored Peers**, do any of the following:
   - To add ignored peers to skip SPF check for a specific sender, specify the sender's domain name, IP address or CIDR block in the text box and click **Add**.

Note

Trend Micro Email Security will not implement SPF check for email messages from the specific domain, IP address or CIDR block. The email messages will continue to the next step in the regular delivery process.

However, this does not mean the email messages have passed SPF check. They will fail subsequent DMARC authentication if they do not actually meet specific criteria of the SPF standard.

- To search for existing ignored peers, type a keyword and click **Search**.
- To import ignored peers from a CSV file, click **Import**.

  The following import options are available:

  - **Merge**: append the ignored peers to the existing list.
  - **Overwrite**: replace the existing list with the ignored peers in the file.
- To export all ignored peers to a CSV file, click **Export**.

9. Click **Add** to finish adding the SPF settings.

Note

All the settings you added take effect only when you click **Add**.

Editing SPF settings

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **Sender Policy Framework (SPF)**.
2. From the list of domains to perform SPF record check, click a domain that you want to edit.

3. Modify the SPF settings as required.

Note

For details about the settings, see *Adding SPF settings on page 5-33*.

4. Click **Save**.

Domainkeys identified mail (DKIM)

DomainKeys Identified Mail (DKIM) is an email validation system that detects email spoofing by validating a domain name identity associated with a message through cryptographic authentication. In addition, DKIM is used to ensure the integrity of incoming messages or ensure that a message has not been tampered with in transit.

To ensure the validity and integrity of email messages, DKIM uses a public and private key pair system. A public and private key pair is created for the sending domain. The private key is stored securely on the mail server and used to sign outgoing messages. The public key is stored and published in DNS as a TXT record of the domain. When an email message is sent, the mail server uses the private key to digitally sign it, which is a part of the message header. When the email message is received, the DKIM signature can be verified against the public key on the domain's DNS.

Trend Micro Email Security implements DKIM authentication only in the following scenarios:

- Verifies DKIM signatures in incoming messages only when the domain specified in the “d=” tag of the DKIM signature header field belongs to the same organizational domain as the domain part of the “From” field in the message header.
- Adds DKIM signatures to outgoing message headers to prevent spoofing only when the domain part of the “From” field in the message header belongs to the same organizational domain as the MAIL FROM address (envelope sender).

Adding DKIM verification settings

Trend Micro Email Security verifies DKIM signatures in incoming email messages and allows administrators to take actions on messages that fail to pass signature verification. If a message's DKIM signature passes verification, the message will continue to the next step in the regular delivery process.

The DKIM verification settings apply only to the selected recipient domain.

Note

Trend Micro Email Security provides a built-in default rule that has the lowest priority to ensure you receive a baseline level of protection. The default rule cannot be deleted.

You can create only one single rule for each “Managed Domain”. The default rule will be applied if no other rules are matched based on the “Managed Domain”.

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Verification**.
2. Click **Add**.

   The **Add DKIM Verification Settings** screen appears.
3. Select a specific recipient domain from the **Managed domain** drop-down list.
4. Select **Enable DKIM verification**.
5. Optionally select **Skip DKIM verification for email messages with no envelope sender addresses**.
6. Optionally select **Insert an X-Header into email messages**.

   X-Header is added to indicate whether DKIM verification is successful or not.

Here are some examples of X-Header:

```
X-TM-Authentication-Results:dkim=pass; No signatures and
verification is not enforced
```

```
X-TM-Authentication-Results:dkim=pass; No processed
signatures and verification is not enforced
```

```
X-TM-Authentication-Results:dkim=fail; No processed
signatures but verification is enforced
```

```
X-TM-Authentication-Results:dkim=pass; Contain
verified signature, header.d=test.com, header.s=TM-
DKIM_201603291435, header.i=sender@test.com
```

```
X-TM-Authentication-Results:dkim=fail; No verified
signatures
```

7. Under **Intercept**, select an action that you want to take on a message that fails DKIM verification.
   - **Do not intercept messages**
   - **Delete entire message**
   - **Quarantine**
8. Under **Tag and Notify**, select further actions that you want to take on the message.
   - **Tag subject**

Note

Tags can be customized. When selecting the **Tag subject** action, note the following:

- This action may destroy the existing DKIM signatures in email messages, leading to a DKIM verification failure by the downstream mail server.
- To prevent tags from breaking digital signatures, select **Do not tag digitally signed messages**.

- **Send notification**

9. Under **Ignored Peers**, do any of the following:

   - To add ignored peers to skip DKIM verification for specific sender domains, specify one or multiple sender domain names, IP addresses, or CIDR blocks, and click **Add**.

     Trend Micro Email Security will not implement DKIM verification for email messages from the specific domain, IP addresses, or CIDR blocks. The email messages will continue to the next step in the regular delivery process.

     However, this does not mean the email messages have passed DKIM verification. They will fail subsequent DMARC authentication if they do not actually meet specific criteria of the DKIM standard.

     Note

     For ignored peers specified using domain names, Trend Micro Email Security uses senders' envelope addresses to match the domain names.

   - To search for existing ignored peers, type a keyword and click **Search**.
   - To import ignored peers from a CSV file, click **Import**.

     The following import options are available:

     - **Merge**: append the ignored peers to the existing list.
     - **Overwrite**: replace the existing list with the ignored peers in the file.

   - To export all ignored peers to a CSV file, click **Export**.

10. Under **Enforced Peers**, do any of the following:

    - Select **Use the header sender to match enforced peers**.

Note

The envelope sender address is always used for matching enforced peers.

Select this option when you want to use the sender address in the message header for matching as well.

- To add enforced peers to enforce DKIM verification for specific sender domains, specify one or multiple sender domain names and click **Add**.

  Each email message from the specified domain must meet specific criteria of the DKIM standard; otherwise, an action will be taken on the message.

  The following criteria must be met:

  - The sender domain must have a DKIM record.
  - There is at least one verified signature in the message.

- To search for, import or export enforced peers, perform similar operations as described in the previous step.

Note

- The ignored peer list takes precedence over the enforced peer list. If a message matches both the ignored peer list and enforced peer list, Trend Micro Email Security skips DKIM verification for the message.
- If you have enabled **Skip DKIM verification for email messages with no envelope sender addresses**, such email messages skip DKIM verification even if their header sender addresses match the enforced peer list.

11. Click **Add** to finish adding the DKIM verification settings.

Note

All the settings you added take effect only when you click **Add**.

Editing DKIM verification settings

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Verification**.
2. From the list of DKIM verification domains, click a domain that you want to edit.
3. Modify the DKIM verification settings as required.

Note

For details about the settings, see *Adding DKIM verification settings on page 5-39*.

4. Click **Save**.

Adding DKIM signing settings

Trend Micro Email Security supports DKIM signing for all outgoing messages from a specific domain. Recipients can verify that the email messages from the domain are authorized by the domain's administrator and that the messages, including attachments, have not been modified during transport.

The DKIM signing settings apply only to the selected sender domain.

Procedure

1. Go to **Outbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Signing**.
2. Click **Add**.

The **Add DKIM Signing Settings** screen appears.

3. Select a specific sender domain from the **Managed domain** drop-down list.
4. Select **Enable DKIM signing**.
5. Optionally select **Sign email messages with no envelope sender addresses**.

   For email messages with no envelope sender addresses (such as auto-reply messages or bounced messages), Trend Micro Email Security attempts to find the sender domain from the email header **From** and applies DKIM signing settings of the sender domain.
6. Configure general settings for DKIM signing.
   - **SDID**: select a signing domain identifier from the drop-down list.
   - **Selector**: selector to subdivide key namespace. Retain the default value.
   - **Headers to sign**: select one or multiple headers to sign and customize more headers if necessary.
   - **Wait time**: specify how long it takes for a key pair to take effect. Trend Micro Email Security starts to count the wait time once it finds the public key in the DNS.
   - **Key pair**: select a key length and click **Generate** to generate a key pair.

Note

Use the generated **DNS TXT record name** and **DNS TXT record value** to publish the public key to your DNS server.

If your domain provider supports the 2048-bit domain key length but limits the size of the TXT record value to 255 characters, split the key into multiple quoted text strings and paste them together in the TXT record value field.

7. Configure advanced settings for DKIM signing.
   - **Header canonicalization**: select **Simple** or **Relaxed**.
   - **Body canonicalization**: select **Simple** or **Relaxed**.

   Note

   Two canonicalization algorithms are defined for each of the email header and the email body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping.

   - **Signature expiration**: set the number of days that the signature will be valid.
   - **Body length**: set the number of bytes allowed for the email body.
   - **AUID**: specify the Agent or User Identifier on behalf of which SDID is taking responsibility.
8. Click **Add** to finish adding the DKIM signing settings.

Editing DKIM signing settings

Procedure

1. Go to **Outbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Signing**.
2. From the list of DKIM signing domains, click a domain that you want to edit.
3. Modify the DKIM signing settings as required.

Note

For details about the settings, see *Adding DKIM signing settings on page 5-43*.

If you regenerate a key pair, make sure you publish the new public key to your DNS server. Before the new public key takes effect, Trend Micro Email Security uses the old public key for signing. Therefore, make sure you do not delete the DNS record for the old key from your DNS server until the new DNS record takes effect.

4. Click **Save**.

Domain-based message authentication, reporting & conformance (DMARC)

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as email messages with forged sender addresses that appear to originate from legitimate organizations. It provides a way to authenticate email messages for specific domains, send feedback to senders, and conform to a published policy.

DMARC fits into the inbound email authentication process of Trend Micro Email Security. The way it works, is to help email recipients to determine if the purported message aligns with what the recipient knows about the sender. If not, DMARC provides guidance on how to handle the non-aligned messages. DMARC requires either of the following:

- A message passes the SPF check, and its identifier domain is in alignment.
- A message passes the DKIM signature check, and its identifier domain is in alignment.

Identifier alignment requires that the domain authenticated by SPF or DKIM be the same as or belong to the same organizational domain as the message header domain. If the alignment mode is “s” (strict), the two domains must

be exactly the same; if the alignment mode is “r” (relaxed), they must belong to the same organizational domain.

Note

If an email message passes the Sender IP Match check, the message is also considered as passing the SPF check of DMARC authentication.

However, some services like mailing lists or account forwarding (also known as intermediaries) might make changes to a legitimate message before sending it on, potentially resulting in SPF, DKIM, and/or DMARC alignment failure. Therefore, the message may not get delivered despite of its legitimacy.

Authenticated Received Chain (ARC) was designed to address such problem. ARC preserves email authentication results across subsequent intermediaries (“hops”) that may modify the message, and thus would cause email authentication measures to fail to verify when that message reaches its final destination. But if an ARC chain were present and validated, a receiver who would otherwise discard the messages might choose to evaluate the ARC results and make an exception, allowing legitimate messages to be delivered.

ARC-enabled intermediaries generally act as both ARC validators (when receiving messages) and ARC sealers (when sending messages onward, not originated locally).

When evaluating ARC results for validity as an ARC validator, Trend Micro Email Security currently evaluates only the following third-party ARC sealers:

- Google
- Microsoft

When signing the messages' validation results as an ARC sealer, Trend Micro Email Security uses the domain name "d=tmes.trendmicro.com" in the ARC headers. If the next hop intermediary is ARC-enabled, Trend Micro suggests that you enable the intermediary to add Trend Micro to its ARC sealer trust list.

Adding DMARC settings

Trend Micro Email Security authenticates incoming email messages of the selected domain and allows administrators to take actions on messages that fail to pass DMARC authentication. If DMARC authentication passes, the messages will be delivered normally. If DMARC authentication fails, the messages will be quarantined, rejected or delivered according to the DMARC settings.

The DMARC settings apply only to the selected recipient domain.

Note

Trend Micro Email Security provides a built-in default rule that has the lowest priority to ensure you receive a baseline level of protection. The default rule cannot be deleted.

You can create only one single rule for each “Managed Domain”. The default rule will be applied if no other rules are matched based on the “Managed Domain”.

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC)**.
2. Click **Add**.

   The **Add DMARC Settings** screen appears.
3. Select a specific recipient domain from the **Managed domain** drop-down list.
4. Select **Enable DMARC**.
5. Optionally select **Skip DMARC for email messages with no envelope sender addresses**.
6. Optionally select **Enable Authenticated Received Chain (ARC)**.

Trend Micro Email Security will successfully authenticate the email messages that fail DMARC authentication but pass ARC validation, and will also insert a set of ARC headers into these email messages.

Here is an example of a set of ARC headers:

```
ARC-Authentication-Results: i=2; tmes.trendmicro.com;
spf=temperror (sender IP address: 10.135.11.245)
smtp.mailfrom=example.com; dkim=none (no processed
signatures) header.d=none; dmarc=fail action=none
header.from=test.com; arc=pass

ARC-Message-Signature: i=2; a=rsa-sha256;
d=tmes.trendmicro.com; s=TM-DKIM-20200223173148;
t=1628750516; c=relaxed/relaxed;
bh=5ffn1pIbUBxx6CFHIVuU2HzEpEvAtzhWZ1Jz7ddgWws=;
h=Date:From:To:Subject:Message-ID:Content-Type;
b=cAaAR+7GtaByy8iSJiWo7GIf8T28Pjod3W2vWKcQWLH/
7YA4n0X51cSBlPwtTygfX otqfftTsCNIO1/
Xx5LtdE2KdVYZbVgrFo+WpDgtCXCLLw6sO7OsdsPSSPbcpEq8r6q
ERfAqu5TNDLaj2+cR197bBhUFYVDJDe7pbfNaAy2g8GL3gOGrkWQcYw1DrR
WXeOSEi
3i59afFHqH3LOY4cmlyWDpZxyDhhn7Rhb3ZNlw9aUuQtMj7iaXkxQaC1M/
T6bxLEAE XXV4jczaONiJ/
5XmsPlR0gvHr0SpC42isWxElyXr2J1C93HgeAmK1Db4JAOGV2mXMF
I3fzA7jbSSLag==

ARC-Seal: i=2; a=rsa-sha256; d=tmes.trendmicro.com; s=TM-
DKIM-20200223173148; t=1628750516; cv=pass; b=LKQY/
mrwXnJKLJIclybRcGQyWziCvHqIFBAZAYtTlz1aYQ2EiHaXaLbkmokgF8ib
C zj5UwsJrIj20lpm0aB+qKDoy4Psme/
I3JZNDa5B1OeLHvkcubfUq9bzfSZadkN/dWC N9FfbNSQwiZ0+
+SOLVwYCcIqh9PkWcfIJa7bo4sP7aUZjJkcXutfcm0q94J9j4fIgz
HWxEh58pvjtuMrSKCVCyMIODGoEYa1EbD2EbiTI7iZ54VfPXHjR79b0+21x
ppZbVEN
0QZGWYuuCoLUrIWDhPzS0kyYyIumPIh4RLe8sMKaBrKECo89XU+BjfNuwZp
APJs/id Q6RbaHHVtp8XA==
```

7. Optionally select **Insert an X-Header into email messages**.

   X-Header is added to indicate whether DMARC authentication is successful or not.

   Here are some examples of X-Header:

   ```
   X-TM-Authentication-Results: spf=pass (sender IP address:
   10.210.128.20) smtp.mailfrom=example.com; dkim=pass
   (signatures verified) header.d=example.com; dmarc=pass
   action=none header.from=example.com; arc=none
   ```

   ```
   X-TM-Authentication-Results: spf=fail (sender IP address:
   10.204.148.40) smtp.mailfrom=example.com; dkim=fail (no
   verified signatures found) header.d=example.com; dmarc=fail
   action=none header.from=example.com; arc=none
   ```

   ```
   X-TM-Authentication-Results: spf=fail (sender IP address:
   10.204.148.40) smtp.mailfrom=example.com; dkim=pass
   (signatures verified) header.d=example.com; dmarc=pass
   action=none header.from=example.com; arc=pass
   ```

   ```
   X-TM-Authentication-Results: spf=pass (sender IP address:
   10.204.128.20) smtp.mailfrom=example.com; dkim=fail (no
   verified signatures found) header.d=example.com; dmarc=pass
   action=none header.from=example.com; arc=pass
   ```

8. Optionally select **Deliver daily reports to senders**.

   If you select this option, aggregated reports will be generated daily for authentication failures and sent back to email senders.

9. Under **Intercept**, specify actions to take on messages that fail DMARC authentication.

   A DMARC tag instructs recipients how to handle email messages that fail DMARC authentication. There are three values for the tag: "none", "quarantine", and "reject". Trend Micro Email Security enables you to specify the action to take in each scenario based on the instructions:

   - **None**: select the action to take when the DMARC tag value is "none".

- **Quarantine**: select the action to take when the DMARC tag value is "quarantine".
- **Reject**: select the action to take when the DMARC tag value is "reject".
- **No DMARC records**: select the action to take when there is no DMARC records.

10. Under **Tag and Notify**, select further actions that you want to take on the messages.

    - **Tag subject**

    Note

    Tags can be customized. When selecting the **Tag subject** action, note the following:

    - This action may destroy the existing DKIM signatures in email messages, leading to a DKIM verification failure by the downstream mail server.
    - To prevent tags from breaking digital signatures, select **Do not tag digitally signed messages**.

    - **Send notification**

11. Under **Ignored Peers**, do any of the following:

    - To add ignored peers to skip DMARC authentication for specific sender domains, specify one or multiple sender domain names, IP addresses, or CIDR blocks, and click **Add**.

      Trend Micro Email Security will not implement DMARC authentication for email messages from the specific domains, IP addresses, or CIDR blocks. The email messages will continue to the next step in the regular delivery process.

Note

For ignored peers specified using domain names, Trend Micro Email Security uses senders' envelope addresses to match the domain names.

- To search for existing ignored peers, type a keyword and click **Search**.
- To import ignored peers from a CSV file, click **Import**.

  The following import options are available:

  - **Merge**: append the ignored peers to the existing list.
  - **Overwrite**: replace the existing list with the ignored peers in the file.
- To export all ignored peers to a CSV file, click **Export**.

12. Under **Enforced Peers**, do any of the following:

    - Select **Use the header sender to match enforced peers**.

      Note

      The envelope sender address is always used for matching enforced peers.

      Select this option when you want to use the sender address in the message header for matching as well.

    - To add enforced peers to enforce DMARC authentication for specific sender domains, specify one or multiple sender domain names and click **Add**.

      Each email message from the specified domain must meet specific criteria of the DMARC standard; otherwise, an action will be taken on the message.

      The following criteria must be met:

- The sender domain has a DMARC record.
- The message passes the SPF check, and its identifier domain is in alignment. Alternatively, the message passes DKIM verification, and its identifier domain is in alignment.

- To search for, import or export enforced peers, perform similar operations as described in the previous step.

Note

- The ignored peer list takes precedence over the enforced peer list. If a message matches both the ignored peer list and enforced peer list, Trend Micro Email Security skips DMARC verification for the message.
- If you have enabled **Skip DMARC for email messages with no envelope sender addresses**, such email messages skip DMARC verification even if their header sender addresses match the enforced peer list.

13. Click **Add** to finish adding the DMARC settings.

Note

All the settings you added take effect only when you click **Add**.

Editing DMARC settings

Procedure

1. Go to **Inbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC)**.
2. From the list of DMARC authentication domains, click a domain that you want to edit.

3. Modify the DMARC settings as required.

Note

For details about the settings, see *Adding DMARC settings on page 5-48*.

4. Click **Save**.

Monitoring DMARC

Monitoring DMARC setup

Monitor whether your configurations for implementing DMARC is complete and quickly review the current DMARC policy tag setting for domains.

To maximize the benefits of your DMARC enforcement, Trend Micro Email Security also helps you implement Brand Indicators for Message Identification (BIMI), allowing your brand's logo to appear alongside the emails you send. This enables your customers to see your logo in their inbox, helping to eliminate online impersonators, build customer trust, and increase the likelihood that your emails are opened.

Procedure

1. Go to **Outbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC) Monitoring**.
2. Go to **DMARC Record Check**.
3. Optionally specify the search criteria and click **Search**.
4. Check the DMARC setup status for the managed domains.

Item	Description
Managed domain	Domain protected by Trend Micro Email Security. All protected domains are listed in the table.

Item	Description
Outbound Protection	Whether outbound protection is enabled for the domain. • Enabled • Disabled To enable outbound protection, go to **Domains**, click the domain, and select **Enable outbound protection** on the displayed screen for editing domain information.
SPF	Whether SPF is enabled for the domain. • Enabled • Disabled SPF is disabled in either of the following scenarios: • No SPF record is available for the domain. • The Trend Micro Email Security server is not included in the SPF record. To enable SPF, depending on your scenario, set up an SPF record for the domain or add the Trend Micro Email Security server address to the SPF record for the domain. You can click **Disabled** to go to the **Domains** screen and follow the onscreen instructions for SPF setup in the **Outbound Servers** section. For more information, see *Adding SPF records on page 4-14*.

Item	Description
DKIM	Whether DKIM is enabled for the domain. • Enabled • Disabled DKIM is disabled in any of the following scenarios: • The DKIM record is not published or is published incorrectly. • The DKIM record is published but is still being propagated. DKIM is enabled after the DKIM record propagation is completed. • No DKIM signing policy is created in Trend Micro Email Security. • The DKIM signing policy is disabled in Trend Micro Email Security. To enable DKIM, depending on your scenario, check the publish of your DKIM record for the domain, or click **Disabled** to go to the **DKIM Signing** screen and *create or enable a DKIM signing policy for the domain on page 5-43*.

Item	Description
DMARC	Whether DMARC is enabled for the domain. • Enabled The screen also shows the policy tag specified in the DMARC record, which can be none, quarantine, or reject, and whether the policy is inherited from an organizational domain, You can click **Enabled** to view the details about the published DMARC record. If you want to update the DMARC record, click **Modify** to generate a new record and publish it to the DNS server. For details about DMARC record options, see *Generating a DMARC record on page 5-59*. • Disabled DMARC is disabled in any of the following scenarios: • No DMARC record is available for the domain. • No policy tag is specified in the DMARC record. To enable DMARC, depending on your scenario, set up a DMARC record for the domain or specify a policy tag in the DMARC record. Trend Micro Email Security provides a DMARC record generator to facilitate your DMARC setup. You can click **Disabled** to create a DMARC record for the domain. For details, see *Generating a DMARC record on page 5-59*.

Item	Description
BIMI	Whether BIMI is enabled for the domain. • Enabled Though enabled, BIMI may not work properly in the following scenarios: • No Verified Mark Certificate (VMC) is provided. • DMARC policy for the domain and the organizational domain (if different) is not enforced. **Note** BIMI only works when the DMARC policy for the domain and the organizational domain (if different) is at enforcement. • Disabled BIMI is disabled in any of the following scenarios: • No BIMI record is available for the domain. • The BIMI record is published incorrectly. • The SVG image or VMC certificate provided in BIMI record generation is invalid. To make BIMI work, depending on your scenario, update your DMARC record or generate a BIMI record for the domain. Trend Micro Email Security provides a BIMI setup wizard where you can view the details about your DMARC and BIMI status and update the problematic record. You can click **Enabled** or **Disabled** to open the BIMI setup wizard. Trend Micro Email Security also provides a BIMI record generator to facilitate your BIMI setup. For details, see *Generating a BIMI record and Implementing BIMI on page 5-63*.

Generating a DMARC record

Procedure

1. Go to **Outbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC) Monitoring**.
2. Go to **DMARC Record Check**.
3. Generate a DMARC record for a domain.
   - For a domain with DMARC disabled, click **Disabled** in the **DMARC** column and then click **Create** on the **DMARC Record in DNS** screen to generate a DMARC record.
   - For a domain with DMARC enabled, click **Enabled** in the **DMARC** column and then click **Modify** on the **DMARC Record in DNS** screen to update the DMARC record options and generate a new record.
4. On the **Generate DMARC Record** screen, specify the basic options.

Note

If you leave an option empty, the corresponding tag does not appear in the resulting DMARC record.

Option	Description
Policy	The action that you expect the receiving server to take when messages from the domain fail DMARC checks. • None: Take no action on messages failing DMARC checks. This action only helps collect DMARC reports and gain insight into your current email flows and their authentication status. • Quarantine: Treat the messages failing DMARC checks as suspicious. The specific action depends on the capability of the receiving server. For example, the action can be placing the message into a spam folder or in a quarantine area. • Reject: Reject messages failing DMARC checks. You must specify a value for this option.
Send Aggregate Data to	The email address for receiving DMARC aggregate reports. Use a comma to separate multiple email addresses. Optionally, you can specify the maximum email size allowed in the format *Email address*!*Size limit*. Example: `dmarc-feedback@example.com,dmarc-admin@example.com!10m` If you leave this option empty, you will not receive aggregate reports.
Send Forensic Data to	The email address for receiving DMARC forensic reports, which are also called failure reports. Use a comma to separate multiple email addresses. Optionally, you can specify the maximum email size allowed in the format *Email address*!*Size limit*. Example: `dmarc-feedback@example.com,dmarc-admin@example.com!10m` If you leave this option empty, you will not receive forensic reports.

5. Optionally specify the advanced options.

Note

If you leave an option empty or select the "-" value, the corresponding tag does not appear in the resulting DMARC record.

Option	Description
Subdomain Policy	The policy you want to apply to all the subdomains of a domain. The value "-" indicates unspecified. In this case, the policy for subdomains is the same as the policy for the primary domain. Change the setting if you want to use a different DMARC policy for your subdomains.
DKIM Identifier Alignment	The alignment policy for DKIM, which defines how strictly the DKIM alignment check is. • -: Unspecified. In this case, the policy "Relaxed" applies during DMARC evaluation. • Relaxed: Partial match is allowed. The sender domain name can be a valid subdomain of the domain name in the "d=" tag in the DKIM mail header. • Strict: The sender domain name must be identical to the domain name in the "d=" tag in the DKIM mail header.
SPF Identifier Alignment	The alignment policy for SPF, which defines how strictly the SPF alignment check is. • -: Unspecified. In this case, the policy "Relaxed" applies during DMARC evaluation. • Relaxed: Partial match is allowed. The sender domain name can be a valid subdomain of the domain name in the SMTP "MAIL FROM" command. • Strict: The sender domain name must be identical to the domain name in the SMTP "MAIL FROM" command.
Reporting Interval	The interval for the receiving server to send aggregate reports. If you leave this option empty, the interval "86400 seconds" (24 hours) applies during DMARC evaluation.

Option	Description
Forensic Report Options	The conditions for sending forensic reports. • Send report only if both SPF and DKIM fail • Send report if either SPF or DKIM fails • Send report if DKIM fails • Send report if SPF fails If you leave this option unspecified, the condition "Send report only if both SPF and DKIM fail" applies during DMARC evaluation.
Forensic Report Format	The format in which reports are sent, which can be AFRF or IODEF. The value "-" indicates unspecified, in which case the format AFRF applies during DMARC evaluation.
Policy Percentage	The percentage of unauthenticated messages to which the DMARC policy will be applied. Specify an integer between 0 and 100. To roll out DMARC slowly, it is recommended that you start with a small percentage. As more messages from your domain pass DMARC checks, you can move to a higher percentage until you reach 100 percent. If you leave this option empty, the value 100 applies during DMARC evaluation.

6. Click **Generate**.

   Trend Micro Email Security generates a DMARC record based on your settings. You can copy the record and publish it to the DNS server.

   Example record: `v=DMARC1; p=none; sp=quarantine; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-fail-reports@example.com; adkim=s; aspf=r; ri=86400; fo=0; rf=afrf; pct=50`

   - `v=DMARC1`: This is version 1 of the DMARC specification.

     This tag is automatically added during the record generation.

- `p=none`: The policy for the primary domain is none, which indicates only monitoring messages from the domain for DMARC authentication.
- `sp=quarantine`: The policy for subdomains is quarantine, which indicates that you expect the receiving server to treat the messages from the subdomains of the primary domain as suspicious.
- `rua=mailto:dmarc-reports@example.com`: The email address for receiving aggregate reports is dmarc-reports@example.com.
- `ruf=mailto:dmarc-fail-reports@example.com`: The email address for receiving aggregate reports is dmarc-fail-reports@example.com.
- `adkim=s`: The DKIM alignment policy is to apply strict DKIM alignment checks.
- `aspf=r`: The SPF alignment policy is to apply relaxed SPF alignment checks.
- `ri=86400`: The interval for sending reports is 86400 seconds.
- `fo=0`: The condition for sending forensic reports is only when both SPF and DKIM fail.
- `rf=afrf`: The format for sending forensic reports is AFRF.
- `pct=50`: The policy will be applied to 50% of the messages.

Generating a BIMI record and Implementing BIMI

Use the BIMI setup wizard to generate a BIMI record and ensure your BIMI implementation works properly.

BIMI only works when the DMARC policy for the domain and the organizational domain (if different) is at enforcement.

Before implementing, make sure you have completed the following:

Prerequisite	Description
Implement DMARC authentication on all your emails	• Emails must pass DMARC validation checks. • The policies for the domain and the organizational domain (if different) must be set to either **Quarantine** with a **policy percentage** of `100` or **Reject**.
Produce an SVG Tiny PS version of your official logo	• The file must be a valid SVG or SVGZ file. • The file cannot be larger than 32 KB. • The file must be validated against the Scalable Vector Graphics (SVG) Tiny PS Specification • For more requirements, see BIMI documentation at https://bimigroup.org/.
(Optional, but highly recommended) Acquire a Verified Mark Certificate (VMC) for your logo	• The VMC must be valid and not expired. • The VMC Mark Type must be supported. • The VMC must include the Extended Key Usage. • The SAN dNSName domain name in the VMC must match that in the BIMI record. • The VMC's certificate chain must be validated using the Root Certificate from the accepted Mark Verifying Authorities: Entrust DataCard or DigiCert • Experimental VMC elements not accepted. • The SVG content in the VMC must match that in the BIMI record. • For more requirements, see BIMI documentation at https://bimigroup.org/.

Procedure

1. Go to **Outbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC) Monitoring**.
2. Go to **DMARC Record Check**.
3. View the status of BIMI for the domain, and then click **Enabled** or **Disabled** to open the BIMI setup wizard.

4. Check whether a DMARC record has been published in DNS for the domain or whether the DMARC policy for the domain and the organizational domain (if different) is enforced. If not, *generate a DMARC record or update the current DMARC record on page 5-59*, and then publish it in DNS.

   Updating the DMARC or BIMI setup takes some time. You can click **Refresh** to get the latest status.

5. Check whether a BIMI record has been published in DNS for the domain or whether the published BIMI record is invalid. If not, click the hyperlink to open the BIMI record generator screen.

6. Specify the URLs to your SVG image and VMC certificate, and click **Generate and Preview**.

   Trend Micro Email Security uses the **default** selector to generate and validate the BIMI record in DNS.

7. Click **Generate and Preview**.

   Trend Micro Email Security generates a BIMI record based on your settings and displays it in the **BIMI Record** area.

   Example record: `v=BIMI1; l=https://example.com/logo.svg; a=https://example.com/cert.pem`

   - `v=BIMI1`: This is version 1 of the BIMI specification.

     This tag is automatically added during the record generation.

   - `l=https://example.com/logo.svg`: The secure URL of where your SVG image is hosted.

   - `a=https://trendmicro.com/cert.pem`: The secure URL of where your VMC certificate is hosted.

8. View the details or possible errors about the provided SVG image and VMC certificate in the **Preview** area.

9. If the BIMI record is generated successfully without any SVG image or VMC errors, copy the record and publish it as a TXT record at the subdomain of **default._bimi.example.com** in DNS.

When a mailbox provider receives an email, it first authenticates the message. If the authentication is successful, the provider checks the DNS for a corresponding BIMI record. An email receiver wishing to query for BIMI policy regarding emails with **example.com** and a selector **default** would query the TXT record located at the subdomain of **default._bimi.example.com**. If a BIMI record is found, the provider can display your brand's logo alongside the email in the inbox.

You can track the effects of your BIMI implementation to know whether the clicks and open rates of your emails have been increased.

Analyzing DMARC reports

Monitor the DMARC authentication trends and anomalies for your domains by using the DMARC Report Analysis feature

Enable DMARC Report Analysis to send DMARC reports to Trend Micro Email Security for analysis. Get easily readable analysis results to monitor trends and identify anomalies in emails sent on behalf of your managed domains.

Procedure

1. Go to **Outbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC) Monitoring**.
2. Go to **DMARC Report Analysis**.
3. Check whether your have configured DMARC records for your domains to send DMARC reports to Trend Micro Email Security by clicking **Reporting Configuration**.

   If you haven't, you can following the on-screen instructions to update your DMARC records.

   The Trend Micro Email Security address for receiving DMARC reports is as follows for each serving site:

Serving Site	Report Receiving Address
North America, Latin America and Asia Pacific	%company_identifier%@dmarcrua.tmes.trendmicro.com
Europe and Africa	%company_identifier%@dmarcrua.tmes.trendmicro.eu
Australia and New Zealand	%company_identifier%@dmarcrua.tmes-anz.trendmicro.com
Japan	%company_identifier%@dmarcrua.tmems-jp.trendmicro.com
Singapore	%company_identifier%@dmarcrua.tmes-sg.trendmicro.com
India	%company_identifier%@dmarcrua.tmes-in.trendmicro.com
Middle East (UAE)	%company_identifier%@dmarcrua.tmes-uae.trendmicro.com

To generate a new DMARC record, you can use the built-in DMARC record generator by clicking **Generate DMARC Record** and following on-screen instructions.

After your DMARC record is updated for DMARC reporting, you can click **Verify** to check whether the new DMARC record has taken effect.

Note

You need to wait because DMARC record update takes some time to propagate across DNS servers.

4. Check the DMARC report analysis results for your domains by clicking the other tabs under **DMARC Report Analysis**.

   Based on received DMARC reports, Trend Micro Email Security generates results to show the DMARC compliance check results and more DMARC authentication details about emails sent on behalf of your domains.

Tab Name	Description	Action
Overview	Displays the DMARC compliance check result for each managed domain. **Note** • The results only show the domains whose DMARC records you have configured to send DMARC reports to Trend Micro Email Security. • Trend Micro Email Security regards an email as passing DMARC compliance checks when the email passes either SPF authentication and alignment check or DKIM authentication and alignment check.	• Filter the results by specifying the managed domain name and time period and clicking **Search**. • View the DMARC compliance check result for a managed domain by sending source by clicking **View by sending source** in the **Action** column. • View more details about the DMARC compliance check by clicking **View details** in the **Action** column.

Tab Name	Description	Action
By Sending Source	Displays the DMARC compliance check result by sending source. A sending source is the email service that sends emails on behalf of a managed domain. Click the right arrow icon () next to the sending source to view the results for each host and IP address that the email service uses for sending emails.	• Filter the results by specifying the managed domain name, sending source, and time period and clicking **Search**. **Note** • For the sending email service, type the exact domain name used by the email service or use wildcards (*) to represent any part of the name. • For the sending hostname, type the exact hostname or use wildcards (*) to represent any part of the name. • For the sending IP address, type an IP address, CIDR block, or the beginning part of an IP address.

Tab Name	Description	Action
		• View more details about the DMARC compliance check for emails from a sending source by clicking **View details** in the **Action** column.
Details	Displays the DMARC compliance check details, including the check result, the sending sources, the disposition of an email by the receiving server, and the SPF/ DKIM authentication details.	Filter the results by specifying the search criteria and clicking **Search**. **Note** • For the sending email service, type the exact domain name used by the email service or use wildcards (*) to represent any part of the name. • For the sending hostname, type the exact hostname or use wildcards (*) to represent any part of the name. • For the sending IP address, type an IP address, CIDR block, or the beginning part of an IP address.

How DMARC works with SPF and DKIM

SPF, DKIM and DMARC are three independent features in Trend Micro Email Security. You can enable or disable those features based on your requirements.

The following are typical scenarios for your reference:

- DMARC enabled only

  Trend Micro Email Security performs its own SPF check and DKIM signature check before alignment check.

- SPF check, DKIM verification and DMARC authentication enabled at the same time

  Trend Micro Email Security checks the sender domain for each inbound email message. If a message does not pass the SPF check, the message will be deleted, quarantined or delivered depending on the action configured.

  If the message passes the SPF check, Trend Micro Email Security verifies DKIM signatures in the message. If the message does not pass DKIM verification, the message will be deleted, quarantined or delivered depending on the action configured.

  If the message continues to the next step in the delivery process, Trend Micro Email Security implements DMARC authentication on the message.

File password analysis

By leveraging a combination of user-defined passwords and message content (subject, body and attachment names), Trend Micro Email Security can heuristically extract or open password-protected files, namely, archive files and document files, in email messages to detect any malicious payload that may be embedded in those files.

You can add or import user-defined passwords to help Trend Micro Email Security efficiently extract or open password-protected files for further scanning.

Note

File password analysis is only applied for virus scan, and not for DLP or content filtering.

Trend Micro Email Security supports the following password-protected archive file types:

- 7z
- rar
- zip

Trend Micro Email Security supports the following password-protected document file types:

- doc
- docx
- pdf
- pptx
- xls
- xlsx

Configuring file password analysis

Procedure

1. Choose **Inbound Protection** > **Virus Scan** > **File Password Analysis**.
2. In the **File Password Analysis Settings** section, select **Enable file password analysis**.
3. Optionally select **Hold on a message to associate later messages for password analysis** and specify a certain amount of time for **Analysis timeout**.

Note

This step is required if you want Trend Micro Email Security to associate later email messages to further analyze the file password for the current email message. The current message will not be released for delivery during the analysis timeout period.

4. Click **Save**.

To help Trend Micro Email Security crack file passwords more efficiently, you can add or import passwords that are commonly used by your organization as the user-defined passwords. Trend Micro Email Security will try the user-defined passwords first before any other ways to extract or open files.

Adding user-defined passwords

A maximum of 100 passwords is allowed.

Procedure

1. In the **User-Defined Passwords** section, click **Add**.

   The **Add Password** dialog box appears.

2. Type a priority value next to **Priority** for the new password.

Note

The priority value ranges from 1 to 100.

The lower the priority value, the higher the priority.

3. Type a password with only ASCII characters.
4. Click **Save**.

   The password you added appears in the user-defined password list.

   If there are multiple passwords, you can click the up or down arrow next to **Priority** to sort the passwords by priority level. To delete one

or multiple passwords, select the check box of each password and click **Delete**.

Importing user-defined passwords

A maximum of 100 passwords is allowed.

Procedure

1. In the **User-Defined Passwords** section, click **Import**.

   The **Import Passwords** dialog box appears.

2. Next to **File location**, browse and select a TXT file to import.

   You can click **Download sample file** to view a sample of a properly formatted file.

   Trend Micro Email Security checks all the entries in the selected file to identify any invalid, duplicate or conflicting passwords.

3. After you confirm all the entries to be imported, click **Import**.

Configuring scan exceptions

Under certain circumstances, you may want to prevent Trend Micro Email Security from scanning certain types of messages that may pose security risks. For example, compressed files provide a number of special security concerns since they can harbor security risks or contain numerous compression layers. Scan exceptions are configured to instruct Trend Micro Email Security to take actions on these messages.

Note

If an email message triggers the scan exception "Malformed messages", Trend Micro Email Security stops scanning and takes the corresponding actions.

If any other scan exception is triggered, Trend Micro Email Security takes the specified actions and will not stop scanning until encountering a terminal scan action. For details about terminal actions, see *"intercept" actions on page 6-59*.

Scan exception list

Trend Micro Email Security allows you to configure different types of exceptions. If an email message meets any of the following conditions, Trend Micro Email Security will trigger an exception and take the specified actions:

- The number of files in a compressed file exceeds 353.
- The decompression ratio of a compressed file exceeds 100.

  Note

  The decompression ratio refers to the ratio between a decompressed file's size and its original compressed size. For example, for a 1 MB compressed file, if the decompressed file size is 100 MB, the ratio would be 100 to 1, which is equivalent to 100.

- The number of decompression layers in a compressed file exceeds 20.

  Trend Micro Email Security checks for malware "smuggled" within nested compressions and supports scanning up to 20 recursive compression layers.

- The size of a single decompressed file exceeds 60 MB.
- An Office file of version 2007 or later contains more than 353 subfiles.

Note

An Office file of version 2007 or later is actually a zip archive of XML files. Therefore, Trend Micro Email Security treats such an Office file as a compressed file and triggers an exception when the Office file consists of more than 353 files.

- An Office file of version 2007 or later contains a subfile whose decompression ratio exceeds 100.
- Malformed messages.
- Virtual Analyzer scan exception.

  Possible scenarios include:

  - Cloud sandbox analysis timed out.
  - Unable to connect to the cloud sandbox.
  - The available sandbox images do not support the file format.
  - The extracted or downloaded file exceeds the file size limit.
  - Unable to access the URL.
  - The URL is invalid.
- Virtual Analyzer submission quota exception.

Note

The Virtual Analyzer scan exception and submission quota exception are available only in inbound protection.

These settings are not included in the Trend Micro Email Security Standard license.

For details about different license versions, see *Available license versions on page 1-26*.

Configuring "scan exceptions" actions

To configure centralized scan exception settings, go to the following paths:

- **Inbound Protection** > **Virus Scan** > **Scan Exceptions**
- **Outbound Protection** > **Virus Scan** > **Scan Exceptions**

Scan exceptions under **Inbound Protection** apply to incoming messages, while scan exceptions under **Outbound Protection** apply to outgoing messages. The scan actions configured for each exception apply to all senders and recipients.

Specify actions for Trend Micro Email Security to take on email messages that meet the scan exception criteria.

Procedure

1. On the **Scan Exceptions** screen, click the action name for an exception in the **Actions** column.

   The **Select Scan Exception Actions** screen appears.

2. Configure **Intercept** settings.

Action	Description
Do not intercept messages	Trend Micro Email Security does not take action on the message and processes the message using other policy rules if other policy rules apply.
Delete entire message	Trend Micro Email Security deletes the message, including its attachments.
Quarantine	Trend Micro Email Security moves the message into quarantine.

3. Configure **Modify** settings.

Action	Description
Tag subject	a. Select the **Tag subject** action to insert configurable text into the message subject line. b. Type a tag in the **Tag** field, for example, `Spam`. c. Optionally select **Do not tag digitally signed messages.** to prevent tags from breaking digital signatures.
Insert X-Header	a. Select **Insert X-Header** to add an X-Header to the header of a message. b. Type the X-Header name and value. **Note** Do not use or start your X-Header name (case-insensitive) with the following since they are reserved for Trend Micro Email Security: • X-TM • X-MT The reserved X-Headers might be adjusted dynamically if necessary.

4. Configure **Monitor** settings.

   a. Select the **Send notification** action.

   b. Click the **message to people** link.

      The **Notifications** screen appears.

   c. Select a notification message from the **Available** pane on the left side and click **Add>**.

The **Add**, **Edit**, **Copy** and **Delete** buttons under **Available** are provided for managing notification messages. For details about managing notifications, see *Managing notifications on page 10-25*.

d. Click **Save** to save the notification setting.

Note

The **Modify** and **Monitor** settings are not mandatory.

5. Click **Save**.

Note

If multiple scan exceptions are triggered for one email message, Trend Micro Email Security chooses the action with the highest priority from the configured "Intercept" actions, combines the action with the "Modify" and "Monitor" actions, and performs those actions together on the message.

"Intercept" actions are listed as follows in descending order of priority:

- **Delete entire message**
- **Quarantine**
- **Do not intercept messages**

High profile domains

Trend Micro Email Security allows you to specify high profile external domains, for example, your partners' domains or domains of famous brands, which are likely to be forged into cousin domains for spam, phishing, and BEC attacks, for example, vendor frauds.

A cousin domain (or look-alike domain) is a domain that looks deceptively similar to a legitimate target domain, which is well-known or familiar to users. Cousin domains are often used in phishing attacks to steal sensitive or confidential information from users. Cousin domains are usually created by replacing one or more characters (for example, replacing the letter "l" with

the number "1") or adding or removing an extra character in the domain name. Without careful inspection of the email addresses, users may not notice the trick and think that an email message is sent from a legitimate domain being forged.

By leveraging the Trend Micro Antispam Engine, Trend Micro Email Security can scan domains in email messages (the from and replyto headers) based on the settings you configure to detect cousin domains of these high profile domains and prevent users from spam, phishing and BEC messages.

Configuring high profile domains

Specify legitimate sender domains that might be frequently forged into cousin domains for spam, phishing, and BEC attacks. Trend Micro Email Security will detect email messages from cousin domains of the specified high profile domains.

Procedure

1. Go to **Inbound Protection** > **Spam Filtering** > **High Profile Domains**.
2. In the **High Profile Domain Settings** section, enable high profile domains, select a detection threshold, and click **Save**.
   - **Aggressive**: This option provides the most number of detections based on fuzzy matches. This is the most rigorous level of spam, phishing, and BEC detection.
   - **Normal**: This is the default and recommended setting. This option provides a moderate number of detections.
   - **Conservative**: This option provides the most accurate detections based on near-exact matches.
3. In the **High Profile Domains** section, maintain a list of legitimate sender domains.
   - Click **Add** to add a high profile domain. Specify the domain name, for example, `domain.com` for the high profile domain.

     Wildcard characters and regular expressions are not supported.

Note

You can add a maximum of 100 high profile domains.

- Click **Delete** to delete a high profile domain.
- Click **Import** to import high profile domains from a TXT file.

  The following import options are available:

  - **Merge**: append the high profile domains to the existing list.
  - **Overwrite**: replace the existing high profile domain list with the domains in the file.
- Click **Export** to export the high profile domain list to a TXT file.

4. In the **Exception List** section, maintain a list of domains that Trend Micro Email Security excludes from scanning for cousin domains.

Note

You can add a maximum of 1,000 domains to the exception list.

High profile users

In Business Email Compromise (BEC) scams, a fraudster impersonates a high profile executive, for example, the CEO or CFO, and attempts to trick an employee, a customer, or a vendor into transferring funds or sensitive information to the fraudster.

Trend Micro Email Security allows you to add high profile users who are likely to be impersonated for detection and classification.

Trend Micro Email Security also integrates with Trend Micro's Writing Style DNA as an additional layer of protection for your organization's users against BEC threats. For more information, see *Configuring Business Email Compromise criteria on page 6-23*.

Note

Writing Style DNA is not included in the Trend Micro Email Security Standard license.

For details about different license versions, see Available License Versions.

Configuring high profile users

Specify the email display names of the high profile users who might be frequently forged. Trend Micro Email Security will check incoming email messages claimed to be sent from those users and apply fraud checking criteria to identify forged messages. Trend Micro Email Security enables you to take actions on the BEC attacks that are detected or suspected by the Antispam Engine or detected by writing style analysis.

The specified high profile users are applicable to all BEC policies of your domains as the global settings.

Procedure

1. Go to **Inbound Protection** > **Spam Filtering** > **High Profile Users**.
2. From the **Source** drop-down list, select either of the following:
   - **Synchronize users from Directory**: select this option to synchronize users from your directory.
     - Click **Select Groups** to select a user group that you want to synchronize.

       A maximum of 500 users can be synchronized from one or multiple directory groups. If there are more than 500 users, Trend Micro Email Security sorts all users alphanumerically in ascending order and applies BEC policies only to the first 500 users.

Note

The Directory Synchronization Tool is required to synchronize user information from the directory server. For details about installing and updating the tool, see the Directory Synchronization Tool User's Guide. To download the tool and the guide, do the following:

a. Go to **Administration** > **Other Settings** > **Directory Management**.

b. On the **Directory Synchronize** tab, find the tool and guide under **Downloads**.

If you select **Microsoft AD Global Catalog** for synchronization in the Directory Synchronization Tool, make sure the `givenName`, `initials` and `sn` attributes have been replicated. By default, these attributes are not replicated to the global catalog server by Microsoft. If they are not replicated, use the Active Directory Schema snap-in in the Microsoft Management Console for replication.

- Click **Export** to export the directory user list to a CSV file.
- Click **Refresh** to refresh the current user list.

- **Custom**: select this option to create a customized list of high profile users.
  - Click **Add** to add a high profile user. Specify the first name, middle name (optional), last name and email addresses (optional) of the user.
  - Click **Delete** to delete a high profile user.
  - Click **Import** to import multiple users from a CSV file.

    The following import options are available:

    - **Merge**: append the users to the existing list.

- **Overwrite**: replace the existing list with the users in the file.

- Click **Export** to export the customized user list to a CSV file.

Configuring time-of-click protection settings

If you enable Time-of-Click Protection when creating a spam policy, Trend Micro Email Security rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click, and will block access to them or show a warning page (depending on your settings) if they are malicious.

You can choose to use the default blocking and warning pages or customize the blocking and warning pages according to your preference.

Procedure

1. Go to **Inbound Protection** > **Spam Filtering** > **Time-of-Click Protection**.
2. In the **Actions** section, do the following:
   - **Dangerous**: Select an action (**Allow**, **Warn** or **Block**) to take on dangerous URLs. The default value is **Block**.

     Dangerous URLs are verified to be fraudulent or known sources of threats.
   - **Highly Suspicious**: Select an action (**Allow**, **Warn** or **Block**) to take on highly suspicious URLs. The default value is **Block**.

     Highly suspicious URLs are suspected to be fraudulent or possible sources of threats.
   - **Suspicious**: Select an action (**Allow**, **Warn** or **Block**) to take on suspicious URLs. The default value is **Warn**.

     Suspicious URLs are associated with spam or possibly compromised.
   - **Untested**: Select an action (**Allow**, **Warn** or **Block**) to take on untested URLs. The default value is **Warn**.

While Trend Micro actively tests URLs for safety, users may encounter untested pages when visiting new or less popular websites. Blocking access to untested pages can improve safety but can also prevent access to safe pages.

3. In the **Blocking and Warning Pages** section, select whether to use the default blocking and warning pages or to customize your own ones.

   - **Use default redirect pages**: The default blocking page or warning page will appear when a malicious URL in the email message is clicked.
   - **Customize redirect pages**: Customize your own blocking page and warning page if you do not want to use the default ones.

     a. Type a title for **Browser Tab Title**.

     b. Next to **Content**, click the

     icon next to the strings on the **Dangerous** tab and customize the strings.

     Repeat the customization settings on the **Highly Suspicious**, **Suspicious**, and **Untested** tabs in sequence.

     Note

     When customizing the strings, you can use the following HTML tags for formatting: <b>, <br>, <i>, <p>, <li>, <ol>, <ul>, <blockquote>

     c. Type the click-through link text.

     The click-through link text you customize apply to the warning pages for malicious URLs at each of the preceding risk levels.

     Note

     The click-through link appears on the warning page only.

4. Click **Save**.

Data Loss Prevention

Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data, referred to as digital assets, against accidental disclosure and intentional theft. DLP allows you to:

- Identify the digital assets to protect
- Create policies that limit or prevent the transmission of digital assets through email
- Enforce compliance to established privacy standards

DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.

With DLP, Trend Micro Email Security allows you to manage your incoming email messages containing sensitive data and protects your organization against data loss by monitoring your outbound email messages.

Data identifier types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure.

  For details, see *Expressions on page 5-87*.

- **File attributes**: File properties such as file type and file size.

  For details, see *File Attributes on page 5-96*.

- **Keyword lists**: A list of special words or phrases.

  For details, see *Keywords on page 5-91*.

Note

Administrators cannot delete a data identifier that a DLP template is using. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

Administrators can use predefined and customized expressions.

For details, see *Predefined Expressions on page 5-87* and *Customized Expressions on page 5-87*.

Predefined Expressions

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted.

Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for custom expressions on page 5-88*.

Criteria for custom expressions

View the available options for creating custom expressions.

TABLE 5-5. Criteria options for customized expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau • Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number • Expression: [^\d]([0123678]\d{8})[^\d] • Characters: 0123456789 • Minimum characters: 9 • Maximum characters: 9

Criteria	Rule	Example
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address • Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle|cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • Suffix characters: 0123456789- • Number of characters: 5 • Minimum characters in the expression: 25 • Maximum characters in the expression: 80
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address • Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimum characters to the left: 3 • Maximum characters to the left: 15 • Maximum characters to the right: 30

Creating a Customized Expression

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Add**.

   A new screen displays.

4. Type an expression name that does not exceed 256 characters in length.
5. Type a description that does not exceed 256 characters in length.
6. Type the displayed data.

   For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.
7. Choose one of the following criteria and configure additional settings for the chosen criteria (see *Criteria for custom expressions on page 5-88*):
   - None
   - Specific characters
   - Suffix
   - Single-character separator
8. Optional: Select a validator for the expression.

Note

Data units follow semantic rules. Not every 9-digit number is a valid social security number and not every 15- or 16-digit number is a valid credit card number. To reduce false positives, expression validators check if the extracted data units follow these rules.

9. Test the expression against an actual data.

   For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.
10. Click **Save** if you are satisfied with the result.

Note

Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

Importing Customized Expressions

Use this option if you have a properly-formatted `.xml` file containing the expressions. You can generate the file by exporting the expressions from the Trend Micro Email Security administrator console.

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Import** and then locate the `.xml` file containing the expressions.
4. Click **Open**.

   A message appears, informing you if the import was successful.

Note

Every customized expression is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the administrator console.

If the file contains a customized expression that already exists, the existing expression is overwritten. If the file contains any predefined expression, the predefined expression is skipped during the import of the remaining customized expressions.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis",

"blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure Data Loss Prevention to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 5-92* and *Custom keyword lists on page 5-92*.

Predefined Keyword Lists

Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Custom keyword lists

Create custom keyword lists if none of the predefined keyword lists meets your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before data loss prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see *Custom keyword list criteria on page 5-93*.

Custom keyword list criteria

View criteria used to create custom keyword lists for use in data loss prevention templates.

TABLE 5-6. Criteria for a keyword list

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.
All keywords	A file must contain all the keywords in the keyword list.
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If Data Loss Prevention detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK**********WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, usually results in a faster scanning time but only covers a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.

Criteria	Rule
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Creating a Keyword List

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Add**.

   A new screen displays.
4. Type a keyword list name that does not exceed 256 characters in length.
5. Type a description that does not exceed 256 characters in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:
   - **Any keyword**
   - **All keywords**
   - **All keywords within <x> characters**
   - **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:
   a. Type a keyword that is 3 to 40 characters in length and specify whether it is case-sensitive.
   b. Click **Add**.
8. To edit a keyword, click a keyword in the list, edit it in the **Keyword** text box, and then click **Update**.
9. To delete keywords, select the keywords and click **Delete**.
10. Click **Save**.

Importing a Keyword List

Use this option if you have a properly-formatted `.xml` file containing the keyword lists. You can generate the file by exporting the keyword lists from the Trend Micro Email Security administrator console.

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Import** and then locate the `.xml` file containing the keyword lists.
4. Click **Open**.

   A message appears, informing you if the import was successful.

Note

Every customized keyword list is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the administrator console.

If the file contains a customized keyword list that already exists, the existing keyword list is overwritten. If the file contains any predefined keyword list, the predefined keyword list is skipped during the import of the remaining customized keyword lists.

File Attributes

File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For example, a software development company may want to limit the sharing of the company's software installer to the R&D department, whose members are responsible for the development and testing of the software. In this case, the Trend Micro Email Security administrator can create a policy that blocks the transmission of executable files that are 10 to 40 MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Predefined file attributes list

Data Loss Prevention comes with a predefined file attributes list. This list cannot be modified or deleted. The list has its own built-in conditions that determine if the template should trigger a policy violation.

Creating a file attribute list

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Add**.

   A new screen displays.
4. Type a file attribute list name that does not exceed 256 characters in length.
5. Type a description that does not exceed 256 characters in length.
6. Select either of the following:
   - **Not selected**: The selected file types will be excluded.
   - **Selected**: The selected file types will be included.
7. Select your preferred true file types.
8. If a file type you want to include is not listed, select **File extensions** and then type the file type's extension. Data Loss Prevention checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:
   - Each extension must start with an asterisk (*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, `*.pol` matches `12345.pol` and `test.pol`.
   - You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (*) to represent two or more characters. See the following examples:

     - `*.*m` matches the following files: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` matches the following files: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

- `*.fm?` matches the following files: `ABC.fme`, `ABC.fml`, `ABC.fmp`

- Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: `*.do*` matches `abc.doctor_john.jpg` and `abc.donor12.pdf`.

- Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.

9. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.

10. Click **Save**.

Importing a file attribute list

Use this option if you have a properly-formatted `.xml` file containing the file attribute lists. You can generate the file by exporting the file attribute lists from the Trend Micro Email Security administrator console.

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Data Identifiers**.

2. Click the **File Attribute** tab.

3. Click **Import** and then locate the `.xml` file containing the file attribute lists.

4. Click **Open**.

   A message appears, informing you if the import was successful.

Note

Every file attribute list is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the administrator console.

If the file contains a customized file attribute list that already exists, Trend Micro Email Security overwrites the existing file attribute list. If the file contains any predefined file attribute list, Trend Micro Email Security skips the predefined file attribute list while importing the remaining customized file attribute lists.

DLP Compliance Templates

A DLP compliance template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

You can create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see *Custom DLP templates on page 5-100* and *Predefined DLP Templates on page 5-99*.

Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

Trend Micro comes with a set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Custom DLP templates

Create your own DLP templates if you have configured data identifiers.

A DLP template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see *Condition statements and logical pperators on page 5-100*.

Condition statements and logical pperators

Apply conditions and operators to custom DLP templates.

Data loss prevention evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

TABLE 5-7. Sample condition statements

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier1] **And** [Data Identifier 2] **Except** [Data Identifier 3]	A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].
[Data Identifier 1] **Or** [Data Identifier 2]	A file must satisfy [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
Except [Data Identifier 1]	A file must not satisfy [Data Identifier 1]. For example: A file must not be [a multimedia file].

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

Creating a Template

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Compliance Templates**.
2. Click **Add**.

   A new screen displays.
3. Type a template name that does not exceed 256 characters in length.
4. Type a description that does not exceed 256 characters in length.
5. Select data identifiers and then click the "add" icon.
6. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before Data Loss Prevention subjects it to a policy.
7. Choose a logical operator for each definition.

Note

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see *Condition statements and logical pperators on page 5-100*.

8. To remove a data identifier from the list of selected identifiers, click the trash bin icon.
9. Click **Save**.

Importing Templates

Use this option if you have a properly-formatted `.xml` file containing the templates. You can generate the file by exporting the templates from the Trend Micro Email Security administrator console.

Procedure

1. Go to **Administration** > **Policy Objects** > **DLP Compliance Templates**.
2. Click **Import** and then locate the `.xml` file containing the templates.
3. Click **Open**.

   A message appears, informing you if the import was successful.

   Note

   Every customized template is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the management console.

   If the file contains a customized template that already exists, the existing template is overwritten. If the file contains any predefined template, the predefined template is skipped during the import of the remaining customized templates.

Chapter 6

Configuring policies

The virus policy, spam policy, Correlated Intelligence policy, content filtering policy and Data Loss Prevention (DLP) policy screens all show a list of the currently defined policy rules and their status. From each screen, you can add a new policy rule and query, reorder, edit, copy, or delete existing policy rules.

Note

If a policy rule applies to multiple domains and your account only has permission to manage a part of these domains, the policy rule is only visible. You cannot reorder, edit, copy, or delete the policy rule.

The policy screens under **Inbound Protection** and **Outbound Protection** are technically separate and can be managed independently.

The policy rules are displayed in a table, sorted by the order in which the policy rules were created by default.

TABLE 6-1. Policy Terminology

COLUMN	DESCRIPTION
Order	Order in which the policy rules are executed.

Column	Description
Status	: A policy rule is enabled. : A policy rule is disabled. : A policy rule is locked.
Rules	Name of the policy rule.
Migration Status	Status of the policy rule migrated from external systems.
Action	Action taken if the policy rule's criteria are met.
Organization Level	Whether the policy rule applies to all email messages sent to or from your organization. • **Yes**: The policy rule applies to all email messages sent to or from your organization. • **No**: The policy rule applies to email messages sent to or from specific users or groups in your organization. For details about the policy rule levels, see *Policy rule overview on page 6-3*.
Modified	Timestamp when the policy rule was last modified.
Last Used	Timestamp of when the policy rule was last used. If the policy rule has not yet been triggered, the value in this column will be “Never”.

Each column's heading can be clicked to sort the list. For example, to re-sort the list alphabetically by **Action**, click the **Action** column heading.

Policy rule overview

Trend Micro Email Security supports policy rules at the following levels in your organization: organization, group, and user.

- An organization-level policy rule applies to all of your organization's domains added to Trend Micro Email Security.

  Organization-level policy rules ease your policy management by automatically applying to all of your organization's domains including the new ones added in the future. With organization-level policy rules, you do not need to manually create new policy rules in case that a new domain is added.

  Trend Micro recommends that you configure organization-level policy rules under **Inbound Protection** and **Outbound Protection** to provide organization-level protection.

- A group-level policy rule applies to one or more specific groups (including domains, LDAP groups and address groups) in your organization.

  Tip

  If an existing domain-level policy rule is applying to all or the great majority of your organization's domains, you are advised to convert it into an organization-level policy rule and configure the rest of the domains as an exception list of the policy rule. This will simplify your policy management.

- A user-level policy rule applies to discrete email addresses that are or may be used by single users in your organization.

A policy rule level is determined by the **Recipients** or **Senders** addresses (depending on the mail traffic direction) that the policy applies to. The following table describes how to configure **Recipients** or **Senders** addresses for the policy rules at different levels. For more information, see *Specifying recipients and senders on page 6-11*.

Policy Rule Level	Inbound Protection	Outbound Protection
Organization	Select **My organization** for **Recipients** addresses on the **Recipients and Senders** tab.	Select **My organization** for **Senders** addresses on the **Recipients and Senders** tab.
Group	Specify domains, LDAP groups or address groups, or type email addresses in the format *@example.com for **Recipients** addresses on the **Recipients and Senders** tab.	Specify domains, LDAP groups or address groups, or type email addresses in the format *@example.com for **Senders** addresses on the **Recipients and Senders** tab.
User	Type one or more discrete email addresses for **Recipients** addresses on the **Recipients and Senders** tab.	Type one or more discrete email addresses for **Senders** addresses on the **Recipients and Senders** tab.

Default policy rules

Trend Micro Email Security comes with a set of default policy rules at the organization level and domain level, as listed in the following tables.

Table 6-2. Default Organization-Level Policy Rules

Policy Type	Inbound Policy Rules	Outbound Policy Rules
Virus scan	Organization: Virus	• Organization: Global Outbound Policy (Virus) **Note** This policy rule is not editable. • Organization: Outbound - Virus

Policy Type	Inbound Policy Rules	Outbound Policy Rules
Spam filtering	• Organization: Spam or Phish • Organization: Newsletter or spam-like • Organization: Probable BEC threat • Organization: Writing style BEC threat **Note** This policy rule is only available in Trend Micro Email Security Advanced.	• Organization: Global Outbound Policy (Spam or Phish) **Note** This policy rule is not editable. • Organization: Outbound - Spam or Phish
Correlated Intelligence	• Organization: Correlated Intelligence Security Risks • Organization: Correlated Intelligence Anomalies	Not applicable
Content filtering	• Organization: High-risk attachment • Organization: Exceeding msg size or # of recipients • Organization: Password protected	• Organization: Outbound - High-risk attachment • Organization: Outbound - Exceeding msg size or # of recipients

Table 6-3. Default Domain-Level Policy Rules

Policy Type	Inbound Policy Rules	Outbound Policy Rules
Virus scan	{{Domain name}}: Virus	{{Domain name}}: Outbound - Virus

Policy Type	Inbound Policy Rules	Outbound Policy Rules
Spam filtering	• {{Domain name}}: Spam or Phish • {{Domain name}}: Newsletter or spam-like • {{Domain name}}: Probable BEC threat • {{Domain name}}: Writing style BEC threat **Note** This policy rule is only available in Trend Micro Email Security Advanced.	{{Domain name}}: Outbound - Spam or Phish
Correlated Intelligence	• {{Domain name}}: Correlated Intelligence Security Risks • {{Domain name}}: Correlated Intelligence Anomalies	Not applicable
Content filtering	• {{Domain name}}: High-risk attachment • {{Domain name}}: Exceeding msg size or # of recipients • {{Domain name}}: Password protected	• {{Domain name}}: Outbound - High-risk attachment • {{Domain name}}: Outbound - Exceeding msg size or # of recipients

Besides the preceding default policy rules, Trend Micro Email Security also presets a built-in policy rule "Global Anti-Virus Rule (Enforced on Unverified Domains)", which is forcibly applied to inbound messages sent to unverified domains.

Note

This policy rule does not appear on the policy screen, and is visible only in mail tracking logs, policy event logs, and quarantine query details.

Managing policy rules

Policy rules are the means by which messaging policies are applied to message traffic in Trend Micro Email Security. At any time, administrators can see the policy rules that apply to their organizations, and make changes to the policy rules that comprise their policy, rename the policy rules, query the policy rules, reorder the policy rules, and create new policy rules. Each policy rule can be disabled if desired without losing its definition, and re-enabled at a later time.

TABLE 6-4. Policy Rule Tasks

TASK	STEP
Adding Policy Rules **Tip** A new policy rule may be similar to the one you already have. In this case, it is easier to copy the policy rule and edit it rather than create a new policy rule from scratch.	Click **Add**. 1. Define the basic information about the policy rule (rule name, whether it is enabled or not, and notes about the rule). See *Naming and enabling a policy rule on page 6-10*. 2. Select the address(es), domains(s) or group(s) that the policy rule applies to. See *Specifying recipients and senders on page 6-11*. 3. Select and configure criteria. See *About policy rule scanning criteria on page 6-16*. 4. Select and configure actions. See *About policy rule actions on page 6-58*.
Copying Policy Rules	In the policy rule list, select the rule or rules to copy. Click **Copy**.

TASK	STEP
Editing Policy Rules	In the policy rule list, click the name of the rule you want to edit and follow the procedures in the “Adding Policy Rules” task.
Reordering Policy Rules	In the policy rule list, do either of the following to reorder policy rules: • Click the up or down arrow button to move policy rules up or down. • Double-click the order number of a policy rule in the **Order** column and specify a new order number for the policy rule. See *Reordering policy rules on page 6-9*.
Enabling or Disabling Policy Rules	In the policy rule list, click the icon to the left of the rule name to enable or disable the policy rule.
Deleting Policy Rules	In the policy rule list, select the rule or rules to delete. Click **Delete**.

Task	Step
Querying Policy Rules	Use the following criteria to perform a policy rule query: • **Sender**: Specify a sender address to search for policy rules that match this address. • **Recipient**: Specify a recipient address to search for policy rules that match this address. **Note** For **Sender** and **Recipient**, the supported formats are `name@info.example.com`, `*@example.com` and `*@info.example.com`. Wildcard domain is not supported in query. • **Rule**: Specify a policy rule name to search for policy rules that match this name. • **Status**: Select **Enabled** or **Disabled** to search for policy rules in the specific status. **Note** For content filtering policy rules, **Criteria type** is provided to narrow down the search results by certain types of criteria. • **Level**: Select **Organization** or **User/Group** to search for policy rules at the specific level. • **Migration status**: Select **Error**, **Warning**, or **Fixed/Confirmed/Successful** to search for policy rules in the specific status.

Reordering policy rules

For each type of policy, the policy rules for all domains in your organization are arranged and prioritized uniformly from the organization's perspective. Meanwhile, the order of policy rules for each domain is retained. For

example, for virus policy rules of a single domain, the original order will still be applied.

Policy rules can be reordered when they are sorted by **Order**. If they are sorted by another column heading, the reorder function is unavailable.

Procedure

1. Do either of the following to reorder policy rules:
   - Click the up or down arrow button to move policy rules up or down.
   - Double-click the order number of a policy rule in the **Order** column and specify a new order number for the rule.

   Policy rules will be reordered as you configured, and email messages will be scanned based on the new rule order.

Naming and enabling a policy rule

Name and enable the policy rule you have just created. You can also add notes about the policy rule.

Procedure

1. On the **Basic Information** tab on the left side:
   a. Select **Enable** to put the policy rule into effect, or clear this option to disable it.
   b. Name the policy rule.

Note

Trend Micro recommends using a descriptive name that will allow administrators to easily identify this policy rule from the rule list. For instance, if you are creating a spam policy rule that applies to the `one.example.com` domain, you might name it something like "One Example Spam Rule".

c. Type any note information for this policy rule.

2. Proceed to the next screen to specify recipients and senders.

Specifying recipients and senders

Configure senders, recipients, and exception lists with your organization or specific users and groups on the **Recipients and Senders** tab. This tab differs slightly depending on which direction the messages are routed and whether **Sender** or **Recipient** addresses are being selected.

Inbound policy rules

Procedure

1. In the **Recipients** section, choose either of the following ways to add recipient addresses from the drop-down list:
   - **My organization**: Select it to configure an organization-level policy.

     Note

     This option is available only if **My organization** was specified for your subaccount during subaccount creation. For details, see *Adding and configuring a subaccount on page 10-33*.

   - **Specify**:
     - **My domains**: Select domains from the available domains and click **Add**.
     - **My LDAP groups**: Select user groups from the available directory groups and click **Add**.
     - **My address groups**: Select address groups from the available address groups and click **Add**.
     - **Type address or domain**: Type a specific domain or wildcard address and click **Add**.

2. In the **Senders** section, choose one of the following ways to specify sender addresses:
   - **Anyone**: Select it to apply any sender addresses for the policy rule.
   - **My organization**: Select it to apply email addresses sent from your organization for the policy rule.
   - **Specify**:
     - **My domains**: Select domains from the available domains and click **Add**.
     - **My address groups**: Select address groups from the available address groups and click **Add**.
     - **Type address or domain**: Type a specific domain or wildcard address and click **Add**.
3. In the **Exceptions** section, specify one or multiple exceptions, each of which consists of a sender part and a recipient part.
   a. Next to **Sender**, choose one of the following ways to specify the sender part of an exception:
      - **Anyone**
      - **My organization**
      - **My domains**
      - **My address groups**
      - **Type address or domain**
   b. Next to **Recipient**, choose one of the following ways to specify the recipient part of an exception:
      - **Anyone**
      - **My organization**
      - **My domains**
      - **My LDAP groups**

- **My address groups**
- **Type address or domain**

c. Click **Add** to add an exception composed of both the sender and recipient parts.

The exception you added appears in the exception list.

For example, if you select **Anyone** for the sender part and specify a specific email address for the recipient part, Trend Micro Email Security considers email messages sent from any senders to this recipient safe and bypasses the policy rule on these messages.

d. Add more exceptions if necessary.

Note

The import and export functions are available for recipients, senders and exception lists. Click **Import** to import groups, addresses or domains from a local file. Click **Export** to export groups, addresses or domains as a local file for future use.

A maximum of 500 records can be imported, and there is no upper limit for export.

4. Proceed to the next screen to specify policy rule scanning criteria.

Outbound policy rules

Procedure

1. In the **Recipients** section, choose one of the following ways to specify recipient addresses:

- **Anyone**: Select it to apply any recipient addresses for a policy rule.
- **My organization**: Select it to apply email addresses sent to your organization for the policy rule.

- **Specify**: Choose any of the following ways to add selected addresses:
  - **My domains**: Select domains from the available domains and click **Add**.
  - **My address groups**: Select address groups from the available address groups and click **Add**.
  - **Type address or domain**: Type a specific domain or wildcard address and click **Add**.

2. In the **Senders** section, choose either of the following ways to add sender addresses from the drop-down list:
   - **My organization**: Select it to configure an organization-level policy.

     Note

     This option is available only if **My organization** was specified for your subaccount during subaccount creation. For details, see *Adding and configuring a subaccount on page 10-33*.

   - **Specify**:
     - **My domains**: Select domains from the available domains and click **Add**.
     - **My LDAP groups**: Select user groups from the available directory groups and click **Add**.
     - **My address groups**: Select address groups from the available address groups and click **Add**.
     - **Type address or domain**: Type a specific domain or wildcard address and click **Add**.
3. In the **Exceptions** section, specify one or multiple exceptions, each of which consists of a sender part and a recipient part.
   a. Next to **Sender**, choose one of the following ways to specify the sender part of an exception:

- **Anyone**
- **My organization**
- **My domains**
- **My LDAP groups**
- **My address groups**
- **Type address or domain**

b. Next to **Recipient**, choose one of the following ways to specify the recipient part of an exception:

- **Anyone**
- **My organization**
- **My domains**
- **My address groups**
- **Type address or domain**

c. Click **Add** to add an exception composed of both the sender and recipient parts.

The exception you added appears in the exception list.

For example, if you specify a specific email address for the sender part and select **Anyone** for the recipient part, Trend Micro Email Security considers email messages sent from this sender to any recipients safe and bypasses the policy rule on these messages.

d. Add more exceptions if necessary.

Note

The import and export functions are available for recipients, senders and exception lists. Click **Import** to import groups, addresses or domains from a local file. Click **Export** to export groups, addresses or domains as a local file for future use.

A maximum of 500 records can be imported, and there is no upper limit for export.

4. Proceed to the next screen to specify policy rule scanning criteria.

About policy rule scanning criteria

Policy rule scanning criteria allow you to specify the conditions that the policy rule applies to messages scanned by Trend Micro Email Security.

The available criteria are shown in a list in the center of the screen. Some of these criteria have links to screens where you specify the associated details.

TABLE 6-5. Basic Criteria

CRITERIA		FILTER BASED ON	AVAILABLE IN
Virus Scan > **Virus Policy**	"**Specify at least one detection type**"	Detected malware, worms, and other threats by pattern-based scanning.	Inbound and outbound protection
	"**Specify Predictive Machine Learning settings**"	Detected unknown threats by Predictive Machine Learning.	Inbound and outbound protection
	"**Specify advanced settings**"	Detected threats by the Advanced Threat Scan Engine.	Inbound protection
Spam Filtering > **Spam Policy**	" **Spam** "	Detected spam.	Inbound and outbound protection

Criteria		Filter Based On	Available In
	"**Business Email Compromise (BEC)**"	Detected BEC attacks.	Inbound protection
	" **Phishing and other suspicious content** "	Detected phishing and other suspicious content.	Inbound and outbound protection
	" **Graymail** "	Detected graymail messages.	Inbound protection
	"**Web reputation**"	Detected URLs on the web or embedded in email messages that pose security risks.	Inbound and outbound protection
	" **Social engineering attack** "	Detected social engineering attacks.	Inbound protection
Correlated Intelligence > **Correlated Intelligence Policy**	"**Security risks**" "**Anomalies**"	Correlation rules that consist of detection signals from various sources such as Virus Scan and Spam Filtering.	Inbound protection
Content Filtering > **Content Policy**	**No criteria**	All messages.	Inbound and outbound protection
	" **All Match** " " **Any Match** "	Specific attribute and content targets. See *Configuring Advanced Criteria on page 6-38*.	Inbound and outbound protection
Data Loss Prevention > **Data Loss Prevention (DLP) Policy**	" **Select fields to scan** " " **Selected Templates** "	Detected DLP incidents.	Inbound and outbound protection

Configuring virus scan criteria

The virus scan criteria allow you to create policy rules that take actions on messages that contain malware, worms, or other malicious code.

Procedure

1. Click **Scanning Criteria**.
2. Specify at least one of the following detection types under the **Specify at least one detection type** section.

Option	Description
Cleanable malware or malicious code	Apply the policy rule to messages or attachments that contain cleanable malware. Cleanable malware are those that can be safely removed from the contents of the infected file, resulting in an uninfected copy of the original message or attachment. **WARNING!** Selecting **Cleanable malware or malicious code** as a policy rule criterion, and then selecting a policy rule action other than Delete or Clean, can result in infected messages or attachments entering your messaging environment. By default, Trend Micro Email Security is configured with malware policy rules to appropriately handle threats when it is installed.
Uncleanables with mass-mailing behavior	Apply the policy rule to messages that contain uncleanable malware, worms, or other threats that cannot be removed from messages or attachments, and that propagate by mass-mailing copies of themselves.
Uncleanables without mass-mailing behavior	Apply the policy rule to messages that contain the following: • Spyware • Dialers • Hacking tools • Password cracking applications • Adware • Joke programs

Option	Description
	• Remote access tools • All others

3. Configure Predictive Machine Learning settings to leverage the Predictive Machine Learning engine to detect emerging unknown security risks.

   a. Select **Enable Predictive Machine Learning** under the **Specify Predictive Machine Learning settings** section.

      For details, see *About Predictive Machine Learning on page 6-22*.

   b. Optionally select the **Allow Trend Micro to collect suspicious files to improve its detection capabilities** check box.

      Note

      By default, this option is selected.

      If you enable this option, Trend Micro only checks potentially risky messages and encrypts all content before transferring any information.

4. Specify advanced settings.

   Note

   These settings are not included in the Trend Micro Email Security Standard license.

   For details about different license versions, see *Available license versions on page 1-26*.

   a. Select **Submit suspicious files to Virtual Analyzer** and select the security level from the drop-down list to perform further observation and analysis on the submitted files.

      Whether a file is suspicious is determined by the Advanced Threat Scan Engine based on the scan results.

Virtual Analyzer performs observation and analysis on samples in a closed environment. It takes 3 minutes on average to analyze and identify the risk of a file, and the time could be as long as 30 minutes for some files.

Note

- When an eligible file is contained in another file, such as included in an archive file or embedded in a file, Trend Micro Email Security extracts the file and submits it to Virtual Analyzer.
- There is a submission quota limiting the number of files that can be sent to Virtual Analyzer within 24 hours. The quota is calculated based on a 24-hour sliding window as follows:

  File submission quota = Seat count * 0.1

  For example, if you have 1,000 seats, a total of 100 files can be submitted to Virtual Analyzer for analysis within 24 hours. The default quota will be 5 if your seat count is less than 50. Note that the submission quota mentioned here is subject to change without notice.

  In addition, the following cases will not be taken into account for quota measurement:

  - Samples hit the local or cloud cache.
  - Samples are in unsupported file format.
  - Other unexpected scan exceptions.

  Once the quota is used up, no more files can be sent to Virtual Analyzer. Nevertheless, the quota will be restored as the 24-hour sliding window moves forward.

  You can configure scan exception actions for the file submissions over quota. For details, see *Configuring "scan exceptions" actions on page 5-77*.

b. Select **Submit suspicious JSE/VBE files, suspicious files with QR codes, and any files with macros** if you want to submit these files to Virtual Analyzer.

Submitting suspicious files with QR codes helps you detect quishing, which is a type of phishing that uses QR codes to deceive users into visiting malicious websites and revealing sensitive information.

Note

Currently, only suspicious PDF files with QR codes are submitted to Virtual Analyzer.

5. Click **Submit**.

About Advanced Threat Scan Engine

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks. By default, this engine is enabled for virus scanning policies.

Its major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities
- Enhanced parsers for handling file deformities

About Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

After detecting an unknown or low-prevalence file, Trend Micro Email Security scans the file using the Advanced Threat Scan Engine to extract file features and sends the report to the Predictive Machine Learning

engine. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains.

Configuring spam filtering criteria

The **Spam**, **Phishing**, **Graymail**, **Web Reputation**, **Social engineering attack**, or **Unusual signal** criteria allow you to create policy rules that take actions on these types of potentially unwanted messages.

Note

Trend Micro Email Security does not apply content-based heuristic spam, BEC, phishing, graymail, Web reputation, social engineering attack, or unusual signal rules to email messages received from email addresses and domains listed on the **Approved Senders** screen.

Configuring spam criteria

Procedure

1. Select "**Spam**".
2. Choose a baseline spam catch rate.
   - Lowest (most conservative)
   - Low
   - Moderately low (the default setting)
   - Moderately high
   - High
   - Highest (most aggressive)

Configuring Business Email Compromise criteria

The BEC criteria are configured to detect and take actions on BEC email messages.

Procedure

1. Select **Business Email Compromise (BEC)**.
2. Click **High Profile Users** to add high profile users for detection and classification.

   Note

   Add high profile users as the global BEC settings so that Trend Micro Email Security will check incoming email messages claimed to be sent from those users and apply fraud checking criteria to identify forged messages.

   For details about high profile users, see *Configuring high profile users on page 5-82*.

3. Choose the type of email messages to apply this policy rule to:

   - **Detected as BEC attacks by Antispam Engine**: apply this policy rule to email messages that are verified to be BEC attacks by the Antispam Engine.
   - **Detected as BEC attacks by writing style analysis**: apply this policy rule to email messages that are verified to be BEC attacks by writing style analysis.

     Trend Micro's Writing Style DNA technology scans email messages of a desired individual to learn the particular writing style and generate a writing style model. The writing style model is a set of properties or features explored with automated methods that uniquely identify the way an individual composes email messages. By leveraging the writing style model trained in Cloud App Security for high profile users, Trend Micro Email Security compares the incoming email messages claimed to be sent from the individual with the model to identify BEC attacks.

     To ensure that the writing style model of a high profile user is available for analysis, Trend Micro Email Security runs a scheduled task every five minutes to synchronize the status of writing style models trained in Cloud App Security.

Note

These settings are not included in the Trend Micro Email Security Standard license.

For details about different license versions, see *Available license versions on page 1-26*.

Note

In this release, writing style analysis applies to email messages written in English, Japanese, German, French, Spanish, Swedish, Danish, Norwegian, Finnish, and Brazilian Portuguese.

To enable writing style analysis, the license for Cloud App Security is required.

- **BEC attacks suspected by Antispam Engine**: apply this policy rule to email messages that are suspected to be BEC attacks by the Antispam Engine.

Configuring phishing criteria

Procedure

1. Select "**Phishing and other suspicious content**".

Note

Trend Micro Email Security leverages Trend Micro Antispam Engine to filter email messages for spam and phishing incidents. Email messages will be categorized as phishing threats if Trend Micro Antispam Engine detects phishing and other suspicious content in those messages.

Configuring graymail criteria

Graymail refers to solicited bulk email messages that do not fit the definition of spam email messages. Trend Micro Email Security detects marketing

messages and newsletters, social network notifications, forum notifications, and bulk email messages as graymail messages.

Procedure

1. Select "**Graymail**".
2. Click **Graymail**.

   The **Graymail Detection Setting** screen appears.
3. Select at least one graymail category from the following:
   - **Marketing message and newsletter**
   - **Social network notification**
   - **Forum notification**
   - **Bulk email message**
4. To omit the IP addresses of specific mail servers from this policy rule, select **Enable the graymail exception list** under **Graymail Exception List**.
5. Specify IP addresses that you want to bypass graymail scanning.

   Note

   The policy rule will not apply to graymail messages from IP addresses in this exception list. The list is specific just to the policy rule being edited.
6. Click **Save**.

Configuring Web Reputation criteria

Trend Micro web reputation technology helps break the infection chain by assigning websites a "reputation" based on an assessment of the trustworthiness of a URL, derived from an analysis of the domain. Web reputation protects against web-based threats including zero-day attacks, before they reach the network. Trend Micro web reputation technology

tracks the lifecycle of hundreds of millions of web domains, extending proven Trend Micro antispam protection to the Internet.

The **Web reputation** criteria are configured to prevent access to malicious URLs in email messages.

Note

Web reputation also scans the QR codes in the body of an email or in an attached image file in the format of JPG, PNG, GIF, or BMP.

Procedure

1. Click **Scanning Criteria**.
2. Select and click **Web reputation**.

   The **Web Reputation Settings** screen appears.
3. Complete web reputation security settings.
   a. Select a baseline web reputation catch rate from the **Security level** drop-down list:
      - Lowest (most conservative)
      - Low
      - Moderately low
      - Moderately high (the default setting)
      - High
      - Highest (most aggressive)
   b. Optionally select **Take action on messages containing URLs that have not been tested by Trend Micro** to block websites that might pose threats.

Note

Web pages change frequently, and it is difficult to find data or follow a link after the underlying page is modified. Such websites are usually used as vehicles for transporting malware and carrying out phishing attacks.

If you select this check box, Trend Micro Email Security will take actions on all email messages containing URLs that have not been tested by Trend Micro. These URLs might include some legitimate URLs.

4. Under **Virtual Analyzer**, do the following:

Note

These settings are not included in the Trend Micro Email Security Standard license.

For details about different license versions, see *Available license versions on page 1-26*.

a. Select **Submit URLs to Virtual Analyzer**.

b. Select a security level from the drop-down list to perform further observation and analysis on the submitted URLs.

Virtual Analyzer performs observation and analysis on samples in a closed environment. It takes 3 minutes on average to analyze and identify the risk of a URL, and the time could be as long as 30 minutes for some URLs.

Note

There is a submission quota limiting the number of URLs that can be sent to Virtual Analyzer within 24 hours. The quota is calculated based on a 24-hour sliding window as follows:

URL submission quota = Seat count * 8

For example, if you have 1,000 seats, a total of 8,000 URLs can be submitted to Virtual Analyzer for analysis within 24 hours. Note that the submission quota mentioned here is subject to change without notice.

In addition, the following cases will not be taken into account for quota measurement:

- Samples hit the local or cloud cache.
- Sample URLs are unreachable.
- Other unexpected scan exceptions.

Once the quota is used up, no more URLs can be sent to Virtual Analyzer. Nevertheless, the quota will be restored as the 24-hour sliding window moves forward.

You can configure scan exception actions for the URL submissions over quota. For details, see *Configuring "scan exceptions" actions on page 5-77*.

5. Under **Time-of-Click Protection**, do the following:

   a. Select **Enable Time-of-Click Protection** and click one of the following:

      - **Apply to URLs that have not been tested by Trend Micro**
      - **Apply to URLs marked by Web Reputation Services as possible security risks**
      - **Apply to all URLs**

Note

Time-of-Click Protection is available only in inbound protection.

Web Reputation Services mark URLs as possible security risks if the URLs host or redirect to malicious files. For example, untested websites, file sharing websites and shortened URLs are marked as possible security risks.

b. Optionally select **Apply to URLs in digitally signed messages** if necessary.

Note

Enabling Time-of-Click Protection for digitally signed messages is not recommended because digital signatures might be destroyed.

6. Select **Enable the Web Reputation Approved List** to exclude URLs matching the specified domains or IP addresses from Web Reputation, Time-of-Click Protection, and Virtual Analyzer scanning.

Note

To manage the Web Reputation Approved List, navigate to the following path:

Administration > **Policy Objects** > **Web Reputation Approved List**

For details, see *Managing the Web Reputation approved list on page 10-6*.

7. Optionally select **Enable the URL keyword exception list** to exclude URLs containing specified keywords from both Time-of-Click Protection and Virtual Analyzer scanning.

Note

To manage the URL keyword exception list, navigate to the following path:

Administration > **Policy Objects** > **URL Keyword Exception List**

The protocol and domain parts of an URL will not be used for keyword match.

For details, see *Managing the URL keyword exception list on page 10-5*.

8. Click **Save**.

Configuring social engineering attack criteria

Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages.

For more information about social engineering attack detections, see *Social engineering attack log details on page 8-9*.

Procedure

1. Select **Social engineering attack**.

Configuring unusual signal criteria

Unusual signals are the behavior or traits of an email that look suspicious to Trend Micro Email Security. A single unusual signal does not mean a definite threat but can indicate possible risks. When detecting one unusual signal in an email message, Trend Micro Email Security supports taking action on the message. For details about unusual signals, see *Unusual signals on page 6-32*.

Note

Trend Micro recommends that you use the "Do not intercept messages" and "Insert stamp in body" actions for unusual signal detection. A default stamp "Unusual signal detection" is available for use.

Procedure

1. Select **Unusual signal**.

Unusual signals

The following table lists the unusual signals that Trend Micro Email Security can detect.

Signal	Description
Account-Takeover	This sender account might be compromised.
Unusual-URL	The URLs in the email are similar to those found in other malicious emails.
Payment-PDF-Free-Email	This message originates from a free email service and discusses payment-related issues in a PDF attachment.
Payment-HTML-Free-Email	This message originates from a free email service and discusses payment-related issues in an HTML attachment.
Payment-HTML-NB-Account	This account has no prior contact history with you and discusses payment-related issues in an HTML attachment.
Forged-Brand	The sender claims to be a well-known brand. However, the behavior of the sender does not match the known behavior of the brand.
Suspicious-Notify	The attachment might contain links used for malicious activity.

Configuring Correlated Intelligence criteria

Detect security risks and identify anomalies by correlating signals across different sources.

Designed to empower you with enhanced detection capabilities against sophisticated attacks, Correlated Intelligence correlates suspicious signals from various sources to detect phishing security risks and anomalies.

Note

Correlated Intelligence is available for Inbound Protection only.

Correlated Intelligence collects signals from Virus Scan and Spam Filtering.

One key advantage of Correlated Intelligence is the capability to see and analyze signals from multiple sources to identify phishing security risks that may go unnoticed by a single security filter. This multi-source approach adds an extra layer of protection to detect potential threats.

Another highlight of Correlated Intelligence is its ability to alert you of anomalies, which shows one or multiple signals that deviate from normal behaviors. Anomalies may not necessarily indicate a security risk, but are unusual enough to warrant attention. With this feature, you can have a more comprehensive view of your security landscape.

Correlated Intelligence operates by first gathering detection signals from various security criteria and then matching the signals against the predefined correlation rules. The aim of this process is to identify any matches that could indicate a phishing security risk or anomaly, providing a more thorough and nuanced analysis of potential security threats.

Trend Micro Email Security comes with a set of predefined correlation rules and detection signals to detect Trend Micro specified security risks and anomalies. To view details about the predefined correlation rules, detection signals, and their targeted threat types of anomalies, go to the **Administration** > **Policy Objects** > **Correlation Rules and Detection Signals** screen. You can also define custom correlation rules and detection signals that are unique and critical to your environment, and then add them to Correlated Intelligence policy rules. This provides you with flexibility of configuring Correlated Intelligence policy that meet your actual needs.

Procedure

1. Click **Scanning Criteria**.
2. Specify security risk detection settings.
   a. Select the **Security risks** check box to enable phishing detection by Correlated Intelligence.

Security risks are high-confidence detections by Correlated Intelligence. These are usually sophisticated attacks that are difficult to detect with a single protection layer. Correlated Intelligence combines signals from various sources to identify advanced attacks designed to bypass traditional, layer-by-layer defenses.

b. Select the check box to submit suspicious files to Virtual Analyzer to perform further observation and analysis on these files, and select the security level from the drop-down list to take configured actions based on Virtual Analyzer's scan results.

Whether a file is suspicious is determined by Correlated Intelligence based on its scan results.

Virtual Analyzer performs observation and analysis on samples in a closed environment. It takes 3 minutes on average to analyze and identify the risk of a file, and the time could be as long as 30 minutes for some files.

Actions for **Virtual Analyzer scan exception** and **Virtual Analyzer submission quota exception** under **Virus Scan** apply to Correlated Intelligence policy when this check box is selected.

If file password analysis is enabled under **Virus Scan**, the analysis results will be used by Correlated Intelligence policy when this check box is selected. If file password analysis is not enabled, Trend Micro Email Security cracks passwords from email content (subject, body, and attachment names).

Note

- When an eligible file is contained in another file, such as included in an archive file or embedded in a file, Trend Micro Email Security extracts the file and submits it to Virtual Analyzer.
- There is a submission quota limiting the number of files that can be sent to Virtual Analyzer within 24 hours. The quota is calculated based on a 24-hour sliding window as follows:

  File submission quota = Seat count * 0.1

  For example, if you have 1,000 seats, a total of 100 files can be submitted to Virtual Analyzer for analysis within 24 hours. The default quota will be 5 if your seat count is less than 50. Note that the submission quota mentioned here is subject to change without notice.

  In addition, the following cases will not be taken into account for quota measurement:

  - Samples hit the local or cloud cache.
  - Samples are in unsupported file format.
  - Other unexpected scan exceptions.

  Once the quota is used up, no more files can be sent to Virtual Analyzer. Nevertheless, the quota will be restored as the 24-hour sliding window moves forward.

  You can configure scan exception actions for the file submissions over quota. For details, see *Configuring "scan exceptions" actions on page 5-77*.

3. Under the **Specify anomaly settings** area, select the **Pre-defined anomalies** check box to enable the detection of Trend Micro specified anomalies, such as Suspicious Email or Possibly Unwanted Email, by predefined correlation rules.

Important

Anomaly detection by Correlated Intelligence correlation rules may not always indicate malicious activity; they align with certain suspicious signals and can vary in effectiveness and expectation. We recommend initially setting actions to **Tag subject** or **Insert stamp in body** to monitor outcomes before applying stronger actions. You can also *create custom correlation rules on page 10-9* and add them in the **Custom Correlated Intelligence** section to better fit your environment.

4. Determine to enforce all or partial predefined correlation rules to detect Trend Micro specified anomalies of different threat types.

   - **All pre-defined rules**

     This option is automatically selected when you select **Pre-defined anomalies**.

     Trend Micro classifies its predefined correlation rules for anomaly detection into three aggressive levels: **Moderate**, **Aggressive**, and **Extra aggressive**. For details about these correlation rules and what scenarios that correlation rules of each aggressive level are suitable for, see *Managing correlation rules and detection signals on page 10-9*.

     a. Select the threat type of Trend Micro specified anomalies that you want to detect using each aggressive level of correlation rules.

     b. Click the digit next to each aggressive level to view the associated predefined correlation rules in the **Correlation Rules and Detection Signals** screen under **Administration**.

        You can also enable or disable the predefined correlation rules in the screen.

   - **Specified pre-defined rules**

     Select and add one or multiple predefined correlation rules.

Note

Disabled correlation rules can be selected but do not apply during scanning.

5. Select the **Custom Correlated Intelligence** check box to enable anomaly detection by *custom correlation rules that you have created on page 10-9* for your environment.

6. Select and add one or multiple custom correlation rules.

Note

Disabled correlation rules can be selected but do not apply during scanning.

Clicking the digit next to **Custom Correlated Intelligence** opens the **Correlation Rules and Detection Signals** screen under **Administration**, where you can view all the existing correlation rules and add new correlation rules.

Configuring Data Loss Prevention criteria

Trend Micro Email Security evaluates email messages, including their content and attachments, against a set of rules defined in Data Loss Prevention (DLP) policies. Policies determine files or data that requires protection from unauthorized transmission and the action that Trend Micro Email Security performs after detecting a transmission.

Create DLP policies after you have configured data identifiers and organized them in templates. For details about the data identifiers and templates, see *Data Loss Prevention on page 5-86*.

Procedure

1. Choose a correct path to create your DLP policy for the proper mail traffic direction:

- **Inbound Protection** > **Data Loss Prevention** > **Data Loss Prevention (DLP) Policy**
- **Outbound Protection** > **Data Loss Prevention** > **Data Loss Prevention (DLP) Policy**

2. Click **Add** to add a DLP policy.
3. Click the **Scanning Criteria** tab.
4. Select fields to scan, for example, **Subject** and **Body**. To add a customized message header field, select **Other** and specify the field in the text box.
5. Select at least one compliance templates from the **Available Templates** list and click the right arrow button.

Note

A maximum of 255 compliance templates can be selected for each DLP policy.

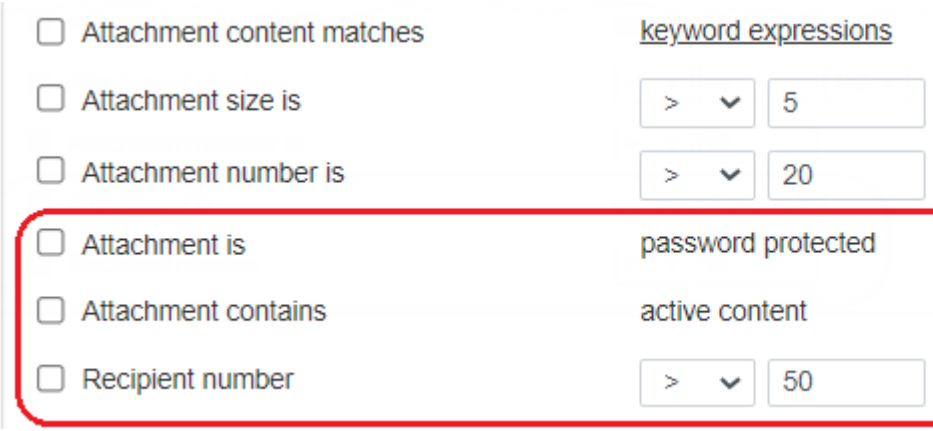
Configuring content filtering criteria

On the **Scanning Criteria** tab, select **Advanced** to display the advanced criteria.

From the drop-down list, do one of the following:

- Select **All Match** to trigger the policy rule only when all selected "Advanced" criteria are matched.
- Select **Any Match** to do the following:
  - Trigger the policy rule when any selected "Advanced" criteria are matched

- Display the **Attachment is** “**password protected**”, **Attachment contains** “**active content**”, and **Recipient number** criteria in the “Advanced” criteria list



The following tables all contain the same information sorted differently. Use the following sorted tables to find appropriate “Advanced” criteria to filter messages by your desired policy rule targets:

TABLE 6-6. Advanced Criteria Sorted by Display Order

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
Sorted by display order	**Envelope sender is**	"**blank**"	Envelope sender
	Message header sender differs from	"**envelope sender**"	Message header sender and envelope sender
	Message header sender differs from	"**header Reply-To**"	Message header sender and message header Reply-To
	Specified header matches	“ **keyword expressions** ”	Keywords in headers and content

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
	Message size is	**>, <=** <number> **KB**, **MB**	Size **Note** A maximum of 150 MB is allowed.
	Subject matches	" **keyword expressions** "	Keywords in headers and content
	Subject is	" **blank** "	
	Body matches	" **keyword expressions** "	
	Body is	"**blank**"	
	Attachment is	" **file name or extension** "	Attachment file name or extension
		" **MIME content type** "	Attachment MIME content type
		" **true file type** "	Attachment true file type **Note** For Microsoft Office files of version 2007 or later, Trend Micro Email Security supports attachment true file type detection only when the files are not encrypted.
	Attachment content matches	" **keyword expressions** "	Keywords in headers and content

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
	Attachment size is	**>, <=** <number> **B, KB, MB**	Attachment size  **Note** A maximum of 150 MB is allowed.
	Attachment number is	**>, <=** <number>	Number of attachments
	Attachment is	" **password protected** "	Zipped, signed, or password-protected attachment
	Attachment contains	" **active content** "	Active content in Microsoft Word, Excel and PowerPoint attachments
	Recipient number	**>, <=** <number>	Number of recipients

TABLE 6-7. Advanced Criteria Sorted by Attribute and Content Targets

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
Envelope sender and message header sender	**Envelope sender is**	"**blank**"	Envelope sender
	Message header sender differs from	"**envelope sender**"	Message header sender and envelope sender
	Message header sender differs from	"**header Reply-To**"	Message header sender and message header Reply-To
Name and type attributes	**Attachment is**	" **file name or extension** "	Attachment file name or extension

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
		“ **MIME content type** ”	Attachment MIME content type
		“ **true file type** ”	Attachment true file type **Note** For Microsoft Office files of version 2007 or later, Trend Micro Email Security supports attachment true file type detection only when the files are not encrypted.
Size attributes	**Message size is**	**>**, **<=** <number> **KB**, **MB**	Size
	Attachment size is	**>**, **<=** <number> **B**, **KB**, **MB**	Attachment size
Keyword content	**Subject matches**	“ **keyword expressions** ”	Keywords in headers and content
	Subject is	“ **blank** ”	
	Body matches	“ **keyword expressions** ”	
	Body is	"**blank**"	
	Specified header matches	“ **keyword expressions** ”	

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
	Attachment content matches	" **keyword expressions** "	
Active content	**Attachment contains**	" **active content** "	Active content in Microsoft Word, Excel and PowerPoint attachments
Quantity attributes	**Attachment number is**	**>**, **<=** <number>	Number of attachments
	Recipient number	**>**, **<=** <number>	Number of recipients
Compressed, signed, or encrypted attributes	**Attachment is**	" **password protected** "	Zipped, signed, or password-protected attachment

TABLE 6-8. Advanced Criteria Sorted by Message-Only or Attachment-Only Targets

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
Message-only	**Envelope sender is**	"**blank**"	Envelope sender
	Message header sender differs from	"**envelope sender**"	Message header sender and envelope sender
	Message header sender differs from	"**header Reply-To**"	Message header sender and message header Reply-To
	Message size is	**>**, **<=** <number> **KB**, **MB**	Size

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
	Subject matches	" **keyword expressions** "	Keywords in headers and content
	Subject is	" **blank** "	
	Body matches	" **keyword expressions** "	
	Body is	"**blank**"	
	Specified header matches	" **keyword expressions** "	
	Recipient number	**>, <=** <number>	Number of recipients
Attachment-only	**Attachment is**	" **file name or extension** "	Attachment file name or extension
		" **MIME content type** "	Attachment MIME content type
		" **true file type** "	Attachment true file type **Note** For Microsoft Office files of version 2007 or later, Trend Micro Email Security supports attachment true file type detection only when the files are not encrypted.
	Attachment content matches	" **keyword expressions** "	Keywords in headers and content

POLICY RULE TARGETS	CRITERIA		FILTER BASED ON
	Attachment size is	**>, <=** <number> **B, KB, MB**	Attachment size
	Attachment number is	**>, <=** <number>	Number of attachments
	Attachment is	" **password protected** "	Zipped, signed, or password-protected attachment
	Attachment contains	" **active content** "	Active content in Microsoft Word, Excel and PowerPoint attachments

Using envelope sender is blank criteria

Spoofing messages often have envelope senders (specified by the envelope field "MAIL FROM") set to blank to evade sender verification. Trend Micro Email Security allows you to scan messages for empty envelope senders to help you combat spoofing.

Note

- Some normal messages may also have empty envelope senders, such as bounce messages or notification messages. Selecting this criteria will affect these messages.
- This criteria is available for inbound protection only.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Envelope sender is blank**.

Using message header sender differs from envelope sender criteria

Spoofed messages often have mismatched message header senders (specified by the header "From") and envelope senders (specified by the envelope field "MAIL FROM"). Trend Micro Email Security provides an anti-spoofing check to detect messages with a message header sender different from the envelope sender.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Message header sender differs from envelope sender**.

Note

A message with a blank envelope sender does not match this criteria.

Using message header sender differs from header reply-to criteria

One common sign of spoofed messages is mismatched message header sender (specified by the header "From") and header Reply-To. Trend Micro Email Security can detect messages with the header sender different from header Reply-To to protect you against spoofing.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Message header sender differs from header Reply-To**.

Using attachment file name or extension criteria

The **Attachment is "file name or extension"** criteria allows you to create policy rules that take actions on messages based on the name or the extension of attachments a message contains. If a message contains a

compressed attachment, the criteria can further match the name or extension of the files included in the compressed attachment.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select the **Attachment is** "**file name or extension**" criteria.
3. Click the "**file name or extension**" link.

   The **Attachment File Name or Extension** screen appears.
4. From the drop-down list, select either **Selected file names or extensions** or **Not selected file names or extensions**.
5. If you want to block attachment names by file extension:
   a. Select **File extensions potentially dangerous** and/or **File extensions commonly exchanged at work**.

      Note

      The **File extensions potentially dangerous** category contains those whose file types commonly act as containers for malware and are not types that are normally exchanged via email in an organization. This list includes extensions such as COM, DLL, and EXE. The commonly exchanged category includes file types that are commonly sent between members of an organization.

      The **File extensions commonly exchanged at work** category includes the DOC extension used by Microsoft Word documents. These files are often used to propagate VB macro viruses, but they are also often commonly exchanged within organizations.

   b. Click the open arrow buttons to drop-down the lists of standard file extensions.
   c. Select the file extensions for Trend Micro Email Security to trigger on for this policy rule.

d. Click the close arrow button to collapse the list.

6. If you want to block attachments with your own specified names:

a. Select **File names**.

b. Type a file name to block.

Tip

Make sure the file name matches the full name of your target file, including the extension. For example, to match a file named "abc.doc", specify "abc.doc" or use an asterisk, such as "*.doc"; specifying only "abc" does not work.

You can use an asterisk (*) as a substitute for any part of a file name.

The following examples are valid file names:

- `*.docx`
- `*.doc*`
- `LOVE-LETTER*.vbs`
- `LOVE-LETTER-FOR-YOU.TXT.vbs`

c. Click **Add**.

The file name is added to the list just below.

Tip

If there are any names in the list that you want to delete, select them and click **Delete**.

Using attachment mime content type criteria

The **Attachment is "MIME content type"** criteria allows you to create policy rules that take actions on messages based on the MIME content-type of attachments a message contains.

Note

Where the **Attachment is "MIME content type"** criteria makes decisions based on the MIME content-type indicated, the **Attachment is "true file type"** criteria scans the headers of the actual attached files themselves for the identifying signatures.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select the **Attachment is "MIME content type"** criteria.
3. Click the "**MIME content type**" link.

   The **Attachment MIME Content Type** screen appears.
4. From the drop-down list, select **Selected MIME content types** or **Not selected MIME content types**.
5. Select the MIME content types for Trend Micro Email Security to match on.
6. If you want to block attachments by explicit MIME content types, type the names of the MIME content types to block, under the **Other MIME content types** text field.

Tip

The following examples are valid:

- `3dm` or `*.3dm`
- `3dmf` or `*.3dmf`

Using attachment true file type criteria

The **Attachment is "true file type"** criteria allows you to create policy rules that take actions on messages based on the true file type of attachments a message contains.

Note

Where the **Attachment is "file name or extension"** criteria makes decisions based on just file names and/or extensions, the **Attachment is "true file type"** criteria scans the headers of the files themselves for the identifying signatures.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select the **Attachment is "true file type"** criteria.
3. Click the "**true file type**" link.

   The **Attachment True File Type** screen appears.
4. From the drop-down list, select **Selected true file types** or **Not selected true file types**.
5. Select the true file types for Trend Micro Email Security to match on.

Note

- For Microsoft Office files of version 2007 or later, Trend Micro Email Security supports attachment true file type detection only when the files are not encrypted.
- The **Compressed file** type of **other** includes only the following file types: `ar`, `arc`, `amg`, `lzw`, `cab`, `lha`, `pklite`, `diet`, `lzh`, and `lz`.

Using message size criteria

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Message size is** in the criteria list.

3. Select **>** or **<=** from the comparison drop-down list.
   - Select **>** to apply the policy rule to messages that are larger than the specified size.
   - Select **<=** to apply the policy rule to messages that are smaller than or equal to the specified size.

   For example, **<= 10 MB** applies the policy rule to all messages that are smaller than or equal to 10 megabytes.
4. Type a number for the size.
5. Select a unit of measurement from the following choices:
   - **KB**: Kilobytes
   - **MB**: Megabytes

   Note

   The **Message size is** criteria is applied to the total size of a message, including any attachments it might contain.

   For example, if a message contained two attachments, one a 3 MB attachment and the other a 1 MB attachment, a policy rule that deletes messages over 2 MB would delete the entire message, including both attachments.

Using subject matches criteria

Trend Micro Email Security can scan the message subject for keyword expressions.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Subject matches** "**keyword expressions**".
3. Click the "**keyword expressions**" link.

4. Configure keywords.

Using subject is blank criteria

Trend Micro Email Security can scan the message for a blank subject line.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Subject is** "**blank**".

Using body matches criteria

Trend Micro Email Security can scan the message body for keyword expressions.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Body matches**.
3. Click the "**keyword expressions**" link.
4. Configure keywords.

Using body is blank criteria

Trend Micro Email Security can scan messages for blank bodies.

Note

Trend Micro Email Security detects any of the following cases as blank bodies:

- Bodies with no text nor HTML tags
- Bodies with only white space characters
- No body entity

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Body is "blank"**.

Using specified header matches criteria

Trend Micro Email Security can scan the message headers for keyword expressions.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select **Specified header matches**.
3. Click the "**keyword expressions**" link.
4. Configure keywords.

Using attachment content matches keyword criteria

The **Attachment content matches** "**keyword expressions**" criteria allows you to create policy rules that take actions on messages based on keyword expressions contained in a message.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.

2. Select the **Attachment content matches** "**keyword expressions**" criteria.
3. Click the "**keyword expressions**" link.

   The **Attachment Content Keyword Expressions** screen appears.
4. Configure the keywords.

Using attachment size criteria

The **Attachment size is** criteria allows you to create policy rules that take actions on messages based on the size of any attachments to the message.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select the **Attachment size is** criteria.
3. Select **>** or **<=** from the comparison drop-down list.
   - Select **>** to apply the policy rule to attachments that are larger than the specified size.
   - Select **<=** to apply the policy rule to attachments that are smaller than or equal to the specified size.

   For example, **<= 10 MB** applies the policy rule to all messages that are equal to or smaller than 10 megabytes.
4. Type a value for the size.
5. Select a unit of measurement from the following choices:
   - **B**: Bytes
   - **KB**: Kilobytes
   - **MB**: Megabytes

Note

The **Attachment size is** criteria is applied to the total size of each attachment.

For example, if a message contained two attachments, one a 3 MB attachment and the other a 1 MB attachment, a policy rule that deletes attachments over 2 MB would delete only the 3 MB attachment. The other attachment would not be deleted.

Using attachment number criteria

The **Attachment number is** criteria allow you to create policy rules that take actions on messages based on the number of attachments the message contains.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select the **Attachment number is** criteria.
3. Select **>** or **<=** from the comparison drop-down list.
   - Select **>** to apply the policy rule to messages that are sent with more than the specified number of attachments.
   - Select **<=** to apply the policy rule to messages that have the same number or fewer than the specified number of attachments.

   For example:

   > 10 applies the policy rule to all messages that have more than 10 attachments.

   <= 10 applies the policy rule to all messages that have 10 or fewer attachments.
4. Type the number of attachments to evaluate.

Using attachment is password protected criteria

Trend Micro Email Security can scan messages for attachments of the following types:

- `.7z`

- .ace
- .arj
- .docx
- .pptx
- .rar
- .xlsx
- .zip
- .pdf

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select "**Any Match**".

   The **Attachment is** "**password protected**", **Attachment contains** "**active content**", and **Recipient number** criteria become available.
3. Select **Attachment is** "**password protected**".

Using attachment contains active content criteria

Trend Micro Email Security can scan messages for the following attachments that contain active content such as macros:

- Microsoft Word files
- Microsoft Excel files
- Microsoft PowerPoint files
- Compressed Microsoft Word, Excel, or PowerPoint files

Note

The Microsoft Office version must be Office 2007 (12.0) or later.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select "**Any Match**".

   The **Attachment is** "**password protected**", **Attachment contains** "**active content**", and **Recipient number** criteria become available.
3. Select **Attachment contains** "**active content**".

Using the number of recipients criteria

The **Recipient Number** criteria allows you to create policy rules that take actions on messages based on the number of recipients the message is addressed to.

Procedure

1. On the **Scanning Criteria** tab, click **Advanced**.
2. Select "**Any Match**".

   The **Attachment is** "**password protected**", **Attachment contains** "**active content**", and **Recipient number** criteria become available.
3. Select **Recipient number**.
4. Select **>** or **<=** from the comparison drop-down list.

   - Select **>** to apply the policy rule to messages that are sent to more than the specified number of recipients.
   - Select **<=** to apply the policy rule to messages that have the same number or fewer than the specified number of recipients.

   For example:

   > 10 applies the policy rule to all messages that have more than 10 recipients.

   <= 10 applies the policy rule to all messages that have 10 or fewer recipients.

5. Type a value for the number of recipients.

About policy rule actions

Policy rule actions allow you to specify what happens to messages that satisfy the conditions of the policy rule's criteria.

Actions fall into these classes:

- “Intercept” actions: Actions in this class intercept the message, preventing it from reaching the original recipient. Intercept actions include deleting the entire message and re-addressing the message.
- “Modify” actions: Actions in this class change the message or its attachments. Modify actions include cleaning cleanable viruses, deleting message attachments, inserting a stamp in the message body, or tagging the subject line.
- “Monitor” actions: Actions in this class allow administrators to monitor messaging. Monitor actions include sending a notification message to others or sending a BCC (blind carbon copy) of the message to others.
- “Encrypt Email Message” actions: Actions in this class encrypt the message and then queue it for delivery. This is a non-intercept action, but no other actions can be taken on the target message after this policy rule is triggered. This action has the lowest priority of all actions, but when triggered it is always the final policy rule run before the message is queued for delivery. If more than one policy rule in the policy rule set is triggered, the policy rule that uses the encrypt email action will always be triggered last.

Note

This action only applies to outbound policy rules.

Each policy rule can contain:

- One and only one intercept action, and
- Any combination of modify or monitor actions

Specifying policy rule actions

Procedure

- To add actions to a policy rule definition, select the desired action.
- To specify details of an action (where required), select the drop-down list, text field, or link that provides more detail for the policy rule.

  For example, if the quarantine action is desired, you need to select which quarantine to send messages to when they trigger this policy rule. You also might want to create a new quarantine based on an existing one. You can click **Edit** there to begin that process.

“intercept” actions

“Intercept” actions prevent a message from being delivered to the mailbox of the original recipient. Instead, the message is deleted, quarantined, or sent to a different recipient.

“Intercept” actions are "terminal" actions. Once a terminal action executes, processing of that policy rule stops and no further action takes place for that policy rule.

Terminal actions execute following a strict priority order:

1. Delete the entire message.
2. Deliver the message now.

WARNING!

The **Deliver now** action is not recommended for use as the only action. If you choose **Deliver now** as the only action for Spam mail, for example, all of that mail will simply be delivered to your recipients, as if there were no spam filter in place.

If you use **Deliver now** with a virus policy rule, ensure that you also have a **Delete** action for the virus policy rule. Only the **Delete** action takes higher priority than **Deliver now** and so would be processed before it (and then terminate the processing of that policy rule).

If you chose **Deliver now** as the only action for a virus policy rule, mail containing viruses would leak through unblocked.

3. Quarantine the message.
4. Change recipient.

Using the delete action

This action deletes the message and all attachments. The message is recorded as deleted in the Trend Micro Email Security logs, but once deleted, the message cannot be recovered. It is one of the “intercept” category of actions. To configure a policy rule action to delete a message:

Procedure

- Select the **Delete entire message** action from the “Intercept” section.

Using the deliver now action

Trend Micro Email Security provides two options for the **Deliver Now** action:

- Deliver the email message to the default mail server

  If you choose this option, Trend Micro Email Security delivers the email message to the default mail server without executing any more policy rules for the affected email message.

By default, all policy rules are automatically ordered for security and execution efficiency. Administrators are relieved of determining the order of policy rule execution. This option bypasses the automatic order of execution so that Trend Micro Email Security can deliver the email message immediately.

WARNING!

This option of **Deliver now** is not recommended for use as the only action. If you choose this option of **Deliver now** as the only action for spam, for example, all of that email message will simply be delivered to your recipients, as if there were no spam filter in place.

If you use this option of **Deliver now** with a malware policy rule, ensure that you also have a **Delete** action for the malware policy rule. Only the **Delete** action takes higher priority than this option and so would be processed before it (and then terminate the processing of that policy rule).

If you chose this option of **Deliver now** as the only action for a malware policy rule, email messages containing malware would leak through unblocked.

- Deliver the email message to a specific mail server

  If you choose this option, Trend Micro Email Security delivers the email message to the specific mail server that you have configured. This option is recommended if you have a secure messaging server on your network that can process or handle the message.

Note

Trend Micro Email Security can track an email message only before it is delivered. After the delivery, the message is no longer traceable as it is not under the control of Trend Micro Email Security.

Procedure

1. Select the **Deliver now** action from the **Intercept** section.
   - Click **To the default mail server**.
   - Click **To a specific mail server**. Specify the FQDN or IP address as well as the listening port number for a specific mail server.

     Click **Test** to check the connection between Trend Micro Email Security and the mail server you specified.

   Note

   The corresponding TLS peer settings will still apply to the communication between Trend Micro Email Security and the mail server you choose.

2. Click **Submit**.
3. Click **OK** on the **Deliver now** warning message that appears.

Using the quarantine action

Quarantined items are now stored in a directory structure created by Trend Micro Email Security. This structure allows for increased performance when the service is saving items into quarantines or when users view them through the End User Console. Quarantined messages are indexed in the Trend Micro Email Security database to provide you with queries and improved search tools.

Procedure

1. In the “Intercept” section of the **Action** tab, select the **Quarantine** action.

Using the change recipient action

The **Change recipient** action intercepts messages and sends them to a new recipient. This means that the original message recipient will not receive a

copy of the message. It is one of the “intercept” class of actions. You can only select a recipient address that is in your domain.

Note

The **Change recipient** action does not change the recipient address in the message header. The message will be routed to the new address and the original recipient will not receive the message. The new recipient, however, will see the original recipient's address in the message header. To have a copy of the message sent to a different address while allowing the original message to go to the original recipient, select the **BCC** action.

WARNING!

Redirected messages may contain viruses or malicious code. Trend Micro recommends against redirecting messages to external addresses unless you have configured an outbound virus policy.

Procedure

1. From the “Intercept” section of the **Action** page, select the **Change recipient** action.
2. Type the email address of the recipient in the field. If you have more than one email address, enter them in the field separated by commas or semicolons.

“modify” actions

“Modify” actions change the message or its attachments. The original sender will still receive the modified message, assuming that the message does not trigger other policy rules with “Intercept” actions.

Note

Note that the "Modify" actions may destroy the existing DKIM signatures in email messages. If this occurs, the messages cannot pass DKIM verification by the downstream mail server.

For more information about specific “Modify” actions, select from the following:

- **Clean cleanable Viruses, delete those that cannot be cleaned** Action

  See *Cleaning Cleanable Viruses on page 6-64*.

- **Delete matching attachments** Action

  See *Deleting matching attachments on page 6-65*.

- **Sanitize attachments** Action

  See *Sanitizing attachments on page 6-66*.

- **Insert X-Header** Action

  See *Inserting an X-Header on page 6-67*.

- **Insert stamp in body** Action

  See *Inserting a stamp on page 6-67*.

- **Tag subject** Action

  See *Tagging the Subject Line on page 6-70*.

Tip

Terminal “Modify” actions have higher execution priority over non-terminal actions. When a terminal “Modify” action is triggered, there is no need to perform any other actions. However, non-terminal actions can be combined, such as **Delete matching attachments** and **Insert stamp in body**.

Cleaning cleanable malware

This action will clean cleanable malware (or other configured threats) contained in message attachments. If the threat cannot be cleaned, the message attachment that contains it will be deleted. **Clean cleanable malware** is one of the “Modify” class of actions.

Important

The **Clean cleanable malware, delete those that cannot be cleaned** action is only available in policies with the target criteria of **Message contains** "**malware or malicious code**". If the **Clean cleanable malware, delete those that cannot be cleaned** action is used in the policy rule, and a message contains an uncleanable malware, the attachment will be deleted.

The **Delete matching attachments** and **Clean cleanable malware, delete those that cannot be cleaned** actions cannot be used in the same policy rule.

To configure a policy rule action to clean malware-infected attachments:

Procedure

- From the "Modify" section of the **Action** page, select the **Clean cleanable malware, delete those that cannot be cleaned** action.

Deleting matching attachments

This action deletes any attachments that match the policy rule criteria. It is one of the "Modify" category of actions.

Important

The **Delete matching attachments** and **Clean cleanable malware, delete those that cannot be cleaned** actions cannot be used in the same policy rule.

The **Delete matching attachments** action is invoked only when one or more of the following criteria trigger a policy rule:

- **Message contains " malware or malicious code "**
- **Attachment is " name or extension "**
- **Attachment is " MIME content-type "**
- **Attachment is " true file type "**

- **Attachment is " password protected "**
- **Attachment size is**
- **Attachment content matches " keyword expressions "**

For example, if a "Message size is" policy rule (by default, greater than 10 MB) is triggered with an action of **Delete matching attachments**, all attachments will be deleted.

To configure a policy rule action to delete attachments that match certain criteria:

Procedure

- Select **Delete matching attachments** from the "Modify" section.

Sanitizing attachments

This action removes active content from the Microsoft Word, Excel, and PowerPoint attachments that match the policy rule criteria. If the active content cannot be removed, you can configure whether to delete the attachment containing the active content. **Sanitize attachments** is one of the "Modify" category of actions.

Important

The **Sanitize attachments** action is only available in policies with the target criteria of **Attachment contains** "**active content**". If the **Sanitize attachments** action is used in the policy rule, and the email attachment contains active content, the active content will be removed.

To configure a policy rule action to remove active content from the attachments that match certain criteria:

Procedure

- Select **Sanitize attachments** from the “Modify” section, and optionally select **Delete attachment if unable to remove active content**.

Inserting an X-Header

The **Insert X-Header** action adds an X-Header to the message header before sending a message to the intended recipients. An X-Header consists of a name field and a body field, which can be customized according to your requirements.

Insert X-Header is one of the "Modify" class of actions.

Procedure

1. Select **Insert X-Header** from the **Modify** section.
2. Type the X-Header name and value.

Note

Do not use or start your X-Header name (case-insensitive) with the following since they are reserved for Trend Micro Email Security:

- X-TM
- X-MT

The reserved X-Headers might be adjusted dynamically if necessary.

Inserting a stamp

The **Insert stamp in body** action inserts some standard confidentiality statement or a similar block of text into the message body. The stamps are maintained as named objects in the database and are selected from a list. The stamp definitions contain the stamp name, stamp content, whether they are to be inserted at the beginning or the end of the message body, and whether or not to avoid stamping TNEF and digitally signed messages to prevent breakage.

Trend Micro Email Security recognizes messages signed using the S/MIME standard.

Procedure

1. Select **Insert stamp in body**.
2. Select from the drop-down list of available stamps.
3. To configure stamps in the list, click **Edit**.

   For more information on how to configure a stamp, see *Managing stamps on page 10-27*.

Configuring stamps

You can edit or add a new message stamp. Stamps are inserted into messages when they trigger the policy rule. Typically they contain some standard confidentiality statement or a similar block of text. Policy Rule Tokens/ Variables (for example, the name of an attached file) can also be included in the text.

To edit or add a new message stamp:

Procedure

1. On the **Actions** page, select **Insert stamp in body**.
2. Click **Edit**.

   The **Stamps** screen appears, showing a list of available stamps.
3. Click **Add** or select a stamp from the list and click **Edit**.

   The **Stamps** screen appears, showing details for the stamp.
4. Type a name in the **Name** field, or edit the exiting name if desired.
5. To exclude TNEF and digitally signed messages from stamping, select **Do not stamp message formats that might become corrupted or unreadable, such as digitally signed and Outlook TNEF**.

Note

Trend Micro Email Security recognizes messages signed using the S/MIME standard.

The Microsoft TNEF format is used when sending rich text email using the Outlook client. If Trend Micro Email Security tries to insert a stamp into a TNEF-formatted email, the message might become corrupted or unreadable. To prevent this, if your organization uses Outlook to send rich text formatted messages, Trend Micro Email Security enables you to exempt TNEF messages from those actions that might corrupt the message.

6. Select whether to insert the stamp at the beginning or the end of the message body.

7. Specify the stamp content and style as needed with the rich text editor.

   Trend Micro Email Security provides a predefined style for the stamp indicating **Information**, **Suspicious**, or **Dangerous** risk level. You can either select a risk level and modify the corresponding HTML stamp, or customize your own HTML stamp.

   As you specify the stamp text and style, Trend Micro Email Security offers a preview of the stamp and generates an automatic plain text version below the rich text editor in real time. The plain text version shows you how the stamp appears to end users who cannot see the HTML version.

   Trend Micro Email Security provides a predefined style for the stamp that indicates **Information**, **Suspicious**, or **Dangerous** risk level. You can either select a risk level and modify the corresponding HTML stamp, or customize your own HTML stamp.

Note

Optionally, include variables in your stamps by using the tokens listed in *Tokens on page 6-70*.

As you customize the HTML stamp, Trend Micro Email Security offers a preview of the stamp and automatically generates the corresponding plain text stamp below the rich text editor in real time.

When a message triggers the policy rule, the HTML stamp will be inserted into **HTML** content of the message, and the plain text stamp will be inserted into **Plain text** content of the message.

Tagging the subject line

The **Tag Subject** action inserts configurable text into the message subject line. It is one of the "Modify" class of actions.

Procedure

1. Select the **Tag Subject** action.
2. Type a tag in the **Tag** field.
3. Optionally select **Do not tag digitally signed messages**.

Note

Trend Micro Email Security recognizes messages signed using the S/MIME standard.

Tokens

Use the following tokens to include variables in notifications and stamps.

TABLE 6-9. Tokens

TOKEN	VARIABLE
%SENDER%	Message sender
%RCPTS%	Message recipients
%SUBJECT%	Message subject

TOKEN	VARIABLE
%DATE&TIME%	Date and time of incident
%HEADERS%	Message headers, including the original header and the headers added by Trend Micro Email Security This token is supported only in stamps and notification body.
%MAILID%	Mail ID
%RULENAME%	Name of the policy rule that contained the triggered filter
%RULETYPE%	Type of a policy rule: Content Filter, Message Size Filter, and others
%DETECTED%	Scan result for virus policy matching, or name of the triggered policy rule or filter for content policy matching
%FILENAME%	Names of files that were affected by the policy rule
%DEF_CHARSET%	Default character set of the notification message
%MSG_SIZE%	Total size of the message and all attachments
%ATTACH_SIZE%	Total size of the attachment(s) that triggered the policy rule
%ATTACH_COUNT%	Number of attachments that triggered the policy rule
%TACTION%	Terminal action taken by Trend Micro Email Security
%ACTION%	All other (non-terminal) actions taken by Trend Micro Email Security
%VIRUSNAME%	Name of any malware detected This token will be empty if the message did not trigger a malware action.
%VIRUSACTION%	Action taken on any malware detected in the message This token will be empty if the message did not trigger a malware action.
%HPU_CONFIRMED_URL%	Option selected by a high profile user to confirm that he or she is the real sender of an email message

Token	Variable
%HPU_DENIED_URL%	Option selected by a high profile user to deny that he or she is the real sender of an email message
%SPFRESULT%	SPF check result returned when SPF check is enabled
%UNUSUAL_SIGNAL_NAME%	Unusual behavior or trait in an email message
%CI_RULE_NAME%	Name of the Correlated Intelligence correlation rule that detected a security risk or anomaly
%CI_RULE_DESC%	Description of the Correlated Intelligence correlation rule that detected a security risk or anomaly

"monitor" actions

"Monitor" actions do not change the original message or its attachments. The original sender will still receive the message, assuming that the message does not trigger other policy rules with intercept actions.

There are two "Monitor" actions:

- **Send notification** action
- **BCC** action

You can combine the first action with any other kind of action. You can combine the BCC action with "modify" actions (and with the first "monitor" action). However, the BCC action cannot be combined with terminal "intercept" actions.

Tip

The notification email message sent to "monitor" actions can be customized using the variables shown in *Policy Rule Tokens/Variables on page 6-70*.

Using the bcc action

The **BCC** action sends a Bcc (blind carbon copy) to a recipient or recipients configured in the policy rule. It is one of the "monitor" class of actions.

You can only configure a notification to be sent to an address in your own domain.

Procedure

1. From the Monitor section of the Action page, select **BCC**.
2. Type the email address of the recipient in the field. If you have more than one email address, enter them in the field separated by commas or semicolons.

Encrypting outbound messages

The purpose of this policy rule action is to protect sensitive data in email messages sent by users in your organization.

Note

This action only applies to outbound policy rules.

For outbound messages with DKIM signing enabled, if you also apply this encryption action which causes mail body change, these messages may not pass downstream DKIM authentication.

Actions in this class encrypt the message and then queue it for delivery. This is a non-intercept action, but no other actions can be taken on the target message after this policy rule is triggered. This action has the lowest priority of all actions, but when triggered it is always the final policy rule run before the message is queued for delivery. If more than one policy rule in the policy rule set is triggered, the policy rule that uses the encrypt email action will always be triggered last.

In most cases, a policy rule to encrypt email messages will be based on one of the following:

- Specific senders or recipients of the message (for example, a policy rule that encrypts all email sent from Human Resources or the Legal department)

- Specific content in the message body
- Sensitive data contained in the message

Procedure

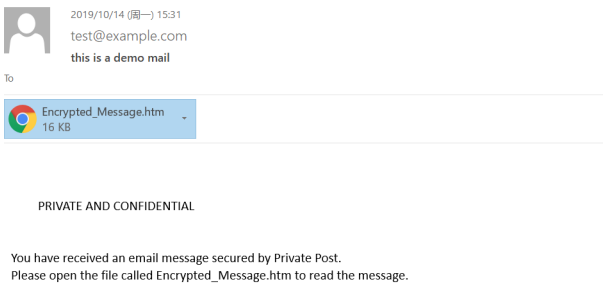
1. From the "Intercept" section of the **Action** page, select **Do not intercept messages**
2. From the "Modify" section of the page, select the **Encrypt email** action.

Reading an encrypted email message

When an "Encrypt Email Message" action is triggered, the recipient can decrypt the resulting encrypted message in the following way:

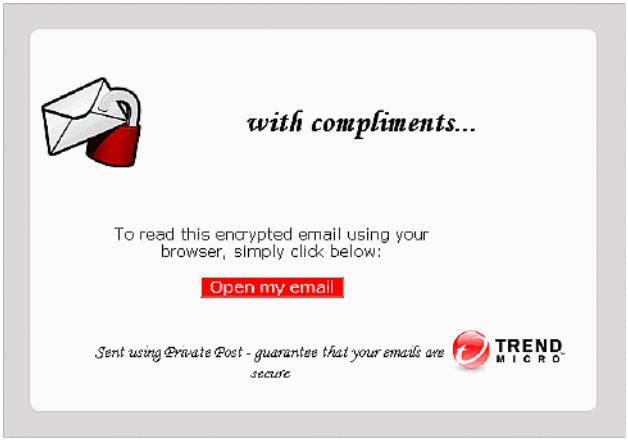
Use a web browser. Recipients of encrypted messages who are not using Email Encryption Client receive an email notification that provides a website link allowing the recipient to view the content of the message.

Below is a sample encrypted email notification message:



Procedure

1. Double-click the attached `Encrypted_Message.htm` file, which opens in your default web browser, as shown below.



2. Click **Open my email**, and if not yet registered, fill in the registration information on the subsequent pages. If you have already registered for this service, the encryption site displays your decrypted email at this point.

Note

The **Open my email** function may not work reliably with some web-based email systems. If the button does not work, the customer can save the attachment to a local computer and then open it again.

Recipients only need to register once. After registering with the Email Encryption service, the recipient will be able to view decrypted email in a browser window by clicking **Open my email**.

3. For enhanced security, match a CAPTCHA image, type and confirm a pass phrase, and select and answer three security questions. Upon successful registration, the email encryption site sends an activation message to the registered email account.

4. Upon receipt of the activation message, click **Please click here to validate your identity**. The Trend Micro email encryption site loads in your browser and displays your decrypted message, as shown below:

From: test@example.com
To:
CC:
Sent: Mon, 14 Oct 2019 07:30:51 +0000 (UTC)
Subject: this is a demo mail

This is a sample message to test encrypt function.

Thanks.

About the send notification action

Notifications are messages that are sent when the policy rule is triggered. They are one of the “Monitor” actions.

You can only send notification messages from addresses within your own domain.

Configuring send notification actions

Procedure

1. Select a message from the list of those available on the left side of the screen.
2. Click the right arrow button (**Add>**).

   The selected message appears in the **Selected** list on the right side.

Duplicating or copying send notification actions

Procedure

1. Select a message that you want to create a copy of from the list of those available on the left side of the screen.

2. Click **Copy**.

   The copy of the selected message appears in the **Available** list, with the prefix **Copy of** in its original name.

Removing notifications from policy rule actions

Procedure

1. Select the message you want to delete from the **Selected** list on the right side.
2. Click **Remove**.

Deleting notifications from lists of messages

To delete an existing notification message from the list of messages:

Procedure

1. Select the message you want to delete from the list of those available on the left side of the screen.
2. Click **Delete**.

Chapter 7

Understanding quarantine

Quarantined messages are blocked as detected spam or other inappropriate content before delivery to an email account. Messages held in quarantine can be reviewed and manually deleted or delivered.

WARNING!

Trend Micro Email Security automatically deletes messages from the quarantine after 30 days.

Do any of the following to manage quarantined messages on the administrator console:

- Use the **Query** screen to view a list of quarantined messages for your managed domains. You can review the messages, delete them, or release them for further scanning.

  Queries include data for up to seven continuous days in one calendar month. Use more than one query to search across calendar months.

- Use the **End User Quarantine Settings** screen to specify the type of sender addresses shown on the End User Console and in the quarantine digest notifications. On this screen, you can also configure settings for end users to view and take action on email messages quarantined for a specific reason.

- Use the **Digest Settings** screen to configure the policy rules and templates that Trend Micro Email Security applies to automatically send quarantine digest notifications. Intended digest recipients can either go to the End User Console or use inline actions in the digest notifications if available to manage quarantined messages.

Querying the quarantine

Use the **Query** screen to view a list of quarantined messages for your managed domains. You can review the messages, delete them, or release them for further scanning.

Procedure

1. In the **Period** field, specify the time range for your query.

   Note

   Queries include data for up to 30 continuous days in one calendar month. Use more than one query to search across calendar months.

2. In the **Direction** field, select a mail traffic direction.
3. Type your search criteria into one or more of the following fields:
   - **Recipient(s)**
   - **Sender(s)**
   - **Subject**

   You can specify up to 10 recipients or senders. Separate multiple recipients or senders by pressing the **ENTER** or **TAB** key, or using a semicolon (;).

   A recipient or sender can be a specific email address or all addresses from a specific domain.

   - Query a specific email address by typing that email address.
   - Query all addresses from a domain by using an asterisk (*) to the left of the at sign (@) in the email address. For example, `*@example.com` will search for all email addresses in the `example.com` domain.

   The following table displays format examples that are valid or not valid:

TABLE 7-1. Format Examples for Mail Tracking and Quarantine Query

VALID	NOT VALID
`name@info.example.com`	`name@*.example.com`
`*@example.com`	`*@*.com`
`*@server.example.com`	`*@*`
	`*@*.example.com`

4. In the **Visibility** field, specify whether to query quarantined messages that end users have access to.

   - **All**: Query all quarantined messages.
   - **Invisible to End Users**: Query the quarantined messages that end users do not have access to.
   - **Visible to End Users**: Query the quarantined messages that end users have access to.

   Quarantined incoming messages that end users have access to depend on your setting based on quarantine reasons on the **End User Quarantine Settings** screen. Quarantined outgoing messages are always invisible to end users.

5. In the **Reason** field, select one or multiple reasons why the message was quarantined.

   - **Sender IP Match**: The message failed Sender IP Match check.
   - **SPF**: The message failed SPF check.
   - **DKIM**: The message failed DKIM verification.
   - **Ransomware**: The message was identified as ransomware.
   - **Advanced Persistent Threat**: The message triggered the advanced threat policy.
     - **Analyzed Advanced Threats (Files)**: The message was identified as advanced file threats according to Virtual Analyzer and the policy configuration.

  - **Analyzed Advanced Threats (URLs)**: The message was identified as advanced URL threats according to Virtual Analyzer and the policy configuration.
  - **Probable Advanced Threats**: The message was treated as suspicious according to policy configuration or the message was not sent to Virtual Analyzer due to exceptions that occurred during analysis.

- **Malware**: The message triggered the malware criteria. The malware may be detected by Predictive Machine Learning or traditional pattern-based scanning.
- **Suspicious Objects**: The message contains suspicious files or suspicious URLs.
- **Scanning Exception**: The message triggered scan exceptions.
- **Spam**: The message was identified as spam.
- **BEC**: The message triggered the Business Email Compromise (BEC) criteria.
- **Phishing**: The message triggered the phishing criteria in Spam Filtering or the security risk criteria in Correlated Intelligence.
- **Graymail**: The message triggered the graymail criteria.
- **Web Reputation**: The message triggered the Web Reputation criteria.
- **Anomaly**: The message triggered the anomaly criteria in Correlated Intelligence.
- **Content Filtering - No Criteria**: The message triggered the **No Criteria** scanning criteria in the Content Filtering policy.
- **Content**: The message triggered the message content criteria. For example, a message's header, body or attachment matches the specified keywords or expressions.
- **Attachment**: The message triggered the message attachment criteria.

- **Data Loss Prevention**: The message triggered the Data Loss Prevention policy.

6. In the **Rule** field, specify the policy rule that was triggered by the quarantined message.

   The **Rule** field supports the following:

   - A maximum of 20 policy rules in use will be listed for you to choose when you click in this text box.
   - Select from the policy rules listed or type keywords for a fuzzy match.

7. In the **Message ID** field, specify the unique identifier of an email message.
8. Click **Search**.
9. Select one or multiple messages to manage.
10. Click one of the following buttons to manage the selected messages:

    - **Delete**: Cancel delivery and permanently delete the message
    - **Deliver**: Release from quarantine

Note

Released messages will no longer trigger the exact policy rule that caused the messages to be quarantined, but they will continue to be processed by Trend Micro Email Security. The following conditions apply to delivery:

- If a message triggers a content-based policy rule with an **Intercept** action of **Quarantine**, it will once again appear in the quarantined message list.
- If a message triggers a content-based policy rule with an **Intercept** action of **Delete entire message** or **Change recipient**, it will not arrive at its intended destination.

The content-based policy rule mentioned above refers to any policy rule that evaluates email messages based on message contents. Typical content-based policy rules include virus policies, spam policies, content filtering policies, and DLP policies.

11. Configure the password settings for downloading quarantined messages.

    a. Click **Set Download Password**.

    b. On the **Password Settings for Message Download** screen, select whether to use a random password or your own custom password for protecting the downloaded messages.

    If you use a custom password, specify a password consisting of 4 to 32 characters in the range "A-Z", "a-z", and "0-9".

    c. Select **Apply password settings to all admin accounts** if you want all administrators to use the same password settings for message download.

Note

This option is available only to the Business Account and superadmin accounts.

12. Optionally click on the **Date** value to view the **Quarantine Query Details** screen for a given message.

    a. Check the summary and detailed information about the message.

       In the **Message Details** area, view message body content in the HTML or plain text format.

       On the **HTML** tab, click **Show Source** or **Hide Source** to switch between viewing the source code and the rendered HTML of the body content. Click **Render Image** or **Hide Image** to display or hide the images within the body content.

       Note

       If the email header exceeds 20 KB, only the first 20 KB is displayed. For messages larger than 1 MB, the HTML content is not rendered. Instead, the message is displayed as truncated HTML source code on the **HTML** tab.

    b. Click **Delete**, **Deliver**, or **Download** to manage the message.

       When you click **Download**, choose whether to download the original email file or password-protected ZIP file to your local host.

       When you download the ZIP file, Trend Micro Email Security generates a password for decompressing the ZIP file. You can find the password on the **Quarantine Query Details** screen or at the end of the ZIP file name.

       Note

       The **Download** button is available only on the **Quarantine Query Details** screen.

Configuring end user quarantine settings

By default, both envelope addresses and message sender addresses are shown in the quarantine list on the End User Console and in the

quarantine digest notifications. Each envelope address is followed by the corresponding message header address in parentheses, in the format Envelope@example.com (Header@example.com).

For incoming email messages quarantined for a specific reason, you can choose to let end users view them and take action on the End User Console and in the quarantine digest notifications. Quarantined outgoing messages are always invisible to end users.

Procedure

1. In the **Sender Address Type** section, specify the type of sender addresses shown on the End User Console and in the quarantine digest notifications.

   - **Envelope addresses**
   - **Message header addresses**

   Note

   If **Message header addresses** is selected on this screen, Trend Micro recommends you also select it on the **Inbound Protection** > **Connection Filtering** > **Sender Filter** > **Sender Filter Settings** screen. Otherwise, the approved or blocked senders added by end users will not work as expected.

2. In the **Quarantined Message Permissions** section, specify the permissions that end users will have on the email messages quarantined for a specific reason.

   For more information about the quarantine reason, see *Querying the quarantine on page 7-3*.

   By default, the “View” and “Take Action” permissions are selected for **Spam** and **Graymail**.

   If you specify the “Take Action” permission for messages quarantined for a specific reason, the “View” permission will be automatically selected.

Note

The "Deliver", "Delete", and "Block Sender" actions are available for messages quarantined for all reasons listed. The "Approve Sender" action, however, is available only for messages quarantined for the reasons under the Spam Filtering category. For more information, see *Configuring approved and blocked sender lists on page 5-3*.

3. Click **Save**.

Quarantine digest settings

Note

Quarantine Digest is only available for **inbound** email messages that have been assigned “View” permissions on the **End User Quarantine Settings** screen.

A quarantine digest notification is an email message Trend Micro Email Security sends to inform end users of email messages that were temporarily quarantined. The digest notification lists up to 100 of each end user's quarantined messages.

You can customize digest rules and templates on the **Digest Settings** screen. A digest notification contains the following information:

- A link to access quarantined messages through the End User Console
- The number of new email messages that have been quarantined since the last notification was sent
- Digest of the new email messages that have been quarantined
  - Quarantined: The time an email message was quarantined
  - Sender: The sender address of the email message
  - Recipient: The recipient address of the email message

- Subject: The email subject
- Manage Messages: The links that users can click to apply actions to the quarantined message, including **Deliver**, **Deliver & Approve Sender**, **Block Sender**, **Approve Sender Domain**, **Block Sender Domain**, and **Preview**.

  When the **Preview** action is selected, Trend Micro Email Security includes a preview link for each quarantined email in a digest notification. This enables end users to view the summary and details of a quarantined email and take inline actions directly from the preview page. End users can switch between viewing the plain text, source code, and rendered HTML of the email body content by clicking the **Plain Text** tab or the **Show Source** or **Hide Source** buttons to on the **HTML** tab. Additionally, end users can click **Render Image** or **Hide Image** to display or hide the images within the body content.

  Different quarantined messages in a digest notification may have different inline actions. The inline actions available for each quarantined message are determined by the following settings:

  - Quarantined message permissions configured on the **Quarantine** > **End User Quarantine Settings** screen

    For more information, see *Configuring end user quarantine settings on page 7-8*.

  - Inline action settings configured in the digest notification template

    For more information, see *Adding or editing a digest template on page 7-14*.

  End users are required to confirm their operations on a dedicated page to prevent unexpected access during the digest notification transmission.

WARNING!

Inline action links display only when you enable **Inline actions** in the digest template.

Once inline actions are enabled, anyone receiving the digest notification can take the actions on quarantined messages. Therefore, administrators must warn digest recipients not to forward the digest notification.

If an end user account manages multiple accounts, Trend Micro Email Security sends digest notifications for the managed accounts as described in the following table.

Source of Managed Accounts	Condition	Digest Notification Recipients
Aliases synchronized from directories	End user has only one email address	Email address
	End user has email aliases but has not set the primary email alias	Each email alias
	End user has email aliases and has set the primary email alias	Primary email alias
Manually added accounts	End user has not set the primary account	Email address
	End user has set the primary account	Primary account

For details about the "Source of Managed Accounts", refer to *Configuring local account logon on page 10-64* for end user management.

Adding or editing a digest rule

You can customize digest rules for different recipients. If there are multiple digest rules, you can set or adjust the priority to apply each rule.

Procedure

1. Go to **Quarantine** > **Digest Settings**.
2. Click the **Digest Rules** tab.
3. Click **Add** or click the name of an existing digest rule.
4. In the **General Information** section, do the following:
   a. Click the **Status** toggle button to enable the current digest rule.
   b. Type the rule name and description.
5. In the **Recipients** section, select the recipients for digest notifications:
   - **All recipients**: This option only applies to the default digest rule. All users of your managed domains will receive digest notifications.
   - **Specified recipients**: This option enables you to choose users from both your LDAP groups and managed domains and add all of them as intended recipients.
6. In the **Schedule** section, select the frequency to send digest notifications:
   - **Daily**: Specify the exact time to send the digest notifications.

     Use the add + and the remove − buttons to manage additional entries.
   - **Weekly**: Specify the days of the week and time of the day to send the digest notifications.

   Note

   The time zone of the browser accessing Trend Micro Email Security is used.
7. In the **Template** section, select the digest template that you want to use for the current digest rule.
8. Click **Save**.

The newly added or edited digest rule displays on the **Digest Rules** screen. You can further change the rule status, set the rule priority, copy and delete the rule.

Note

If the recipient scope for different digest rules conflicts with each other, a red exclamation mark icon will be shown next to the recipients of each digest rule. Hover over the icon to view the current recipients, conflict rules and conflict recipients. Digest notifications are sent to the conflict recipients according to the rule with the higher priority. The smaller the priority number, the higher the priority.

The following table is an example for your reference.

Digest Rule	Priority	Recipients
Rule1	1	domain1.com
Rule2	2	domain2.com; usergroup1

If `Rule1` and `Rule2` are both enabled and `usergroup1` contains some recipients in `domain1.com`, this means the two rules have a recipient conflict. In this case, Trend Micro Email Security applies `Rule1` that has the higher priority to send digest notifications to the conflict recipients.

Adding or editing a digest template

You can create digest templates to define the format and content of notification email messages that end users receive.

Procedure

1. Go to **Quarantine** > **Digest Settings**.
2. Click the **Digest Templates** tab.

3. Click **Add** or click the name of an existing template.
4. In the **General Information** section, specify the template name and description.
5. In the **Digest Notification Template** section, configure the following:

Note

The digest notification template is available either in HTML or plain text versions. Each version of the template can incorporate tokens to customize output for digest recipients. You can right-click any of the following fields to display a list of available and selectable tokens for the field.

- **From**: Specify the email address that displays as the sender of the digest notification.

TABLE 7-2. From field digest tokens

TOKEN	CONTENT IN SENT DIGEST NOTIFICATIONS
%DIGEST_RCPT%	Digest recipient's email address appears in the **From** field of the received digest notification

- **Subject**: Specify the subject line for the digest notification.

TABLE 7-3. Subject field digest tokens

TOKEN	CONTENT IN SENT DIGEST NOTIFICATIONS
%DIGEST_RCPT%	Digest recipient's email address appears in the subject line
%DIGEST_DATE%	Digest date appears in the subject line

- **HTML**:
  - Specify if **Inline actions** should be **Enabled** or **Disabled** using the toggle button to the right of **Inline actions**.
  - Select the language you want to use for inline actions from the **Language** drop-down list.

- Customize the inline actions that digest recipients can take in the digest notifications.

  The following inline actions are available for your customization and the first three ones are selected by default:

  - **Deliver**
  - **Deliver & Approve Sender**
  - **Block Sender**
  - **Approve Sender Domain**
  - **Block Sender Domain**
  - **Preview**

- Specify the HTML content of the digest notification if the email client accepts HTML messages.

TABLE 7-4. HTML field digest tokens

TOKEN	CONTENT IN SENT DIGEST NOTIFICATIONS
%DIGEST_RCPT%	Digest recipient's email address appears in the HTML body
%DIGEST_DATE%	Digest date appears in the HTML body
%DIGEST_BODY_HTML%	Digest summary in HTML table format appears in the HTML body
%DIGEST_PAGE_COUNT%	Total number of quarantined messages listed in the digest summary (up to 100) appears in the HTML body
%DIGEST_TOTAL_COUNT%	Total number of new found messages in quarantine appears in the HTML body
%EUC_HOST_SERVER%	Web address of Trend Micro Email Security End User Console appears in the HTML body

- **Plain text**: Specify the plain text content of the digest notification if the email client only accepts plain text messages.

TABLE 7-5. Plain text field digest tokens

TOKEN	CONTENT IN SENT DIGEST NOTIFICATIONS
%DIGEST_RCPT%	Digest recipient's email address appears in the text body
%DIGEST_DATE%	Digest date appears in the text body
%DIGEST_BODY_TEXT%	Digest summary in plain text format appears in the text body
%DIGEST_PAGE_COUNT%	Total number of quarantined messages listed in the digest summary (up to 100) appears in the plain text body
%DIGEST_TOTAL_COUNT%	Total number of new found messages in quarantine appears in the plain text body
%EUC_HOST_SERVER%	Web address of Trend Micro Email Security End User Console appears in the plain text body

6. In the **Test Digest Mail** section, specify the intended digest recipient and click **Test** to test digest notification delivery.

   The digest recipient receives a notification message. The sender, subject and content of the notification and the available inline actions match the configured settings.

7. Click **Save**.

   The newly added or edited template displays on the **Digest Templates** screen. You can further copy and delete the template if necessary.

Chapter 8

Logs in Trend Micro Email Security

Understanding mail tracking

This screen is designed for you to track email messages that passed through Trend Micro Email Security, including blocked or delivered messages. Trend Micro Email Security maintains up to 90 days of mail tracking logs. The sliding window for mail tracking log search is 60 continuous days that may cross calendar months.

Note

The sliding window for mail tracking log search is 30 days in the Trend Micro Email Security Standard license.

For details about different license versions, see *Available license versions on page 1-26*.

The **Mail Tracking** screen provides the following search criteria:

- **Period**: The time range for your query.
  - **Last 1 hour**
  - **Last 24 hours**
  - **Last 7 days**
  - **Last 14 days**
  - **Last 30 days**
  - **Custom range**
- **Direction**: The direction of messages.
  - **Incoming**
  - **Outgoing**
- **Recipient**: The envelope recipient address. Specify up to 10 email addresses.
- **Sender**: The envelope sender address. Specify up to 10 email addresses.

- **Email Header (To)**: The recipient address in the message header. Specify up to 10 email addresses.
- **Email Header (From)**: The sender address in the message header. Specify up to 10 email addresses.

Note

Pay attention to the following when setting the preceding four address fields:

- Specify an exact email address or use wildcards (*) to substitute any characters in a search. In the general format of an email address (local-part@domain), be aware that:
  - The local part must be a wildcard (*) or a character string that does not start with *, for example, *@example.com or test*@example.com.
  - The domain must be a wildcard (*) or a character string that does not end with *, for example, example@* or example@*.test.com.
  - If this field is left blank, *@* is used by default.
- Use wildcards (*) strategically to expand or narrow your search results. For example, put a wildcard (*) in the domain part to search by a particular user account on all domains or in the local part to match all accounts on a particular domain.

- **Type**: The type of email traffic that you want to query.
  - **Accepted traffic**: The messages that were allowed in by Trend Micro Email Security for further processing.

    If you select **Accepted traffic** as your search condition, a summary of email message traffic accepted by Trend Micro Email Security is displayed. For a message that has multiple recipients, the result will be organized as one recipient per entry.

- **Blocked traffic**: The attempts to send messages that were stopped by connection-based filtering at the MTA connection level or by Trend Micro Email Security incoming security filtering.

  If you select **Blocked traffic** as your search condition, you can further select a block reason. See *Blocked message details on page 3-16* for details about the block reasons. A summary of email message traffic blocked by Trend Micro Email Security is displayed.

  Note

  Content-based filtering is not included in this category.

- **Action**: The last action taken on the message.
  - **All**: All the actions will be matched for your search.
  - **Bounced**: Trend Micro Email Security bounced the message back to the sender because the message was rejected by the downstream MTA.
  - **Temporary delivery error**: Trend Micro Email Security attempted to deliver the message to the downstream MTA but failed due to unexpected errors. This is a transient state of the message, and a message should not remain in this state for an extended period of time.
  - **Deleted**: Trend Micro Email Security deleted the entire email message according to the matched policy.
  - **Delivered**: Trend Micro Email Security delivered the message to the downstream MTA.
  - **Expired**: Trend Micro Email Security bounced the message back to the sender because the message had not been delivered successfully for a long time.
  - **Quarantined**: Trend Micro Email Security held the message in quarantine awaiting actions because the message triggered a certain policy rule. Quarantined messages can be reviewed and manually deleted or delivered.

- **Redirected**: Trend Micro Email Security redirected the message to a different recipient according to the matched policy.
- **Submitted to sandbox**: Trend Micro Email Security submitted the message to Virtual Analyzer for further analysis. This is a transient state of the message, and the state will change once the Virtual Analyzer analysis result is returned or Virtual Analyzer scan exception is triggered.
- **Password analyzing**: Trend Micro Email Security submitted the message to Password Analyzer for password analysis. This is a transient state of the message, and the state will change once the Password Analyzer returns a result.

- **Subject**: The email message subject.

  The **Subject** field supports the following:

  - Fuzzy match

    Type one or multiple keywords for a fuzzy match. If you type more than one keyword, all keywords will be matched based on a logical AND, which means the matched subject must contain every keyword. Wildcards (*) will be automatically added before and after each keyword for a fuzzy match.

  - Exact keyword or phrase match

    Enclose a keyword or phrase in quotes for an exact match. Only records that contain the exact keyword or phrase will be matched.

  For example, there are three email subjects:

  - Subject1: Hello world
  - Subject2: Hello new world
  - Subject3: "Hello"

  If you type `Hello world` in the **Subject** field, this is a fuzzy match, and Subject1 and Subject2 will be matched. If you type `"Hello world"`, this is an exact match using quotes, and only Subject1 will be matched. If you want to search for Subject3, be aware that quotes are contained by the

subject itself. In this particular case, use backslashes (\) as the escape characters and type `\"Hello\"` for search.

- **Message ID**: The unique ID of an email message.
- **Sender IP**: The IP address of the host where the message was sent from.
- **Delivered To**: The IP address of the host where the message was delivered to.

Note

Type an IPv4 address or an IPv4 address prefix for the preceding two IP address fields.

- **Upstream TLS**: The version of the TLS protocol used by the upstream server to connect to Trend Micro Email Security.
  - **All**
  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**
  - **TLS 1.3**
  - **None**
- **Downstream TLS**: The version of the TLS protocol used by Trend Micro Email Security to connect to the downstream server.
  - **All**
  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**
  - **TLS 1.3**
  - **None**

- **Downstream DANE**: Whether DANE authentication is applied to TLS connections between Trend Micro Email Security and the downstream server.
  - **All**
  - **Yes**
  - **No**

Note

This field appears only when you set **Direction** to **Outgoing** and **Type** to **Accepted traffic**.

- **Timestamp**: The time a message was received.

  Choose the ascending or descending order of time to sort the search results.

- **Messages with attachments only**: Query only messages that contain attachments.

  When this option is selected, you can further specify the following criteria:

  - **Attachment SHA256 Hash**: The SHA256 hash value of a message attachment. Specify a SHA256 hash value consisting of 64 hexadecimal characters or leave it blank.
  - **Attachment Filename**: The filename of the attachment. You can use wildcards (*) to represent any characters in the filename.
  - **Attachment Status**: The status of the attachment after it was processed by Trend Micro Email Security.
    - **All**: The attachment was in any status. This is the default option.
    - **Deleted**: The attachment was deleted.
    - **Cleaned**: The attachment was cleaned for malware.

- **Bypassed**: The attachment was bypassed.
- **Sanitized**: The attachment was sanitized.

- **Attachment Password Analysis**: Whether the attachment was subjected to password analysis and decrypted successfully.
  - **Not analyzed**: The attachment was not subjected to password analysis because it was not password-protected, its file type was not supported, or File Password Analysis was not enabled.
  - **Analyzed**: The attachment was subjected to password analysis.
    - **Decrypted**: The attachment was decrypted.
    - **Not decrypted**: The attachment could not be decrypted.

- **Messages with end user feedback**: Query messages that were reported by end users as spam, phishing, or not a risk through the Email Reporting add-in.

  Note

  - This field appears only when you set **Direction** to **Incoming** and **Type** to **Accepted traffic**.
  - This feature is not available at the Japan site.

  When this option is selected, you can further specify **Reported Risk**, namely **All**, **Spam**, **Phishing**, or **Not a Risk**.

When you query mail tracking information, use the various criteria fields to restrict your searches. After a query is performed, Trend Micro Email Security provides a list of log records that satisfy the criteria. Select one or more records and click **Export Selected** to export them to a CSV file. Click **Export All** to export all the queried log records if needed. If the number of log records to export is large, the export task needs to take time to complete. Go to **Logs** > **Log Export Query** to check the export status. Note that you can export up to 50,000 log records at a time and the maximum number of times of exporting all the queried log records is 5 per day, which is calculated based on the time zone UTC+00:00.

The most efficient way to query mail tracking information is to provide both sender and recipient email addresses within a time range that you want to search. For an email message that has multiple recipients, the result will be organized as one recipient per entry.

If the message you are tracking cannot be located using this strategy, consider the following:

- Expand the result set by omitting the recipient.

  If the sender is actually blocked by connection-based filtering, the **Blocked traffic** results that do not match the intended recipient might indicate this. Provide only the sender and time range for a larger result set.

- Look for other intended recipients of the same message.
  If the sender IP address has a "bad" reputation, mail tracking information will only be kept for the first recipient in a list of recipients. Therefore, the remaining message recipient addresses will not be listed when querying this sender.

- Expand the result set by omitting the sender.

  If the sender IP address has a "bad" reputation, omit the sender and provide only the recipient. If only the recipient email address is provided, all the messages that pertain to the recipient will be listed.

Social engineering attack log details

Trend Micro Email Security provides detailed information for email messages detected as possible social engineering attacks. To view social engineering attack details, click the **Details** link beside **Social engineering attack** on the **Mail Tracking Details** screen.

The following table lists the possible reasons for social engineering attack detections.

TABLE 8-1. Possible reasons for social engineering attack detections

EMAIL CHARACTERISTICS	DESCRIPTION
Inconsistent sender host names	The Message-ID host name (<host_name>) does not match the From host name (<host_name>).
Broken mail routing path	Broken mail routing path from hop (<IP_address>) to hop (<IP_address>).
Mail routing path contains mail server with bad reputation	The mail routing path contains mail server with bad reputation (<IP_address>).
Significant time gap during email message transit	Significant time gap (<duration>) detected during email message transit between hops (<source> & <destination>) from time (<date_time>) to time (<date_time>).
Inconsistent recipient accounts	Envelope recipient (<email_address>) is inconsistent with header recipient (<email_address>).
Inconsistent sender ASNs or unexpected relay or forward	The sender host (<host_address>) belongs to an ASN (<ASN>) that does not match the ASN (<ASN>) of the sender account (<email_address>). This message may occur from an unexpected server-side relay or forward.
Email message travels across multiple time zones	The email message travels across time zones (<time_zone_list>).
Possible social engineering attack characterized by suspicious charsets in email entities	Suspicious charsets (<character_set_list>) are identified in a single email message, implying the email message originated from a foreign region. This behavior is an indicator of a social engineering attack.
Violation of time headers	Multiple time headers (<date_time>, <date_time>) exist in one message, which violates RFC5322 section 3.6.
Malicious client IP address	The client IP address (<IP_address>) has been associated with known malicious activity
Possibly forged sender (Yahoo)	The email message claimed from Yahoo (<email_address>) lost required headers.
Executable files with tampered extension names in the attachment	Files in compressed attachment (<file_name>) may be executable files with modified extension names.

Email Characteristics	Description
Anomalous relationship between sender/recipient(s) related email headers	Anomalous relationship between sender/recipient(s) related email headers (<email_address>).
Encrypted attachment intends to bypass antivirus scan engines	Encrypted attachment (<file_name>) with password (<password>) provided in email content possibly intends to bypass antivirus scan engines.
Exploitable attachment	The attached file (<file_name>) may contain exploits.
Email message might be sent from a self-written mail agent due to abnormal transfer encoding in email entities	Content-Transfer-Encoding (<encoding_type>) is abnormal in the email message. The email message might be sent from a self-written mail agent.
Short message body	The body text or the HTML text of the email is short. The text length (<character_count> characters, for body text/HTML text respectively) may suggest that the email content has little meaning.
Replied or forwarded email contains no corresponding headers	The email message was claimed as a forwarded or replied message with subject-tagging (<email_subject>), but the email message does not contain corresponding email headers (RFC 5322).
Email message travels across multiple ASNs	The email message travels across multiple ASNs (<ASN_list>).
Email message travels across multiple countries	The email message travels across multiple countries (<country_code_list>).
Abnormal Content-type behavior in email message	Content-type in email content should not have attributes (<attribute_list>).
Executable files archived in the compressed attachment	The compressed attachment (<file_name>) contains executable files.
Exploitable file types detected in the compressed attachment	The compressed attachment (<file_name>) contains exploitable file types.

Email Characteristics	Description
Inconsistent host domains or unexpected relay or forward	The sender host (<host_address>) belongs to a different domain from the sender account (<email_address>). This message may occur from an unexpected server-side relay or forward.
Email nickname is inconsistent with email address	The recipient account uses an email nickname (<nickname>) that is inconsistent with its email address (<email_address>).
Sender account is inconsistent with reply-to account	The sender account (<email_account>) is inconsistent with the reply-to account (<email_account>).
Sender host name possibly associated with targeted attacks	The sender host name (<host_name>) has been associated with one or more targeted attacks or performed behavior consistent with targeted attacks.
Sender IP address possibly associated with targeted attacks	The sender IP address (<ip_address>) has been associated with one or more targeted attacks or performed behavior consistent with targeted attacks.
Sender account possibly associated with targeted attacks	The sender account (<email_account>) has been associated with one or more targeted attacks or performed behavior consistent with targeted attacks.
Sender account header potentially modified	The email message was sent from an email client or service provider (<user_agent>) that allows modification of the sender address or nickname.
Internal email with a public reply-to domain	The reply-to domain (<domain_name>) belongs to a public messaging service but the sender and recipient domains are the same (<domain_name>). The email message may be disguised to appear internal.
Internal email with a disguised reply-to domain	The reply-to domain (<domain_name>) has been disguised to be similar to the sender and recipient domains (domain_name). The email message may be disguised to appear internal.
Reply-to account disguised to be similar to sender account	The reply-to account (<email_account>) uses a different domain but similar information to the sender account (<email_account>) to disguise the two accounts to be from the same individual.

Email Characteristics	Description
Conversation history in email body	The email message includes a conversation history between (<email_account>) and (<email_account>). This email message may be part of a man-in-the-middle attack.
Nickname of company executive with public domain address	The sender header (<sender_header>) contains a nickname that appears to be a company executive and an email address from a public messaging service.
Sender domain disguised to be similar to recipient domain	The sender domain (<domain_name>) is different but similar to the recipient domain (<domain_name>). The email message may be disguised to appear internal.
Potentially deceptive message header text	Because (<header_text>) closely resembles (<header_text>), this message seems intended to deceive the recipient.
Message contains suspicious content	Some text in the message meets the criteria for the (<category_name>) category, indicating a possible intent to deceive the recipient.
Name of a protected sender used with a suspicious domain	The message uses the name (<sender_name>) in combination with an unfamiliar domain in an apparent attempt to deceive the recipient.

Business Email Compromise log details

Trend Micro Email Security provides detailed information for email messages detected as analyzed or probable Business Email Compromise (BEC) attacks. To view BEC attack details, click the **BEC Report** link in the **Actions** section on the **Mail Tracking Details** screen.

The possible reasons for BEC attack detections are the same as those for social engineering attack detections. See *Social engineering attack log details on page 8-9* for details.

Antispam engine scan details

Trend Micro Email Security provides detailed information about email message scan by the Antispam Engine. To view the scan details, click the **Antispam Engine Scan Details** link in the **Actions** section on the **Mail Tracking Details** screen.

Note

This link is available if the message triggers scan by the Antispam Engine.

TABLE 8-2. Antispam Engine scan details

ITEM	DESCRIPTION
Engine Version (X-TMASE-Version)	The version of the Antispam Engine performing the scan.
Scan Result (X-TMASE-Result)	The scan result for the message. The value is formatted as <TrendType>-<Spam Score>-<Spam Threshold>. • <TrendType>: Threat type. • <Spam Score>: Spam score assigned by the Antispam Engine. A negative score may appear sometimes. For example, in the spam result 10--5.534000-4.000000, the score is -5.534. • <Spam Threshold>: Spam level configured in the spam policy. For details, see *Configuring spam criteria on page 6-23*.
Matched Rule ID (X-TMASE-MatchedRID)	The Antispam Engine rule matched by the message during the scan.

Understanding policy events

This screen enables you to track threat detections in email messages received or sent by Trend Micro Email Security. Trend Micro Email Security maintains up to 90 days of policy event logs. The sliding window for policy event log search is 60 continuous days that may cross calendar months.

Note

The sliding window for policy event log search is 30 days in the Trend Micro Email Security Standard license.

For details about different license versions, see *Available license versions on page 1-26*.

The **Policy Events** screen provides the following search criteria:

- **Period**: The time range for your query.
  - **Last 1 hour**
  - **Last 24 hours**
  - **Last 7 days**
  - **Last 14 days**
  - **Last 30 days**
  - **Custom range**
- **Direction**: The direction of messages.
  - **Incoming**
  - **Outgoing**
- **Recipient**: The envelope recipient address. Specify up to 10 email addresses.
- **Sender**: The envelope sender address. Specify up to 10 email addresses.
- **Email Header (To)**: The recipient address in the message header. Specify up to 10 email addresses.
- **Email Header (From)**: The sender address in the message header. Specify up to 10 email addresses.

Note

Pay attention to the following when setting the preceding four address fields:

- Specify an exact email address or use wildcards (*) to substitute any characters in a search. In the general format of an email address (local-part@domain), be aware that:
  - The local part must be a wildcard (*) or a character string that does not start with *, for example, *@example.com or test*@example.com.
  - The domain must be a wildcard (*) or a character string that does not end with *, for example, example@* or example@*.test.com.
  - If this field is left blank, *@* is used by default.
- Use wildcards (*) strategically to expand or narrow your search results. For example, put a wildcard (*) in the domain part to search by a particular user account on all domains or in the local part to match all accounts on a particular domain.

- **Subject**: The email message subject.

  The **Subject** field supports the following:

  - Fuzzy match

    Type one or multiple keywords for a fuzzy match. If you type more than one keyword, all keywords will be matched based on a logical AND, which means the matched subject must contain every keyword. Wildcards (*) will be automatically added before and after each keyword for a fuzzy match.

  - Exact keyword or phrase match

    Enclose a keyword or phrase in quotes for an exact match. Only records that contain the exact keyword or phrase will be matched.

  For example, there are three email subjects:

- Subject1: Hello world
- Subject2: Hello new world
- Subject3: "Hello"

If you type `Hello world` in the **Subject** field, this is a fuzzy match, and Subject1 and Subject2 will be matched. If you type `"Hello world"`, this is an exact match using quotes, and only Subject1 will be matched. If you want to search for Subject3, be aware that quotes are contained by the subject itself. In this particular case, use backslashes (\) as the escape characters and type `\"Hello\"` for search.

- **Rule Name**: The name of the policy rule that was triggered by email messages.

  The **Rule Name** field supports the following:

  - A maximum of 20 policy rules in use will be listed for you to choose when you click in this text box.
  - Select from the policy rules listed or type keywords for a fuzzy match.

- **Threat Type**: The type of threats detected in email messages.
  - **All**: Query all messages.
  - **Domain-based Authentication**: Query the messages that failed to pass domain-based authentication.
    - **All**: Query the messages that failed Sender IP Match, SPF, DKIM and DMARC authentication.
    - **Sender IP Match**: Query the messages that failed Sender IP Match check.
    - **SPF**: Query the messages that failed SPF check.
    - **DKIM**: Query the messages that failed DKIM verification.
    - **DMARC**: Query the messages that failed DMARC authentication.

- **Ransomware**: Query the messages that are identified as ransomware.
  - **Detected by Web Reputation**:
  - **Detected by Pattern-based Scanning**
  - **Detected by Predictive Machine Learning**
  - **Detected by Virtual Analyzer**
  - **Detected by Spam Protection**
- **Advanced Persistent Threat**: Query the messages that triggered the advanced threat policy.
  - **All**: Query all messages triggering the advanced threat policy.
  - **Analyzed Advanced Threats (Files)**: Query the messages that are identified as advanced file threats according to Virtual Analyzer and the policy configuration
  - **Analyzed Advanced Threats (URLs)**: Query the messages that are identified as advanced URL threats according to Virtual Analyzer and the policy configuration
  - **Probable Advanced Threats**: Query the messages that are treated as suspicious according to policy configuration or the messages that are not sent to Virtual Analyzer due to exceptions that occurred during analysis.
- **Malware**: Query the messages that triggered the malware criteria.

  When **Malware** is selected as the threat type, the **Detected By** field displays with the following options:
  - **All**: Query all messages triggering the malware criteria.
  - **Predictive Machine Learning**: Query the messages containing malware, as detected by Predictive Machine Learning.
  - **Pattern-based scanning**: Query the messages containing malware, as detected by traditional pattern-based scanning.

- **Suspicious Objects**: Query the messages that contain suspicious files and URLs.
  - **All**: Query all messages containing suspicious objects.
  - **Suspicious Files (Apex Central)**: Query all messages containing suspicious files matching the suspicious objects synchronized from Apex Central.
  - **Suspicious Files (Trend Vision One)**: Query all messages containing suspicious files matching the suspicious objects synchronized from Trend Vision One.
  - **Suspicious URLs (Apex Central)**: Query all messages containing suspicious URLs matching the suspicious objects synchronized from Apex Central.
  - **Suspicious URLs (Trend Vision One)**: Query all messages containing suspicious URLs matching the suspicious objects synchronized from Trend Vision One.
- **Scan Exception**: Query the messages that triggered scan exceptions.
  - **Virtual Analyzer scan exception**
  - **Virtual Analyzer submission quota exception**
  - **Password protected attachment**
  - **Other exceptions**
- **Spam**: Query the messages that are identified as spam.
- **Business Email Compromise (BEC)**: Query the messages that triggered the Business Email Compromise (BEC) criteria.
  - **All**: Query all messages triggering the BEC criteria.
  - **Detected by Antispam Engine**: Query the messages that are verified to be BEC attacks by the Antispam Engine.
  - **Detected by writing style analysis**: Query the messages that are verified to be BEC attacks by writing style analysis.

    - **Suspected by Antispam Engine**: Query the messages that are suspected to be BEC attacks by the Antispam Engine.
- **Phishing**: Query the messages that triggered the phishing criteria in Spam Filtering or the security risk criteria in Correlated Intelligence.
    - **All**: Query all messages triggering the phishing criteria in Spam Filtering or the security risk criteria in Correlated Intelligence.
    - **Detected by Antispam Engine**: Query the messages that are verified to be phishing by the Antispam Engine.
    - **Detected by Correlated Intelligence**: Query the messages that are verified to be phishing by Correlated Intelligence.
- **Graymail**: Query the messages that triggered the graymail criteria.
    - **All**: Query all graymail messages.
    - **Marketing message and newsletter**
    - **Social network notification**
    - **Forum notification**
    - **Bulk email message**
- **Web Reputation**: Query the messages that triggered the Web Reputation criteria.
- **Anomaly**: Query the messages that triggered the anomaly criteria in Correlated Intelligence.
    - **All**: Query all messages that triggered the anomaly criteria in Correlated Intelligence.
    - **Suspicious Email**: Query the messages whose anomaly threat type is Suspicious Email.
    - **Possibly Unwanted Email**: Query the messages whose anomaly threat type is Possibly Unwanted Email.
    - **Customized Anomaly**: Query the messages that were detected as anomalies by custom correlation rules defined by customers.

  - **Content**: Query the messages that triggered the message content criteria. For example, a message's header, body or attachment matches the specified keywords or expressions.
  - **Attachment**: Query the messages that triggered the message attachment criteria.
  - **Data Loss Prevention**: Query the messages that triggered the Data Loss Prevention policy.
- **Threat Name**: The name of threats detected in email messages.

  Trend Micro Email Security automatically suggests trending threats (such as quishing, also known as QR code phishing) or top threats detected in your environment.
- **Message ID**: A unique identifier for the message.

When you query policy event information, use the various criteria fields to restrict your searches. After a query is performed, Trend Micro Email Security provides a list of log records that satisfy the criteria. Select one or more records and click **Export Selected** to export them to a CSV file. Click **Export All** to export all the queried log records if needed. If the number of log records to export is large, the export task needs to take time to complete. Go to **Logs** > **Log Export Query** to check the export status. Note that you can export up to 50,000 log records at a time and the maximum number of times of exporting all the queried log records is 5 per day.

The most efficient way to query policy event information is to provide both sender and recipient email addresses, message subject and message ID within a time range that you want to search. For an email message that has multiple recipients, the result will be organized as one entry.

In addition to the search criteria, detailed policy event information provides the following:

- **Timestamp**: The time the policy event occurred. Click on the **Timestamp** value to view the event details for a given message.
- **Message Size**: The size of the message. This information is not always available.

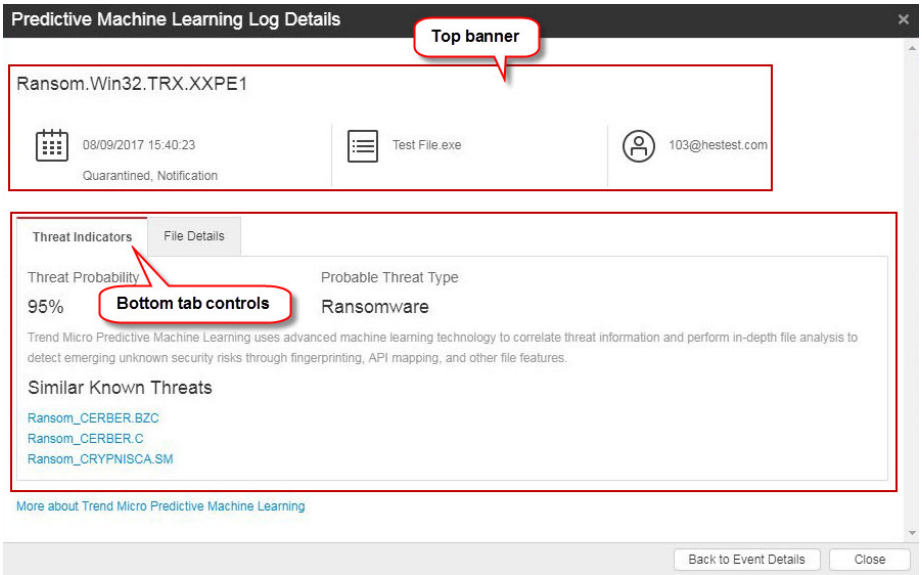
- **Action**: The action taken on the email message.
  - **Attachment sanitized**: Removed active content contained in the attachment.
  - **Attachment deleted upon failure to remove active content**: Deleted the attachment containing active content that failed to be removed.
  - **Attachment deleted**: Deleted the attachment from the message.
  - **BCC**: Sent a blind carbon copy (BCC) to the recipient.
  - **Bypassed**: Did not intercept the message.
  - **Cleaned**: Cleaned the message for malware.
  - **Delivered**: Delivered the message to the recipient.
  - **Message deleted**: Deleted the entire email message.
  - **Notification sent**: Sent a notification message to the recipient when a policy was triggered.
  - **Quarantined**: Held the message in quarantine awaiting user actions on the End User Console. Messages held in quarantine can be reviewed and manually deleted or delivered.
  - **Recipient changed**: Changed the recipient and redirected the message to a different recipient as configured in the policy triggered.
  - **Stamp inserted**: Inserted a stamp into the message body.
  - **Subject tagged**: Inserted configurable text into the message subject line.
  - **Submitted for encryption**: Submitted to the encryption server for processing. After encryption is complete, Trend Micro Email Security will queue the message for delivery.
  - **X-Header inserted**: Inserted an X-Header to the message header.
- (Optional) **Risk Rating**: The risk rating of the message identified by Virtual Analyzer.

- (Optional) **Violating URLs**: The URLs in the message that violated the Web Reputation criteria.
- (Optional) **Violating Files**: The files in the message that violated the malware, ransomware, or attachment-related criteria.
- (Optional) **Malware**: The specific malware detected in the message.
- (Optional) **Scanned File Reports**: The reports for the attached files in messages. If a file is analyzed for advanced threats, the risk level for the file is displayed here. If a report exists, click **View Report** to see the detailed report.

  Detailed reports are available only for suspicious files that are analyzed by Virtual Analyzer.
- (Optional) **Scanned URL Reports**: The reports for the embedded URLs in messages. If a URL is analyzed as advanced threats, the risk level of the URL is displayed here. If a report exists, click **View Report** to see the detailed report.
- (Optional) **DLP Incident**: The information about the DLP incident triggered by the message. Click **View Details** to check the incident details.
- (Optional) **Analyzed Report**: The information about BEC related characteristics that were detected in the message.
- (Optional) **Exception Details**: The specific exception that was triggered by the message.
- (Optional) **Antispam Engine Scan Details**: The details of the Antispam Engine scan for the message. For details, see *Antispam engine scan details on page 8-13*.

Predictive Machine Learning log details

You can view a comprehensive report for each Predictive Machine Learning log detection by clicking the **Predictive Machine Learning Log Details** link on the **Policy Event Details** screen.



The **Predictive Machine Learning Log Details** screen consists of two sections:

- Top banner: Specific details related to this particular log detection
- Bottom tab controls: Details related to the Predictive Machine Learning threat, including threat probability scores and file information

The following table discusses the information provided in the top banner.

TABLE 8-3. Log Details - Top Banner

SECTION	DESCRIPTION
Detection name	Indicates the name of the Predictive Machine Learning detection Example: Ransom.Win32.TRX.XXPE1
Detection time / Action	Indicates when this specific log detection occurred and the action taken on the threat
File name	Indicates the name of the file that triggered the detection
Recipient	Displays the recipient of the email message that triggered the detection

The following table discusses the information provided on the bottom tabs.

TABLE 8-4. Log Details - Tab Information

TAB	DESCRIPTION
Threat Indicators	Provides the results of the Predictive Machine Learning analysis • **Threat Probability**: Indicates how closely the file matched the malware model • **Probable Threat Type**: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • **Similar Known Threats**: Provides a list of known threat types that exhibit similar file features to the detection
File Details	Provides general details about the file properties for this specific detection log

Understanding URL click tracking

The **URL Click Tracking** screen enables you to track the URL clicks where Trend Micro Email Security provides Time-of-Click Protection.

Trend Micro Email Security maintains up to 30 days of URL click tracking log information.

The **URL Click Tracking** screen provides the following search criteria:

- **Dates**: The time range for your query.
- **Direction**: The direction of messages.

Note

URL click tracking applies only to URL clicks protected by Trend Micro Email Security using Time-of-Click Protection.

- **Recipient**: The recipient email address.
- **Sender**: The sender email address.
- **URL**: The URL contained in the message.
- **Message ID**: A unique identifier for the message.

When you query URL click tracking information, use the various criteria fields to restrict your searches. After a query is performed, Trend Micro Email Security provides a list of log records that satisfy the criteria. Select one or more records and click **Export to CSV** to export them to a CSV file.

In addition to the search criteria, detailed URL click tracking information provides the following:

- **Time of Click**: The time a URL was clicked.
- **Action Applied**: The action taken on the URL. For all the actions, see Actions below.
  - Blocked: Trend Micro Email Security blocked the URL that a user wanted to access.
  - Allowed: Trend Micro Email Security allowed a user to access the requested URL.
  - Warned and stopped: Trend Micro Email Security warned a user of the threat, and the user stopped access to the URL.
  - Warned but accessed: Trend Micro Email Security warned a user of the threat, but the user continued to access the URL.

Understanding audit log

The **Audit Log** screen enables you to track the administration and user events occurred in Trend Micro Email Security.

Trend Micro Email Security maintains up to 180 days of audit log information.

The **Audit Log** screen provides the following search criteria:

- **Account** and **Activity Type**: The account name and the type of activity for which you want to search the audit log.
- **Dates**: The time range for your query.

When you query audit logs, use the various criteria fields to restrict your searches. After a query is performed, Trend Micro Email Security provides a list of log records that satisfy the criteria. Select one or more records and click **Export to CSV** to export them to a CSV file.

To see the detail of an event, click on the time under the **Timestamp** column.

The **Audit Log Details** screen displays the following information:

- **User**: The administrator or user name under which the event occurred.
- **Event Type**: The type of event that occurred.
- **Timestamp**: The date and time when the event occurred.
- **Affected Domain(s)**: The domains (if any) that were affected by the event.
- **Fields**:
  - **Field**: The name of the fields that were affected by the event.
  - **New Value**: The latest value of the field after the event occurred.
  - **Previous Value**: The previous value of the field (if any) before the event occurred.

Configuring syslog settings

When receiving events, Trend Micro Email Security stores the events in its database and forwards syslog messages to an external syslog server in a structured format, which allows third-party application integration.

The **Syslog Settings** screen is composed of the following tabs:

- **Syslog Forwarding**: Specifies the mapping between syslog servers and different types of logs.
- **Syslog Server Profiles**: Enables you to add, edit or delete syslog servers for syslog forwarding.

To ensure Trend Micro Email Security can properly forward syslog messages, configure your firewall to accept connections from the following IP addresses or CIDR blocks:

- North America, Latin America and Asia Pacific:

  `18.208.22.64/26`

  `18.208.22.128/25`

  `18.188.9.192/26`

  `18.188.239.128/26`

- Europe and Africa:

  `18.185.115.0/25`

  `18.185.115.128/26`

  `34.253.238.128/26`

  `34.253.238.192/26`

- Australia and New Zealand:

  `13.238.202.0/25`

  `13.238.202.128/26`

- Japan:

  18.176.203.128/26

  18.176.203.192/26

  18.177.156.0/26

  18.177.156.64/26

  15.168.56.0/25

  15.168.49.64/26

  15.168.56.128/26

- Singapore:

  13.213.174.128/25

  13.213.220.0/26

- India:

  3.110.59.128/25

  3.110.71.192/26

- Middle East (UAE):

  3.29.202.0/25

  3.29.194.192/26

Note

Be aware that Trend Micro Email Security keeps syslog messages for 7 days if your syslog server is unavailable. Messages older than 7 days will not be restored when your syslog server recovers.

Syslog forwarding

Configure the syslog server where Trend Micro Email Security forwards different types of logs.

Procedure

1. Go to **Logs** > **Syslog Settings**.

   The **Syslog Forwarding** tab appears by default.

2. From the **Detection logs** drop-down list, select a syslog server for Trend Micro Email Security to forward syslog messages on threat detections.

   a. Select from any of the following options:

      - **None**: Select this option to disable syslog forwarding for this type of logs.
      - **New**: Select this option to add a new syslog server.

        For details on syslog server profiles, see *Syslog server profiles on page 8-31*.
      - Any syslog server profile: select any profile you configured for forwarding this type of logs.

   b. Select the **Include spam detections** check box if you want to include spam detection logs in syslog forwarding.

3. From the **Audit logs** drop-down list, select a syslog server for Trend Micro Email Security to forward syslog messages for audit logs.

4. From the **Mail tracking logs** drop-down list, select a syslog server for Trend Micro Email Security to forward syslog messages for mail tracking logs, which are related to the accepted traffic that passed through Trend Micro Email Security.

   Note

   For details about the accepted traffic defined in mail tracking logs, see *Understanding mail tracking on page 8-2*.

5. From the **URL click tracking logs** drop-down list, select a syslog server for Trend Micro Email Security to forward syslog messages for URL click tracking logs.

Syslog server profiles

Trend Micro Email Security allows you to add, edit or delete syslog server profiles for syslog forwarding.

Procedure

1. Go to **Logs** > **Syslog Settings**.

   The **Syslog Forwarding** tab appears by default.

2. Click the **Syslog Server Profiles** tab.

3. Click **Add** or click the name of an existing profile name.

   The **Add Syslog Server Profile** or **Edit Syslog Server Profile** screen appears.

4. Specify or edit the following for a syslog server:

   - **Profile name**: Unique profile name for a syslog server.
   - **Description**: Description of this profile.
   - **Server address**: IP address or FQDN of the syslog server.
   - **Port**: Port number of the syslog server.
   - **Protocol**: Protocol to be used to transport logs to the syslog server.
     - **TCP**
     - **TLS+TCP**

       This option applies the Transport Layer Security (TLS) encryption for messages sent to the syslog server.
   - **Format**: Format in which logs are sent to the syslog server.
     - **Key value**
     - **CEF**

       For details about the Common Event Format (CEF) format, see *Content mapping between log output and CEF syslog type on page 8-33*.

- **Severity**: Severity level assigned to syslog messages.
  - **Emergency**
  - **Alert**
  - **Critical**
  - **Error**
  - **Warning**
  - **Notice**
  - **Informational**
  - **Debug**
- **Facility**:
  - **user**
  - **mail**
  - **auth**
  - **authpriv**
  - **local0**
  - **local1**
  - **local2**
  - **local3**
  - **local4**
  - **local5**
  - **local6**
  - **local7**
- **Enable TLS authentication**: Whether to enable TLS authentication for the connection between the syslog server and Trend Micro Email Security.

5. Click **Save**.

   If you select the **Enable TLS authentication** check box, Trend Micro Email Security starts to execute TLS authentication.

   - If the TLS authentication is successful, the new syslog server profile appears in the profile list on the **Syslog Server Profiles** tab or the existing profile is updated.
   - If the TLS authentication is unsuccessful, the **Peer Certificate Summary** dialog box pops up, displaying peer certificate information such as the certificate ID, subject, and subject key ID.

     When detecting that the certificate is not issued by a known Certificate Authority (CA), Trend Micro Email Security prompts you to trust or not trust the certificate. In other cases, an error message is displayed, instructing you how to fix the error.

Note

To test the connection between the syslog server and Trend Micro Email Security, click **Test** under **Connection**.

Content mapping between log output and CEF syslog type

To enable flexible integration with third-party log management systems, Trend Micro Email Security supports Common Event Format (CEF) as the syslog message format.

Common Event Format (CEF) is an open log management standard created by HP ArcSight. Trend Micro Email Security uses a subset of the CEF dictionary.

The following tables outline syslog content mapping between Trend Micro Email Security log output and CEF syslog types.

CEF detection logs

TABLE 8-5. CEF Detection Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TMES
Header (pver)	Appliance version	Example: 1.0.0.0
Header (eventid)	Signature ID	100101
Header (eventName)	Description	DETECTION
Header (severity)	Email severity	6
rt	Log generation time	Example: 2019-12-10T08:26:46.728Z
cs1Label	Event type	eventType
cs1	Event type	Example: ransomware
cs2Label	Domain name	domainName
cs2	Domain name	Example: example1.com
suser	Email sender	Example: user1@example1.com
duser	Email recipients	Example: user2@example2.com
cs3Label	Email message direction	direction
cs3	Email message direction	• incoming • outgoing
cs4Label	Unique message identifier	messageId
cs4	Unique message identifier	Example: 20160518164213822374 7@trend.com
msg	Email subject	Example: hello

CEF Key	Description	Value
cn1Label	Email message size	messageSize
cn1	Email message size	Example: 1809
cs5Label	Violated event analysis	policyName
cs5	Violated event analysis	Example: Spam
cs6Label	Violated event details	details
cs6	Violated event details	Example: `{"threatNames":"Troj", "fileInfo": [{"fileName":"file1","fileSha256":"abcd1234dae60bcae54516be6c9953b4bb9644e188606ceac00feebf95bbf10e", "threatName":"Troj"}]}`
act	Action in the event	• Quarantine • Bypass • Delete Attachment • Insert Stamp • Tag Subject • Change Recipient • Delete Message • Send Notification • Clean • BCC • Deliver • Insert X-Header • Encryption in progress

Log sample:

```
CEF:0|Trend Micro|TMES|1.0.0.0|100101|DETECTION|6|rt=2019-12-10T08:26:46.728Z
cs1Label=eventType cs1=virus cs2Label=domainName cs2=example1.com
suser=user1@example1.com duser=user2@example2.com cs3Label=direction
cs3=incoming cs4Label=messageId cs4=20160518164213822374 7@trend.com
msg=test sample cn1Label=messageSize cn1=1809 cs5Label=policyName
cs5=Test Rule act=Quarantine cs6Label=details cs6={"threatNames":"Troj",
"fileInfo":[{"fileName":"file1",
"fileSha256":"abcd1234dae60bcae54516be6c9953b4bb9644e188606ceac00feebf95bbf10e",
"threatName":"Troj"}]}
```

CEF audit logs

TABLE 8-6. CEF Audit Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TMES
Header (pver)	Appliance version	Example: 1.0.0.0
Header (eventid)	Signature ID	300101
Header (eventName)	Description	AUDIT
Header (severity)	Email severity	4
rt	Log generation time	Example: 2018-06-28 03:22:31
cs1Label	Account type	accountType
cs1	Account type	• end user • admin
suser	Email sender	Example: user1@example1.com
cs2Label	Event type	eventType
cs2	Event type	Example: End-User Actions

CEF Key	Description	Value
act	Action in the event	Example: User login to End User Console
cs3Label	Domain affected by the event	affectedDomains
cs3	Domain affected by the event	Example: example1.com

Log sample:

```
CEF:0|Trend Micro|TMES|1.0.0.0|300101|AUDIT|4|rt=2018-06-28 03:22:31
cs1Label=accountType cs1=end user suser=user1@example1.com cs2Label=eventType
cs2=End-User Actions act=User login to End User Console cs3Label=affectedDomains
cs3=
```

CEF mail tracking logs (accepted traffic)

Table 8-7. CEF Mail Tracking Logs (Accepted Traffic)

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TMES
Header (pver)	Appliance version	Example: 1.0.0.0
Header (eventid)	Signature ID	400101
Header (eventName)	Description	TRACKING
Header (severity)	Email severity	4
rt	Log generation time	Example: 2019-12-10T08:26:46.728Z
suser	Email sender	Example: user1@example1.com
duser	Email recipients	Example: user2@example2.com
msg	Email subject	Example: hello
src	Source IP address	Example: 10.1.144.199

CEF Key	Description	Value
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
cs1Label	Internal email message ID	mailUuid
cs1	Internal email message ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Email message direction	direction
cs2	Email message direction	• incoming • outgoing
cs3Label	Unique message identifier	messageId
cs3	Unique message identifier	Example: 20160518164213822374 7@trend.com
cs4Label	Email attachments	attachments
cs4	Email attachments	Example: [["filename", "sha256"], ["filename", "sha256"], ...]
cn1Label	Email message size	messageSize
cn1	Email message size	Example: 1809
act	Action on an email message	• Bounced • Temporary delivery error • Deleted • Delivered • Expired • Quarantined • Redirected • Submitted to sandbox • Password analyzing
cs5Label	TLS information	tlsInfo

CEF Key	Description	Value
cs5	TLS information	Example: upstreamTLS: None; downstreamTLS: TLS 1.2
cs6Label	URLs embedded in email	embeddedUrl
cs6	URLs embedded in email	Example: ["http://example1.com", "http://example2.com"]

Log sample:

```
CEF:0|Trend Micro|TMES|1.0.0.0|400101|TRACKING|4|rt=2019-12-10T08:26:46.728Z
suser=user1@example1.com duser=user2@example2.com msg=DLP--test src=1.1.1.1
deviceTranslatedAddress=2.2.2.2 cs1Label=mailUuid
cs1=7ea8f636-c26e-4b78-a341-9b5becb83db7 cs2Label=direction cs2=incoming
cs3Label=messageId cs3=<20180206155858177203l@example.com>
cn1Label=messageSize cn1=41438 act=Delivered cs4Label=attachments
cs4=[{"sha256":"f78960148721b59dcb563b9964a4d47e2a834a4259f46cd12db7c1cfe82ff32e"}]
cs5Label=tlsInfo cs5=upstreamTLS: None; downstreamTLS: TLS 1.2
cs6Lable=embeddedUrl cs6=["http://example1.com", "http://example2.com"]
```

Chapter 9

Reports

Trend Micro Email Security provides reports to assist in mitigating threats and optimizing system settings. Generate reports based on a daily, weekly, monthly, or quarterly schedule. Trend Micro Email Security offers flexibility in specifying the content for each report within your managed domain scope.

The reports generate in PDF format.

Generated reports

The **Generated Reports** tab shows all reports generated by Trend Micro Email Security.

From the **Frequency** drop-down list, sort out the generated reports you want to view by frequency. You can also specify a report name to search for the desired report.

Field	Description
Reporting period	Time range that a report covers
Frequency	How often that the report is generated
Format	File format of the report, which is PDF only
Last generated	The most recent time when the report was generated

In the generated reports table, you can sort the reports by the time they were generated and download reports to your local system for further analysis.

The information displayed in a report could vary depending on the options you select, and threat types included in reports are consistent with those shown on the dashboard.

Trend Micro Email Security saves a maximum of 31 daily reports, 12 weekly reports, 12 monthly reports, and 4 quarterly reports for each configured report setting. For example, if you create a daily report with setting A and another daily report with setting B, Trend Micro Email Security will save up to 31 reports for setting A and 31 reports for setting B. If the number of reports reaches the maximum, the oldest report will be overwritten. You can select and delete one or multiple generated reports that no longer needed.

Report settings

The **Report Settings** tab allows you to manage and configure report settings for scheduled report generation and delivery.

Scheduled reports automatically generate on a predetermined day based on the configured frequency, and this day is not configurable. Specifically,

- Daily reports generate on every day.
- Weekly reports generate on every Sunday.
- Monthly reports generate on the first calendar day of every month.
- Quarterly reports generate on the first calendar day of every quarter.

Note

This screen does not contain any generated reports. To view the generated reports, go to **Reports** > **Generated Reports**.

Procedure

1. Go to **Reports** > **Report Settings**.
2. Click **Add**, and then complete settings for the report.

Section	Setting
General Settings	• **Status**: Move the toggle to enable or disable the report. • **Name**: Specify a name that uniquely identifies the report. • **Description**: Optionally add a description for the report. • **Frequency**: Select how often you want the report to be generated. Options include **Daily**, **Weekly**, **Monthly**, and **Quarterly**.
Report Content	Specify the detailed information contained in the report.
Managed Domains	Select the domains on which you want to include email traffic and threat detection data in the report. Only domains you have permission to manage are available for selection. To view the domains you can manage, go to the account management settings.

Section	Setting
Notifications	• **Recipients**: Specify the email addresses of recipients that receive the report via email. **Note** Make sure the recipients' domains are your managed domains. Separate multiple recipients with a semicolon. A maximum of 10 recipients is supported. • **Sending schedule**: Specify when reports will be sent by email based on the configured **Frequency** and time zone. • **Note** When a monthly report is set to send reports on the 29th, 30th, or 31st day, the report is delivered on the last day of the month for months with fewer days. For example, if you select 31, the report is delivered on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

3. Click **Save**.

Chapter 10

Configuring administration settings

Policy objects

Common policy objects, such as keyword expressions, notifications, stamps and Web Reputation Approved List, simplifies policy management by storing configurations that can be shared across all policies.

Managing address groups

Creating an address group facilitates your policy management. You can use **Address Groups** screen to manage address groups in Trend Micro Email Security.

TABLE 10-1. Address Groups Screen

TASKS	STEPS
Querying Address Groups	1. Specify an address group name, an email address, or a domain name. 2. Click **Search**. **Note** For **Email**, make sure you specify the exact email address or use wildcards (*) to represent the local part, domain, or subdomain. For more information about the valid formats, see the table below. The search returns a range of relevant results. For example, searching for `name@*.example.com` can return `name@info.example.com`, `name@*.example.com`, `name@*.com`, `name@*`, `*@info.example.com`, `*@*.example.com`, and `*@*.com`.
Adding an Address Group	Click **Add**. 1. In the **Basic Information** section, provide the following information: • **Name**: A name for the address group. • **Description** (optional): A description for the address group.

Tasks	Steps

	• **Internal group** (optional): An address group that only contains managed domains or email addresses that belong to managed domains.
	
	Important
	You must use internal groups when specifying senders (or sender exceptions) in outbound policies or recipients (or recipient exceptions) in inbound policies.
	
	• In the **Email Addresses** section, choose either of the following ways to specify the email addresses in the address group:
	  • Specify the email address and its description, and click **Add**.
	
	Note
	  • Only one email address can be added at a time.
	  • For more information about the valid formats of the email addresses, see the table below.
	  • The maximum length of the description is 1024 characters.
	
	  • Import email addresses.
	  a. Click **Import**.
	  b. Next to **File location**, browse and select a CSV file to import.
	
	  You can click **Download sample file** to view a sample of a properly formatted file.
	
	  Trend Micro Email Security checks all the entries in the selected file to identify any

Tasks	Steps
	invalid and duplicate email addresses as well as overlong descriptions. c. After you confirm all the entries to be imported, click **Import**. To search for email addresses, type an email address or domain name and click **Search**. **Note** Make sure you specify the exact email address or use wildcards (*) to represent the local part, domain, or subdomain. For more information about the valid formats, see the table below. The search returns a range of relevant results. For example, searching for `name@*.example.com` can return `name@info.example.com`, `name@*.example.com`, `name@*.com`, `name@*`, `*@info.example.com`, `*@*.example.com`, and `*@*.com`. • Click **Submit**.
Editing an Address Group	In the **Address Groups** list, click the name of the group you want to edit and follow the instructions in **Adding an Address Group** procedure in this table. **Note** A hybrid address group cannot be changed into an internal group if the group contains at least one wildcard domain member.
Deleting Address Groups	In the **Address Groups** list, select the groups to delete. Click **Delete**, and click **OK** to confirm.

Tasks	Steps
	Note Only address groups that are not referenced by any policies can be deleted.

The following table displays format examples for address groups:

Table 10-2. Format Examples for Address Groups

Valid for Internal Address Group	Valid for Hybrid Address Group
name@example.com name@info.example.com	name@example.com name@info.example.com
*@example.com *@info.example.com	*@example.com *@info.example.com
	name@*
	name@*.example.com
	@.example.com

Managing the URL keyword exception list

URLs that contain any of the specified keywords will bypass Time-of-Click Protection and Virtual Analyzer scanning. This bypass is useful, for example, for one-click URLs, because subjecting such URLs to the two types of scanning can possibly invalidate the links.

Note that the protocol and domain parts of an URL will not be used for keyword match. The following is an example:

Keyword	URL	Keyword Match Result
registration	http://example.com/**registration**	Match

KEYWORD	URL	KEYWORD MATCH RESULT
	http://**registration**.example.com/Dashboard?T=XCdSN	Not match

You can manage keywords on the **URL Keyword Exception List** screen.

TABLE 10-3. URL Keyword Exception List Screen

Add keywords	1. Click **Add**. 2. Specify a keyword that consists of 3 to 256 alphanumeric characters and underscores. 3. Click **Save**. The new keyword appears in the keyword list. 4. Add multiple entries if necessary. **Note** If your Customer Licensing Portal or Licensing Management Platform account has created multiple administrator accounts, be aware that the total number of entries added by all the accounts cannot exceed 100 entries.
Delete keywords	Select the keywords you want to delete and click **Delete**.

Managing the Web Reputation approved list

The Web Reputation Approved List provides you a way to bypass scanning and blocking of URLs that you considered safe. When URLs match the domains, IP addresses, or URLs specified in the Web Reputation Approved List, the URLs will not be scanned by Time-of-Click Protection and Virtual Analyzer. You can configure whether to bypass Web Reputation Services as well.

Procedure

1. Enable the Web Reputation Approved List.
   a. Create or edit an inbound or outbound spam policy.

      For details about configuring a policy, see *Configuring policies on page 6-1*.

   b. Click the **Scanning Criteria** tab.

   c. Select and click **Web reputation**.

   d. Under **Web Reputation Approved List**, select the **Enable the Web Reputation Approved List** check box.

2. Manage the Web Reputation Approved List.

   The Web Reputation Approved List is available in the following path:

   Administration > **Policy Objects** > **Web Reputation Approved List**

Action	Description
Search for an item	Type a domain name, IP address, or URL in the **Item** text box, or select a type from the **Type** drop-down box, and click **Search**.

Action	Description
Add an item	a. Click **Add**. The **Add Item** screen appears. b. Specify **Domain**, **IP address**, or **URL** as the type. c. Type a domain, IP address, or URL. **Note** Specify a domain in one of the following formats: • example.com • subdomain.example.com • *.example.com This format matches all the subdomains under the example.com domain, for example, a.example.com, a.b.example.com. d. (Optional) Description: Provide a description. e. Select whether to bypass Web Reputation Services. **Note** This item always bypasses Time-of-Click Protection and Virtual Analyzer scanning. f. Click **Save**.
Edit an item	a. Click an item in the **Item** column. b. On the **Edit Item** screen, change the description or select whether to bypass Web Reputation Services. c. Click **Save**.

Action	Description
Import items	a. Click **Import**. b. On the **Import Items** screen, click **Choose File** and select a CSV file to import. You can click **Download sample file** to download the file for reference or use it for import. Make sure the CSV file meets the following requirements: • The file size does not exceed 2 MB. • Column A (item), column C (item type), and Column D (whether to bypass Web Reputation Services) are all filled. c. Select **Merge** or **Overwrite** as the import option. d. Click **Preview**. e. After you confirm all the entries to be imported, click **Import**.
Delete items	a. Select one or multiple items from the existing list and click **Delete**. b. Click **OK** to confirm your deletion.

Managing correlation rules and detection signals

Manage predefined and custom correlation rules and detection signals that you can use for anomaly detection by Correlated Intelligence.

Trend Micro defines a set of correlation rules and detection signals, and continually introduces new rules and signals. Each predefined correlation rule consists of one or multiple predefined detection signals.

You can also add custom correlation rules to accommodate detection requirements in your environment.

The following table outlines the available actions on the **Correlation Rules** tab of the **Correlation Rules and Detection Signals** screen.

TABLE 10-4. The Correlation Rules Tab

ACTION	DESCRIPTION
Enable or disable a correlation rule	On the **Correlation Rules** tab, click the **Enable** or **Disable** icon in the **Status** column of a correlation rule. The configurations apply to anomaly detection in all Correlated Intelligence policy rules.

View predefined correlation rule details	View the targeted threat type and aggressive level of a predefined correlation rule.
	
	• **Targeted threat type**: The currently supported threat types of Trend Micro specified anomalies include **Suspicious Email** and **Possibly Unwanted Email**.
	
	• **Aggressive level**: Trend Micro classifies its predefined correlation rules for anomaly detection into three aggressive levels.
	
	  • **Moderate**: This level is designed to seek a balance between effective anomaly detection and maintaining a relatively low rate of false positives. It is suitable for everyday monitoring and for customers who prefer a safer approach without significant disruptions to their regular email flow.
	
	  • **Aggressive**: This level increases the sensitivity of anomaly detection and offers a more robust detection capability, which may result in a higher number of false positives. It is tailored for customers who require more stringent security measures to combat sophisticated attacks and are willing to accept some trade-offs in false alerts.
	
	  • **Extra Aggressive**: This highest level of aggression is recommended for critical situations, such as during an active attack or after a security breach has been identified. It provides the most aggressive form of prevention but may significantly impact normal email communication due to the high likelihood of false positives.

Add a custom correlation rule	Select one or multiple predefined or custom detection signals to define a custom correlation rule. For details, see *Adding a custom correlation rule on page 10-11*.
Edit a custom correlation rule	Click the name of a custom correlation rule, and then modify the basic properties and statement definition of the rule.

Action	Description
View detection signals comprising a correlation rule	Click the name of a correlation rule to open the rule detail screen and understand what the rule is about, what detection signals are used, and how the rule is matched.
Search for correlation rules	Use the filter fields to search for desired correlation rules by rule name, status, targeted threat type, or aggressive level.

The following table outlines the available actions on the **Detection Signals** tab.

Table 10-5. The Detection Signals Tab

Action	Description
View predefined detection signal details	View each detection signal defined by Trend Micro and what the signal is about.
Add a custom detection signal	Select one of the predefined conditions to define a custom detection signal. For details, see *Adding a custom detection signal on page 10-12*.
View conditions comprising a detection signal	Click the name of a detection signal to open the signal detail screen and understand what the signal is about, what condition is used, and how the condition is configured.
Edit a custom detection signal	Click the name of a custom detection signal, and then modify the basic properties and definition of the signal.
Search for detection signals	Use the filter field to search for desired signals by signal name and signal type.

Adding a custom correlation rule

Add custom correlation rules to accommodate detection requirements in your environment.

Procedure

1. On the **Correlation Rules** tab, click **Add**.

2. Specify a name for the rule and optionally provide a description in the **Basic Properties** area. The name can help clearly identify what anomaly you want to detect.
3. Define one or multiple statements that comprise the rule.

   A statement combines detection signals and the AND operator.

   a. Select a detection signal type from the drop-down list to filter out the available signals, and then select a desired signal from the next drop-down list.

   b. If you need one more signals to comprise the statement, click **Add Signal**.

   c. Repeat the previous step to add more signals to the statement.

      Click the icon to remove a signal if it is not needed.

   d. When the statement definition is completed, click **Add Statement to Rule**.
4. Define more statements as needed and add them to the **Rule Definition** area by repeating Step 3.
5. View and confirm that the rule definition meets your requirement.

   A rule combines statements and the OR operator to tag and detect the required anomalies in your environment. The rule is matched when any of its statements is met.
6. Click **Save**.

Adding a custom detection signal

Add custom detection signals that are unique and critical to your environment.

Procedure

1. On the **Detection Signals** tab, click **Add**.

2. Specify a name for the signal and optionally provide a description in the **Basic Properties** area. The name can help clearly identify what signals deviating from normal behaviors that you want to detect.
3. In the **Signal Definition** area, define the signal.
   a. Select a condition field from the drop-down list.
   b. Select the desired operator from the drop-down list.

      Available operators include both integer value comparison operators and string value matching operators. For example, ≤ means that the condition field contains an integer that less than or equal to the specified integer value.
   c. Enter or select the desired value as a string or integer if necessary.

      The following table describes the supported conditions

Condition Field	Operator	Description
Sender address	• Is In • Is Not In	The sender's address of an email is or is not in the specified email address list. A maximum of 50 email addresses is supported. The asterisk (*) wildcard is supported to represent zero or more characters in the local part and domain of an email address, for example, `*@example.com`, `name@*.com`, and `*@*.example.com`
Sender domain registration age	≤	The sender's domain in the **From** header field of an email was registered for less than or equal to the specified number of days. Default value: 7. Range: 1 - 366. Unit: days. For example, setting the value to 1 means that the sender domain has just been registered within the past 24 hours.

Condition Field	Operator	Description
Sender domain activity within the past 30 days	≤	The sender's domain in the **From** header field of an email has exhibited activity for less than or equal to the specified number of days in the past 30 days. Default value: 5. Range: 0 - 30. Unit: days. For example, setting the value to 0 means that the sender domain has not shown any activity in the past 30 days.
Sender address activity within the past 30 days	≤	The sender's address in the **From** header field of an email has exhibited activity for less than or equal to the specified number of days in the past 30 days. Default value: 5. Range: 0 - 30. Unit: days. For example, setting the value to 0 means that the sender address has not shown any activity in the past 30 days.
Reply-To domain activity within the past 30 days	≤	The recipient's domain in the **Reply-To** header field of an email has exhibited activity for less than or equal to the specified number of days in the past 30 days. Default value: 5. Range: 0 - 30. Unit: days. For example, setting the value to 0 means that the Reply-To domain has not shown any activity in the past 30 days.

Condition Field	Operator	Description
Reply-To address activity within the past 30 days	≤	The recipient's address in the **Reply-To** header field of an email has exhibited activity for less than or equal to the specified number of days in the past 30 days. Default value: 5. Range: 0 - 30. Unit: days. For example, setting the value to 0 means that the Reply-To address has not shown any activity in the past 30 days.
URL domain registration age in email	≤	The domain of any URL in an email was registered for less than or equal to the specified number of days. Default value: 30. Range: 1 - 366. Unit: days. For example, setting the value to 1 means that the domain of at least one URL in an email has just been registered within the past 24 hours.

Note

Currently, you can configure only one condition in the signal definition.

4. View and confirm that the signal definition meets your requirement.
5. Click **Save**.

Keyword expressions

Keyword expressions can be:

- Groups of literal text characters
- Patterns, defined using symbols (regular expressions) that describe a range of possible groupings of text

- A mixture of literal text and symbolic patterns

For example, a keyword expression might be a single word, a phrase, or even a substring; or it might be a pattern that defines a more general grouping of text, such as an asterisk used as a wildcard to stand in for any text of one or more characters in length.

Regular expressions, often called regexes, are sets of symbols and syntactic elements used to match patterns of text. The symbols stand in for character patterns or define how the expression is to be evaluated. Using regular expressions is sophisticated way to search for complex character patterns in large blocks of text. For example, suppose you want to search for the occurrence of an email address—any email address—in a block of text. You can build a regular expression that will match any pattern of text that has any valid name string, followed by an @ character, followed by any valid domain name string, followed by a period, followed by any valid domain suffix string.

Trend Micro Email Security uses a subset of POSIX regular expression syntax.

Tip

If your expression includes the characters \ | ( ) { } [ ] . ^ $ * + or ?, you must escape them by using a \ immediately before the character. Otherwise, they will be assumed to be regular expression operators rather than literal characters.

This help system contains a brief summary of common regex elements, but a thorough guide to regular expression syntax is beyond the scope of this help system. However, there are many sources of reference information available on the Web or in books.

About regular expressions

Trend Micro Email Security treats all keyword expressions as regular expressions. Trend Micro Email Security uses a subset of POSIX regular expression syntax and supports the following regular expressions.

Characters

REGULAR EXPRESSION	DESCRIPTION
. (dot)	Any character (byte) except newline
x	The character 'x'
\\	The character '\'
\a	The alert (bell) character (ASCII 0x07)

\b	• If this meta-symbol is within square brackets [] or by itself, it will be treated as the backspace character (ASCII 0x08). For example, [\b] or \b
	• If this meta-symbol is at the beginning (or end) of a regular expression, it means any matched string of the regular expression must check whether the left (or right) side of the matched string is a boundary. For example:
	  • \bluck > left side must be the boundary
	  • luck\b > right side must be the boundary
	  • \bluck\b > both sides must be the boundary
	• If this meta-symbol appears in the middle of a regular expression, it will cause a syntax error.

\f	The form-feed character (ASCII 0x0C)
\n	The newline (line feed) character (ASCII 0x0A)
\r	The carriage-return character (ASCII 0x0D)
\t	The normal (horizontal) tab character (ASCII 0x09)
\v	The vertical tab character (ASCII 0x0B)

REGULAR EXPRESSION	DESCRIPTION
\n	The character with octal value 0n (0 <= n <= 7)
\nn	The character with octal value 0nn (0 <= n <= 7)
\mnn	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh	The character with a hexadecimal value 0xhh, for example, \x20 means the space character

Tip

If your expression includes the characters \ | ( ) { } [ ] . ^ $ * + or ?, you must escape them by using a \ immediately before the character. Otherwise, they will be assumed to be regular expression operators rather than literal characters.

Bracket expression and character classes

Bracket expressions are a list of characters and/or character classes enclosed in brackets []. Use bracket expressions to match single characters in a list, or a range of characters in a list. If the first character of the list is the carat ^ then it matches characters that are not in the list.

For example:

EXPRESSION	MATCHES
[abc]	a, b, or c
[a-z]	a through z
[^abc]	Any character except a, b, or c
[[:alpha:]]	Any alphabetic character (see below)

The following character classes must be within a bracket expression or it will be treated as a common expression.

CHARACTER CLASS	DESCRIPTION
[:alpha:]	Alphabetic characters
[:digit:]	Digits
[:alnum:]	Alphabetic characters and numeric characters
[:cntrl:]	Control character
[:blank:]	Space and tab
[:space:]	All white space characters
[:graph:]	Non-blank (not spaces, control characters, or the like)
[:print:]	Like [:graph:], but includes the space character
[:punct:]	Punctuation characters
[:lower:]	Lowercase alphabetic character
[:upper:]	Uppercase alphabetic character
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)

For example:

- **a[[:digit:]]b** matches "a0b", "a1b", ..., "a9b".
- **a[:digit:]b** matches "a:b", "adb", ..., "atb".
- **[[:digit:]abc]** matches any digit or any of "a", "b", and "c".
- **[abc[:digit:]]** matches any digit or any of "a", "b", and "c".

For a case-insensitive expression, [:lower:] and [:upper:] are equivalent to [:alpha:].

Boundary matches

EXPRESSION	DESCRIPTION
^	Beginning of line
$	End of line

Greedy quantifiers

EXPRESSION	DESCRIPTION
R?	Matches R, once or not at all
R*	Matches R, zero or more times
R+	Matches R, one or more times
R{n}	Matches R, exactly n times
R{n,}	Matches R, at least n times
R{n,m}	Matches R, at least n but no more than m times

R is a regular expression.

Trend Micro does not recommend using ".*" in a regular expression. ".*" matches any length of letters and the large number of matches may increase memory usage and affect performance.

For example:

If the content is 123456abc, the regular expression ".*abc" match results are:

- 12345abc
- 23455abc
- 3456abc
- 456abc
- 56abc

- 6abc
- abc

In this example, replace ".*abc" with "abc" to prevent excessive use of resources.

Logical operators

EXPRESSION	DESCRIPTION
RS	R followed by S (concatenation)
R|S	Either R or S
(R)	Grouping R
.REG.	Indicates the following operand is a regular expression
.WILD.	Compares the operands, which follow it with wildcard comparison
.NOT.	Inverts the logic meaning
.AND.	Logical AND Both operands must appear in the entity to trigger the expression.
.OR.	Logical OR At least one of the operands must appear in the entity to trigger the expression.

R and S are regular expressions.

Shorthand and meta-symbol

Trend Micro Email Security provides the following shorthand for writing complicated regular expressions. Trend Micro Email Security will pre-process expressions and translate the shorthand into regular expressions.

For example, {D}+ would be translated to [0-9]+. If a shorthand expression is enclosed in brackets (example: {}) or double-quotes, then Trend Micro Email Security will not translate that shorthand expression to a regular expression.

SHORTHAND	DESCRIPTION
{D}	[0-9]
{L}	[A-Za-z]
{SP}	[(),;\.\\<>@\[\]:]
{NUMBER}	[0-9]+
{WORD}	[A-Za-z]+
{CR}	\r
{LF}	\n
{LWSP}	[\t]
{CRLF}	(\r\n)
{WSP}	[\t\f]+
{ALLC}	.

Trend Micro Email Security also provides the following meta-symbols. The difference between shorthand and meta-symbols is that meta-symbols can be within a bracket expression.

META-SYMBOL	DESCRIPTION
\s	[[:space:]]
\S	[^[:space:]]
\d	[[:digit:]]
\D	[^[:digit:]]
\w	[_[:alnum:]]
\W	[^_[:alnum:]]

Using keyword expressions

You can select existing keyword expressions from the list of those available. New keyword expressions can be defined and saved, either from scratch or by copying and editing an existing expression.

Procedure

1. Create or edit a content filtering policy.
2. Click the **Scanning Criteria** tab.
3. Select **Advanced** and click **keyword expressions** for each condition.
4. Select an existing keyword expression from the **Available** field.
5. Click the move button (**Add>**) to move the selected keyword expression to the **Selected** field.

   Note

   You can also add, edit, copy, or delete keyword expressions.

6. Repeat until you have moved all the keyword expressions you want to apply.

Adding keyword expressions

New keyword expressions can be defined and saved, and then applied to a policy rule.

Procedure

1. Go to **Administration** > **Policy Objects** > **Keywords and Expressions**.
2. Click **Add**.
3. Type a name for the list of keyword expressions.
4. Next to **Match**, select one of the following that specifies when Trend Micro Email Security takes action:

- Select **Any specified** to match keywords based on a logical OR.
- Select **All specified** to match keywords based on a logical AND.
- Select **Not the specified** to apply the policy rule to messages that do not contain the keywords.
- Select **Only when combined score reaches threshold** to apply the policy rule to messages that contains one or more keywords whose combined score reaches a threshold.

  Next to **Total message score to trigger action**, specify a number that represents the maximum score for allowed keyword expressions. When you add an expression, you can set a value for `Score`.

5. Create keyword expressions for the list.
   a. Click **Add**.
   b. Specify a keyword expression, set whether it is case sensitive, specify a description for the added keyword expression, and click **Save**.
   c. In the **Test Area** section, test the keyword expression against actual data.

      For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.
   d. Click **Save** if you are satisfied with the result.
6. Click **Save**.

Editing keyword expressions

Existing keyword expressions can be modified, or can be copied with a new name.

Procedure

1. Go to **Administration** > **Policy Objects** > **Keywords and Expressions**.
2. Click the name of a keyword expression list.
3. Edit the keyword expression information as required.
4. Click **Save**.

Managing notifications

You can use **Notifications** screen to manage notifications in Trend Micro Email Security.

For information on using and configuring notifications, see *About the send notification action on page 6-76*.

TABLE 10-6. Notifications Screen

TASKS	STEPS
Adding a Notification **Tip** Often a new notification will be very similar to one you already have. In that case, it is usually easier to copy the notification and edit it rather than create a new notification from scratch.	Click **Add**. 1. Provide the following information: • **Name**: A name for the notification email message. • **From**: The email addresses that you want to use to send notifications message from. • **To**: The recipient email address. • **Subject**: The notification email message subject. You can use tokens to include variables in the subject. For details, see *Tokens on page 6-70*. • **Body** (optional): The email notification message body. You can use tokens to include variables. For details, see *Tokens on page 6-70*. a. When using the token %DATE&TIME%, customize the time zone by selecting **Customize time zone for %DATE&TIME%** and selecting a time zone. By default, the time zone UTC+0 is used. Optionally select **Display UTC offset** if you want to include the UTC offset (such as UTC+0800) to the end of the date and time. b. Define the email body content in the HTML format by selecting a predefined style or custom style and specifying the body content. Three types of predefined style are available for use, **Informational**, **Suspicious**, or **Dangerous**. c. Define the email body content in plain text. If there is any hypertext in plain text, type the target URL next to the hypertext for recipients to know the destination address to access. • **Attachment** (optional): Select the **Attach the original message** check box and specify when to attach the original message in the notification. If the message content was altered due to the policy actions you

Tasks	Steps
	configured, Trend Micro Email Security attaches the message that has been processed rather than the original message. 2. Click **Save**.
Copying Notifications	In the **Notifications** list, select the notification to copy. Click **Copy**.
Editing Notifications	In the **Notifications** list, click the name of the notification you want to edit and follow the instructions in **Adding a Notification** procedure in this table.
Deleting Notifications	In the **Notifications** list, select the notifications to delete. Click **Delete**, and click **OK** to confirm.

Managing stamps

Trend Micro Email Security supports both HTML stamps and plain text stamps.

You can use **Stamps** screen to manage stamps in Trend Micro Email Security.

For information on inserting and configuring stamps, see *Inserting a stamp on page 6-67*.

TABLE 10-7. Stamps Screen

TASKS	STEPS
Adding a Stamp **Tip** Often a new stamp will be very similar to one you already have. In that case, it is usually easier to copy the stamp and edit it rather than create a new stamp from scratch.	Click **Add**. 1. Provide the following information: • **Name**: A name for the stamp. Optionally select **Do not stamp message formats that might become corrupted or unreadable, such as digitally signed and Outlook TNEF.** if necessary. • **Insert at**: Select whether you want to insert the stamp at the beginning or at the end of the message body. • **HTML**: Specify the HTML content for the stamp as desired. a. Select a style type: • **Predefined style**: Trend Micro Email Security provides a predefined style for HTML stamps that indicate **Information**, **Suspicious**, or **Dangerous** risk level. Select a risk level and modify the HTML content with the rich text editor. Trend Micro Email Security offers a preview of the stamp and automatically generates a plain text stamp with same content in real time. • **Customized style**: Trend Micro Email Security allows you to specify HTML stamp content and plain text stamp content separately. b. Edit the stamp content. Optionally include variables in your stamps by using the tokens listed in *Tokens on page 6-70*. When you use the token %DATE&TIME%, select **Customize time zone for %DATE&TIME%** and select a time zone. By default, the time zone UTC+0 is used.

Tasks	Steps
	Optionally select **Display UTC offset** if you want to include the UTC offset (such as UTC+0800) to the end of the date and time. **Note** When a message triggers the policy rule, the HTML stamp will be inserted into **HTML** content of the message, and the plain text stamp will be inserted into **Plain text** content of the message. 2. Click **Save**.
Copying Stamps	In the **Stamps** list, select the stamp to copy. Click **Copy**.
Editing Stamps	In the **Stamps** list, click the name of the stamp you want to edit and follow the instructions in **Adding a Stamp** procedure in this table.
Deleting Stamps	In the **Stamps** list, select the stamps to delete. Click **Delete**, and click **OK** to confirm.

Administrator management

Trend Micro Email Security allows you to perform the following administrator management tasks:

- Creating and managing administrator subaccounts and superadmin accounts
- Configuring the way that administrator subaccounts and superadmin accounts access the administrator console

Account management

Use the **Administration** > **Administrator Management** > **Account Management** screen to search for administrator subaccounts and superadmin accounts under your control and perform actions on behalf of those accounts.

Both administrator subaccounts and superadmin accounts are local accounts, which can be created by an administrator account (Trend Micro Business Account) and have the administrator account privileges. The differences are as follows:

- A subaccount can perform privileged operations only within managed domains. Even a subaccount created with **Full Control** permission over all features may still not be able to perform certain operations. For example, a subaccount with **Full Control** permission over domains cannot add or delete domains.
- A superadmin account is created to ease the administrative burden of the Business Account. The superadmin account owns all the permissions of the Business Account, including creating subaccounts or superadmin accounts. The superadmin account can perform operations in all domains added to your organization and has unrestricted access to all features on the administrator console.

For more information about the accessible features of the local accounts, see *Accessible features of the local accounts on page 10-30*.

After clicking **Assume Control** beside a local account in the list, you will be able to perform privileged operations on behalf of the account.

To stop acting on behalf of the local account, click **Release** in the title bar area.

Accessible features of the local accounts

The following table lists the accessible features of administrator subaccounts with **Full Control** permission and superadmin accounts on the administrator console.

TABLE 10-8. Accessible features of administrator subaccounts with Full Control permission and superadmin accounts

FEATURE			SUBACCOUNT WITH FULL CONTROL PERMISSION	SUPERADMIN ACCOUNT
Dashboard			All	All
Domains			Cannot add or delete domains	All
Security Policies	Inbound Protection	Connection Filtering	All	All
		Domain-based Authentication	Cannot edit default policy rules	All
		Virus Scan	All	All
		Spam Filtering	All	All
		Correlated Intelligence	All	All
		Content Filtering	All	All
		Data Loss Prevention (DLP)	All	All
	Outbound Protection		All	All
	Policy Objects		All	All
Quarantine		Query	All	All
		End User Console Settings	All	All
		Digest Settings	Cannot edit default digest rules	All
Logs			Can only query audit logs of themselves	All

Feature			Subaccount with Full Control Permission	Superadmin Account
Reports			All	All
Administration	Email Continuity		All	All
	Administrator Management		Cannot see this menu	All
	End User Management	Passwords	All	All
		Managed Accounts	All	All
		Logon Methods	Cannot see the **Single sign-on** toggle button	All
	Logon Access Control		Cannot see this menu	All
	Directory Management		All	All
	Co-Branding		All	All
	Service Integration	API Access	All	All
		Log Retrieval	All	All
		Apex Central	All	All
		Remote Manager	Cannot integrate with Remote Manager	All
	License Information		All	All
	IMSS/IMSVA Migration Tool		Cannot see this menu	All
Help			All	All
REST API Access			All	All

Feature	Subaccount with Full Control Permission	Superadmin Account
Administrator Profile Verification	Cannot see the notice of resending the email message for verification	Cannot see the notice of resending the email message for verification
Change Password	All	All
Release Control	All	All
Log Off	All	All
Two-Factor Authentication	All	All
Logon to the Administrator Console through SSO	All	All

Adding and configuring a subaccount

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Click **Add Subaccount**.

   The **Add Subaccount** screen appears.
3. Configure the following information on the screen:
   - **Subaccount Basic Information**: type the account name and email address.

Note

If you want to enable single sign-on for this subaccount, the email address specified here will be used to map to its equivalent from your identity provider to verify the identity of this subaccount. Therefore, set up the subaccount with the email address used by your identity provider.

- **Select Permission Types**: select permissions from the **Predefined Permission Types** drop-down list, or configure permissions for each of the feature manually.

Note

- When you assign the read-only quarantine permissions, you can control whether to include the permissions for viewing the quarantined message details and downloading quarantined messages. By default, these permissions are included.
- A subaccount has no permission to add or delete domains, even if that subaccount has **Full Control** permission over the domains. Only the Business Account and superadmin accounts can perform such operations.

- **Select Domains**: select domains that the account can manage.
  - **My organization**: select the entire organization for the subaccount to manage.

Important

Selecting **My organization** does not grant the subaccount permission to add or delete domains. It just enables the subaccount to use organization-level features such as creating an organization-level policy rule.

If **My organization** is selected, the subaccount can manage the new domains added by the Business Account in the future.

- **Specify**: select one or more domains for the subaccount to manage.

4. Click **Save**.

   Trend Micro Email Security sends an email message with logon information to the newly created account owner.

Note

The **Reset Password** button resets the password and sends a new notification message to the account owner.

Adding and configuring a superadmin account

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Click **Add Superadmin Account**.

   The **Add Superadmin Account** screen appears.
3. Type the account name and email address.

Note

If you want to enable single sign-on for this superadmin account, the email address specified here will be used to map to its equivalent from your identity provider to verify the identity of this superadmin account. Therefore, set up the superadmin account with the email address used by your identity provider.

4. Click **Save**.

   Trend Micro Email Security sends an email message with logon information to the newly created account owner.

Note

The **Reset Password** button resets the password and sends a new notification message to the account owner.

Editing a subaccount

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Click name of the subaccount that you want to edit.

   The **Edit Subaccount** screen appears.
3. Modify the following information on the screen as required:
   - **Subaccount Basic Information**: modify the email address if necessary.

     Note

     The account name cannot be modified.
   - **Select Permission Types**: select a predefined permission from the **Predefined Permission Types** drop-down list, or configure permissions for each of the feature manually.

     Note that a subaccount has no permission to add or delete domains, even if that subaccount has **Full Control** permission over the domains. Only the Business Account can perform such operations.
   - **Select Domains**: select the domains that the account can manage.
     - **My organization**: select the entire organization for the subaccount to manage.

Important

Selecting **My organization** does not grant the subaccount permission to add or delete domains. It just enables the subaccount to use organization-level features such as creating an organization-level policy rule.

If **My organization** is selected, the subaccount can manage the new domains added by the Business Account in the future.

- **Specify**: select one or more domains for the subaccount to manage.

4. Click **OK**.

Editing a superadmin account

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Click name of the superadmin account that you want to edit.

   The **Edit Superadmin Account** screen appears.
3. Modify the email address as required.

Note

The account name cannot be modified.

4. Click **OK**.

Deleting subaccounts or superadmin accounts

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Select the subaccounts or superadmin accounts that you want to delete, and then click **Delete**.
3. Click **OK** in the confirmation dialog box.

Changing the password of a subaccount or superadmin account

Note

If you have a Business Account on the Customer Licensing Portal or Licensing Management Platform, sign in to your account and follow the instructions provided there to change your password. Trend Micro recommends changing your password regularly.

The password cannot be changed for a disabled subaccount or superadmin account.

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Select the subaccount or superadmin account for which you want to change the password, and then click **Reset Password**.

   Trend Micro Email Security sends an email with a password reset link to the account owner.

Enabling or disabling a subaccount or superadmin account

Procedure

1. Go to **Administration** > **Administrator Management** > **Account Management**.
2. Click (enabled) or (disabled) to toggle the status of a subaccount or superadmin account, and then click **OK** in the confirmation dialog box.

Logon methods

Trend Micro Email Security allows you to control the way that administrator subaccounts and superadmin accounts access the administrator console.

On the **Logon Methods** screen, you can enable or disable the following logon methods:

- **Local Account Logon**

  If this method is enabled, subaccounts and superadmin accounts can log on to the administrator console with their user name and password. Enforcing two-factor authentication adds an extra layer of security to the accounts.

- **Single Sign-On**

  Once you enable single sign-on (SSO) and complete required settings, subaccounts and superadmin accounts can log on to the administrator console through SSO with their existing identity provider credentials. You can create multiple SSO profiles so that different accounts can log on to the administrator console from different identity provider servers through SSO.

  Trend Micro Email Security currently supports the following identity providers for SSO:

  - Microsoft Active Directory Federation Services (AD FS)
  - Microsoft Entra ID

- Okta

Configuring local account logon

Procedure

1. Go to **Administration** > **Administrator Management** > **Logon Methods**.
2. In the **Local Account Logon** section, configure the settings for local account logon.
   a. Click the toggle button to enable local account logon.

      This allows administrator subaccounts and superadmin accounts to log on to the administrator console with their user name and password.

   b. Click the toggle button to enforce two-factor authentication.

      Two-factor authentication adds an extra layer of security to the accounts.

      After enforcing two-factor authentication, the accounts must provide the following authentication credentials each time they log on to the administrator console:

      - Local account and password
      - A one-time password generated by the Google Authenticator app

Setting up two-factor authentication

Note

If your administrator has enforced two-factor authentication, it means that two-factor authentication must be used every time you log on to the administrator console and it cannot be disabled. Complete the following steps to set up two-factor authentication before you can access the administrator console.

The Trend Micro Email Security administrator console provides two-factor authentication support. Two-factor authentication provides an added layer of security for the local accounts and prevents unauthorized access to your Trend Micro Email Security administrator console, even if your password is stolen.

After enabling two-factor authentication, local accounts need to provide the following authentication credentials each time they sign in:

- Local account and password
- A one-time password generated by the Google Authenticator app

This section describes how to set up two-factor authentication with a local account.

Procedure

1. Log on to the Trend Micro Email Security administrator console with your local account and password.
2. Click your account name in the top right corner and choose **Two-Factor Authentication** to open the setup wizard.
3. Set up two-factor authentication in the wizard.
   a. Click **Get Started**.
   b. Verify your email address and click **Next**.
   c. Obtain the verification code from the notification sent to your email address.

      Note

      If you did not get the verification code, wait for at least 3 minutes before clicking **Resend Code**.

   d. Type the verification code and click **Next**.
   e. Follow the instructions to set up two-factor authentication.

1. Download Google Authenticator either from Apple's App Store or Google Play and install it on your mobile phone.
2. Add your Trend Micro Email Security account to Google Authenticator by scanning the QR code.
3. Provide the 6-digit code generated by Google Authenticator to verify that your authentication works properly.

f. Click **Finish**.

Your account will be presented with the two-factor authentication when they try to log on.

If you want to disable two-factor authentication, click **Disable** on the **Two-Factor Authentication** screen. If your administrator has enforced two-factor authentication, click **Reset** to reset two-factor authentication if necessary.

Configuring single sign-on

Before specifying single sign-on (SSO) settings on the administrator console, configure the identity provider you choose for SSO, that is, AD FS 4.0, Microsoft Entra ID or Okta:

- *Configuring Active Directory Federation Services on page 10-44*
- *Configuring Microsoft ENTRA ID on page 10-48*
- *Configuring Okta on page 10-51*

Note

Gather required settings from your identity provider before setting up the administrator console.

Procedure

1. Go to **Administration** > **Administrator Management** > **Logon Methods**.
2. In the **Single Sign-On** section, click the toggle button to enable SSO.

3. Click **Add** to create an SSO profile.
4. Configure general information for SSO.
   a. Specify an SSO profile name.
   b. Specify an identifier that is globally unique at your site.

      The administrator console URL is generated.

      If you have to change the unique identifier due to conflict with another identifier, make sure you also change it in your identity provider configuration.
5. Select the accounts to which the current profile applies:
   - **All accounts**: applies this profile to all accounts.

     Note

     You can create only one profile that is applied to all accounts.
   - **Specified accounts**: applies this profile to specified accounts.

     Select accounts from the **Available** pane and click **Add >** to add them to the **Selected** pane.
6. Complete identity provider configuration for SSO.
   a. Select your identity provider from the **Identity provider** drop-down list.
   b. Specify the logon and logoff URLs for your identity provider.

      Note

      Use the logon URL collected from AD FS, Microsoft Entra ID or Okta configurations.

      The logoff URL logs you off and also terminates the current identity provider logon session.
   c. (For Okta only) Click **Download Logoff Certificate** to obtain the certificate file to upload to your federation server.

d. Locate the certificate file you downloaded from AD FS, Microsoft Entra ID or Okta configurations and upload it for signature validation.

e. Specify the identity claim type based on the claim you configured for AD FS, Microsoft Entra ID or Okta. For example, if you use `email` as the claim name, type `email`.

7. Click **Save** to save the profile.

8. Click **Save** to save SSO settings.

   Once you have completed the configuration, log on with an account using the administrator console URL generated in Step 4 to initiate SSO from the identity provider to the Trend Micro Email Security administrator console. The identity claim type specified in Step 6 is used to get the mapping claim value from your identity provider. In this case, Trend Micro Email Security obtains the email address of the logon account and checks if it matches the account email address you set before. If they are matched, you will be successfully logged on to the administrator console with the account.

Configuring Active Directory Federation Services

Active Directory Federation Services (AD FS) provides support for claims-aware identity solutions that involve Windows Server and Active Directory technology. AD FS supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

This section uses Windows 2016 as an example to describe how to configure AD FS as a SAML server to work with Trend Micro Email Security. Make sure you have installed AD FS successfully.

Procedure

1. Go to **Start** > **All Programs** > **Windows Administrative Tools** > **AD FS Management**.

2. On the AD FS management console, go to **AD FS**, right-click **Relying Party Trusts**, and then choose **Add Relying Party Trust**.

3. Complete settings for each screen in the Add Relying Party Trust wizard.

   a. On the **Welcome** screen, select **Claims aware** and click **Start**.

   b. On the **Select Data Source** screen, select **Enter data about the relying party manually** and click **Next**.

   c. On the **Specify Display Name** screen, specify a display name, for example, `Trend Micro Email Security Administrator Console`, and click **Next**.

   d. On the **Configure Certificate** screen, click **Next**.

   Note

   No encryption certificate is required, and HTTPS will be used for communication between Trend Micro Email Security and federation servers.

   e. On the **Configure URL** screen, select **Enable support for the SAML 2.0 WebSSO protocol**, type the relying party SAML 2.0 SSO service URL, and then click **Next**.

Note

Specify the SAML 2.0 SSO service URL for your region as follows:

`https://ui.<domain_name>/uiserver/subaccount/ssoAssert?cmpID=<unique_identifier>`

In the preceding and following URLs:

- Replace `<unique_identifier>` with a unique identifier. Record the unique identifier, which will be used when you create an SSO profile on the Trend Micro Email Security administrator console.
- Replace `<domain_name>` with any of the following based on your location:
  - North America, Latin America and Asia Pacific:

    `tmes.trendmicro.com`
  - Europe and Africa:

    `tmes.trendmicro.eu`
  - Australia and New Zealand:

    `tmes-anz.trendmicro.com`
  - Japan:

    `tmems-jp.trendmicro.com`
  - Singapore:

    `tmes-sg.trendmicro.com`
  - India:

    `tmes-in.trendmicro.com`
  - Middle East (UAE):

    `tmes-uae.trendmicro.com`

f. On the **Configure Identifiers** screen, type the identifier for the relying party trust, click **Add**, and then click **Next**.

Note

Specify the identifier for the relying party trust for your region as follows:

`https://ui.<domain_name>/uiserver/subaccount/ssoLogin`

---

g. On the **Choose Access Control Policy** screen, choose an access control policy and click **Next**.

h. Continue clicking **Next** in the wizard and finally click **Close**.

4. From the **Edit Claim Issuance Policy for Trend Micro Email Security Administrator Console** dialog box, click **Add Rule** in the **Issuance Transform Rules** tab.

5. Complete settings for each screen in the Add Transform Claim Rule wizard.

a. On the **Select Rule Template** screen, select **Send LDAP Attributes as Claims** for **Claim rule template** and click **Next**.

b. On the **Configure Rule** screen, specify a claim rule name and select **Active Directory** for **Attribute store**.

c. Select LDAP attributes and specify an outgoing claim type for each attribute. For example, select **E-Mail-Addresses** and type `email` as the outgoing claim type.

Important

When configuring the identity claim type for an SSO profile on Trend Micro Email Security, make sure you use the claim type specified here.

---

d. Click **Finish**.

e. Click **OK** to close the wizard.

6. From **AD FS** > **Relying Party Trust**, double-click the relying party trust file you created earlier.
   a. From the **Test Properties** dialog box, click the **Advanced** tab.
   b. Select **SHA1** from the **Secure hash algorithm** drop-down list and click **OK**.
7. Collect the single sign-on logon and logoff URLs and obtain a certificate for signature validation from AD FS.
   a. On the AD FS management console, go to **AD FS** > **Service** > **Endpoints**.
   b. Look for the **SAML 2.0/WS-Federation** type endpoint and collect the URL path.

      Note

      The URL path will be used when you configure logon and logoff URLs on Trend Micro Email Security.

      - Logon URL: <adfs_domain_name>/adfs/ls/
      - Logoff URL: <adfs_domain_name>/adfs/ls/?wa=wsignout1.0

   c. Go to **AD FS** > **Service** > **Certificates**.
   d. Look for the **Token-signing** certificate, right-click it, and then select **View Certificate**.
   e. Click the **Details** tab and click **Copy to File**.
   f. Using the Certificate export wizard, select **Base-64 Encoded X.509 (.CER)**.
   g. Assign a name to the file to complete the export of the certificate into a file.

Configuring Microsoft ENTRA ID

Microsoft Entra ID is Microsoft's multi-tenant cloud based directory and identity management service.

Make sure you have a valid subscription in Microsoft Entra ID that handles the sign-in process and eventually provides the authentication credentials of local accounts to the administrator console.

Procedure

1. On the Microsoft Entra ID management portal, select an active directory that you want to implement SSO.
2. Click **Enterprise applications** in the navigation area on the left and click **New application**.
3. On the **Browse Microsoft Entra ID Gallery (Preview)** screen, click **Create your own application**.
4. On the **Create your own application** panel that appears on the right, specify a name for your application, for example, `Trend Micro Email Security Administrator Console`, and click **Create**.
5. Under **Getting Started** in the overview of your application, click **1. Assign users and groups**, click **Add user/group**, select a specific user or group for this application and click **Assign**.
6. In the navigation area of your application, click **Single sign-on**.
7. Click **SAML** to configure the connection from your application to Microsoft Entra ID using the SAML protocol.
   a. Under **Basic SAML Configuration**, click **Edit**, specify the identifier and reply URL, and click **Save**.

Note

Specify the identifier for your region as follows:

`https://ui.<domain_name>/uiserver/subaccount/ssoLogin`

Specify the reply URL for your region as follows:

`https://ui.<domain_name>/uiserver/subaccount/ssoAssert?cmpID=<unique_identifier>`

In the preceding and following URLs:

- Replace *<unique_identifier>* with a unique identifier. Record the unique identifier, which will be used when you create an SSO profile on the Trend Micro Email Security administrator console.
- Replace *<domain_name>* with any of the following based on your location:
  - North America, Latin America and Asia Pacific:

    `tmes.trendmicro.com`
  - Europe and Africa:

    `tmes.trendmicro.eu`
  - Australia and New Zealand:

    `tmes-anz.trendmicro.com`
  - Japan:

    `tmems-jp.trendmicro.com`
  - Singapore:

    `tmes-sg.trendmicro.com`
  - India:

    `tmes-in.trendmicro.com`
  - Middle East (UAE):

    `tmes-uae.trendmicro.com`

Click **No, I'll test later** when you are prompted to choose whether to test single sign-on with `Trend Micro Email Security Administrator Console`. You are advised to perform a test after all SSO settings are complete.

b. Under **User Attributes & Claims**, click **Edit**, and specify the identity claim.

User attributes and claims are used to get the email addresses of logon accounts to authenticate their identity. By default, the source attribute **user.mail** is preconfigured to get the email addresses. If the email addresses in your organization are defined by another source attribute, do the following to add a new claim name:

Click **Add new claim**. On the **Manage claim** screen, specify the claim name, leave **Namespace** empty, select **Attribute** as **Source**, select a value from the **Source attribute** drop-down list, and click **Save**.

Important

When configuring the identity claim type for an SSO profile on Trend Micro Email Security, make sure you use the claim name specified here.

c. Under **SAML Signing Certificate**, click **Edit**, specify an email address for **Notification Email Addresses**, and click **Save**. Click **Download** next to **Certificate (Base64)** to download a certificate file for Microsoft Entra ID signature validation on Trend Micro Email Security.

d. Under **Set up Trend Micro Email Security Administrator Console**, record the login and logout URLs.

Configuring Okta

This section describes how to add Trend Micro Email Security as a new application and configure SSO settings on your Okta Admin Console.

Procedure

1. Navigate to the Admin Console by clicking **Admin** in the upper-right corner.

   Note

   If you are in the Developer Console, click **< > Developer Console** in the upper-left corner and then click **Classic UI** to switch over to the Admin Console.

2. In the Admin Console, go to **Applications** > **Applications**.
3. Click **Add Application**, and then click **Create New App**.

   The **Create a New Application Integration** screen appears.
4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**, and then click **Create**.
5. On the **General Settings** screen, type a name for Trend Micro Email Security in **App name**, for example, `Trend Micro Email Security Administrator Console`, and click **Next**.
6. On the **Configure SAML** screen, specify the following:
   a. Type `https://ui.<domain_name>/uiserver/subaccount/ssoAssert?cmpID=<unique_identifier>` in **Single sign on URL** based on your serving site.

Note

In the preceding and following URLs:

- Replace `<unique_identifier>` with a unique identifier. Record the unique identifier, which will be used when you create an SSO profile on the Trend Micro Email Security administrator console.
- Replace `<domain_name>` with any of the following based on your location:
  - North America, Latin America and Asia Pacific:

    `tmes.trendmicro.com`
  - Europe and Africa:

    `tmes.trendmicro.eu`
  - Australia and New Zealand:

    `tmes-anz.trendmicro.com`
  - Japan:

    `tmems-jp.trendmicro.com`
  - Singapore:

    `tmes-sg.trendmicro.com`
  - India:

    `tmes-in.trendmicro.com`
  - Middle East (UAE):

    `tmes-uae.trendmicro.com`

b. Select **Use this for Recipient URL and Destination URL**.

c. Type `https://ui.<domain_name>/uiserver/subaccount/ssoLogin` in **Audience URI (SP Entity ID)**.

d. Select **EmailAddress** in **Name ID format**.

e. Select **Okta username** in **Application username**.

f. (Optional) Click **Show Advanced Settings**, specify the following:

This step is required only if you want to configure a logoff URL on the Trend Micro Email Security administrator console. The logoff URL is used to log you off and also terminate the current identity provider logon session.

1. Next to **Enable Single Logout**, select the **Allow application to initiate Single Logout** check box.
2. Type `https://ui.<domain_name>/uiserver/subaccount/sloAssert?cmpID=<unique_identifier>` in **Single Logout URL**.
3. Type `https://ui.<domain_name>/uiserver/subaccount/ssoLogout` in **SP Issuer**.
4. Upload the logoff certificate in the **Signature Certificate** area.

   You need to download the logoff certificate from the Trend Micro Email Security administrator console in advance. Go to **Administration** > **Administrator Management** > **Logon Methods**. Click **Add** in the **Single Sign-on** section. On the pop-up screen, locate the **Identity Provider Configuration** section, select **Okta** as **Identity provider** and click **Download Logoff Certificate** to download the certificate file.
5. Keep the default values for other settings.

g. Under **ATTRIBUTE STATEMENTS (OPTIONAL)**, specify `email` in **Name**, and select **Unspecified** in **Name format** and **user.email** in **Value**.

Important

When configuring the identity claim type for an SSO profile on Trend Micro Email Security, make sure you use the attribute name specified here.

h. Click **Next**.

7. On the **Feedback** screen, click **I'm an Okta customer adding an internal app**, and then click **Finish**.

   The **Sign On** tab of your newly created Trend Micro Email Security application appears.

8. Click **View Setup Instructions**, and record the URL in **Identity Provider Single Sign-On URL** and download the certificate in **X.509 Certificate**.

End user management

Trend Micro Email Security allows you to perform the following management tasks for end user accounts on Trend Micro Email Security End User Console:

- Managing local end user accounts
- Managing end user account management relationships
- Configuring the way that end users access the End User Console

Local accounts

In addition to SSO using existing credentials, an local account is another way for end users to access the End User Console. On **Administration** > **End User Management** > **Local Accounts** screen, Trend Micro Email Security allows you to manage the local accounts of end users that belong to the managed domains. The local accounts can be registered by either administrators or end users.

TABLE 10-9. Local Accounts Screen

TASKS	STEPS
Adding a local account	**Note** Before adding local accounts for end users, make sure you have enabled local account logon for end users. For details, see *Configuring local account logon on page 10-64*. 1. Type an email address and click **Add**. **Note** Make sure the email address meets the following requirements: • Belongs to one of the managed domains • Is a valid recipient of a managed domain when the recipient filter is enabled for the domain The email address appears in the local account list below. The email address will receive a password reset message for the local account. After the end user resets the password, they can use the account to log on to the End User Console.
Deleting local accounts	1. Select one or multiple local accounts and click **Delete**. **Note** To delete a primary account that manages other accounts, remove the account management relationships first. For details, see *Removing end user managed accounts on page 10-62*. 2. On the **Delete End User** screen, click **OK**. The local accounts are removed from the local account lists and can no longer log on to the End User Console.

Tasks	Steps
Importing local accounts	**Note** Before adding local accounts for end users, make sure you have enabled local account logon for end users. For details, see *Configuring local account logon on page 10-64*. 1. Click **Import**. 2. (Optional) Click **Download sample file** to download the sample file for reference or import. 3. On the **Import End Users** screen, click **Choose File...** and select a CSV file that contains the end user accounts to import. You can click **Download sample file** to download a sample CSV file for reference or use it to import accounts. Make sure the CSV file meet the following requirements: • The file size does not exceed 1 MB. • The email addresses belong to the managed domains. • The email addresses are the valid recipients of a managed domain when the recipient filter is enabled for the domain. 4. Click **Preview** to preview the import result. 5. Click **Import**. The email addresses imported successfully appear in the local account list below. The email addresses will receive a password reset message for the local accounts. After the end users reset the password, they can use the accounts to log on to the End User Console.
Exporting local accounts	1. Click **Export All**. All local accounts are exported to a CSV file.

Tasks	Steps
Enabling or disabling local accounts	1. Click (enabled) or (disabled) to toggle the status of a local account, and then click **OK** in the confirmation dialog box. **Note** You cannot enable or disable managed accounts. Enabled accounts can log on to the End User Console while disabled accounts cannot.

Adding a local account

Note

Before adding local accounts for end users, make sure you have enabled local account logon for end users. For details, see *Configuring local account logon on page 10-64*.

Procedure

1. Go to **Administration** > **End User Management** > **Local Accounts**.
2. Type an email address and click **Add**.

   Make sure the email address meets the following requirements:

   - Belongs to one of the managed domains
   - Is a valid recipient of a managed domain when the recipient filter is enabled for the domain

   The email address appears in the local account list below.

   The email address will receive a password reset message for the local account. After the end user resets the password, they can use the account to log on to the End User Console.

Deleting local accounts

Procedure

1. Go to **Administration** > **End User Management** > **Local Accounts**.
2. Select one or multiple local accounts and click **Delete**.

   Note

   To delete a primary account that manages other accounts, remove the account management relationships first. For details, see *Removing end user managed accounts on page 10-62*.

3. On the **Delete End User** screen, click **OK**.

   The local accounts are removed from the local account lists and can no longer log on to the End User Console.

Importing local accounts

Note

Before adding local accounts for end users, make sure you have enabled local account logon for end users. For details, see *Configuring local account logon on page 10-64*.

Procedure

1. Go to **Administration** > **End User Management** > **Local Accounts**.
2. Click **Import**.
3. (Optional) Click **Download sample file** to download the sample file for reference or import.
4. On the **Import End Users** screen, click **Choose File...** and select a CSV file that contains the end user accounts to import.

You can click **Download sample file** to download a sample CSV file for reference or use it to import accounts.

Make sure the CSV file meet the following requirements:

- The file size does not exceed 1 MB.
- The email addresses belong to the managed domains.
- The email addresses are the valid recipients of a managed domain when the recipient filter is enabled for the domain.

5. Click **Preview** to preview the import result.
6. Click **Import**.

   The email addresses imported successfully appear in the local account list below.

   The email addresses will receive a password reset message for the local accounts. After the end users reset the password, they can use the accounts to log on to the End User Console.

Exporting local accounts

Procedure

1. Go to **Administration** > **End User Management** > **Local Accounts**.
2. Click **Export All**.

   All local accounts are exported to a CSV file.

Enabling or disabling local accounts

Procedure

1. Go to **Administration** > **End User Management** > **Local Accounts**.
2. Click ✓ (enabled) or ⊗ (disabled) to toggle the status of a local account, and then click **OK** in the confirmation dialog box.

Note

You cannot enable or disable managed accounts.

Enabled accounts can log on to the End User Console while disabled accounts cannot.

Managed accounts

End users can use one End User Console local account to manage multiple local accounts. After an account becomes the managing account, namely the primary account, they can view the quarantined messages and set the Approved Senders associated with that account.

After logging in to the End User console with a primary account, end users can specify one of their managed accounts or **All managed accounts** at the top of the screen to view Quarantined messages and set Approved Senders for the specified account or accounts.

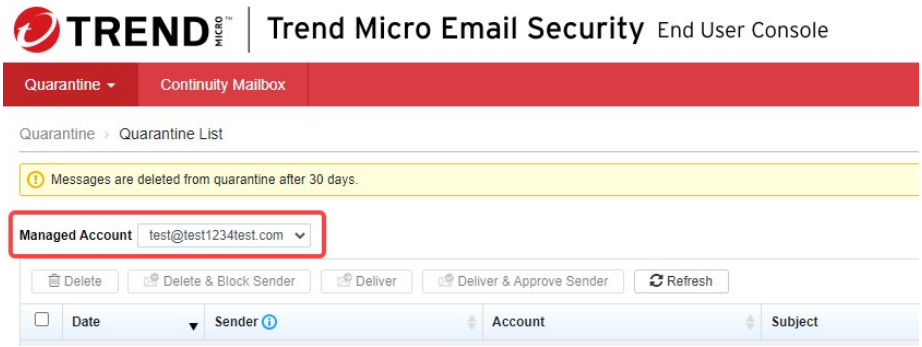


FIGURE 10-1. Example of the Managed Account Control

After an end user begins managing an account, that managed account will be unable to log on to the End User Console. The managed account will be able to log on again only if the account management relationship is removed. To allow the account to log on again, the primary account can remove the managed account from the **Managed Accounts** screen of the End User Console.

Adding a managed account does not change the credentials for that account. Disabling the feature does not change the account management relationship of accounts that end users have already added.

End users can always remove accounts from their list of managed accounts. However, end users can only add management of accounts under the following conditions:

- The account is a registered End User Console account.
- The account is not currently a managed account of another End User Console account.
- The end user is able to open the confirmation email message sent to the account address.
- The end user has the End User Console password for the account.

Removing end user managed accounts

The primary account can remove the managed account from the **Managed Accounts** screen of the End User Console.

To remove an account management relationship using the Trend Micro Email Security administrator console, use the following procedure.

Procedure

1. Go to **Administration** > **End User Management** > **Managed Accounts**.
2. Select the primary account and managed account pair or pairs in the list.
3. Click **Remove**.

Logon methods

Trend Micro Email Security allows you to control the way that end users access the End User Console.

On the **Logon Methods** screen, you can enable or disable the following logon methods:

- **Local Account Logon**

  If this method is enabled, end users can log on to the End User Console with their user name and password of the local managed accounts they have registered on the End User Console. Enforcing two-factor authentication adds an extra layer of security to the end user accounts.

- **Single Sign-On**

  Once you enable single sign-on (SSO) and complete required settings, end users can log on to the End User Console through SSO with their existing identity provider credentials. You can create multiple SSO profiles so that different end users can log on to the End User Console from different identity provider servers through SSO.

  When creating an SSO profile, you need to specify the domains to which the profile applies. Assume that subaccount A manages domain A, B and C, subaccount B manages domain B and subaccount C manages domain C. The relationship between SSO profiles, managed domains and subaccount permissions are as follows:

SSO Profile	Managed Domains	Subaccount Permission
Profile 1	Domains A and B	• Subaccount A: read and edit • Subaccount B: read only • Subaccount C: cannot read, edit or delete
Profile 2	Domain C	• Subaccount A: read and edit • Subaccount B: cannot read, edit or delete • Subaccount C: read and edit

SSO Profile	Managed Domains	Subaccount Permission
Profile 3	All domains	• Subaccount A: read only • Subaccount B: read only • Subaccount C: read only

Trend Micro Email Security currently supports the following identity providers for SSO:

- Microsoft Active Directory Federation Services (AD FS)
- Microsoft Entra ID
- Okta

Configuring local account logon

Procedure

1. Go to **Administration** > **End User Management** > **Logon Methods**.
2. In the **Local Account Logon** section, configure the settings for local account logon.
   a. Click the toggle button to enable **Local Account Logon**.

      This allows end users to log on to the End User Console with their user name and password of the local managed accounts.

   b. Click the toggle button to enforce two-factor authentication.

      Two-factor authentication adds an extra layer of security to the end user accounts.

      After enforcing two-factor authentication, end user accounts must provide the following authentication credentials each time they log on to the End User Console:

      - Local account and password

- A one-time password generated by the Google Authenticator app

c. From the **Source of managed accounts** drop-down list, select the source of accounts to be managed when end users log on to the End User Console.

- **Aliases synchronized from directories**: If you select this option, the logon users will have all the aliases synchronized from LDAP directories as their managed accounts.
- **Manually added accounts**: If you select this option, the logon users will have all the accounts they added manually as their managed accounts.

Configuring single sign-on

Before specifying SSO settings on the administrator console, configure the identity provider you choose for single sign-on, that is, AD FS 4.0, Microsoft Entra ID or Okta:

- *Configuring Active Directory Federation Services on page 10-68*
- *Configuring Microsoft ENTRA ID on page 10-73*
- *Configuring Okta on page 10-77*

Note

Gather required settings from your identity provider before setting up the administrator console.

Procedure

1. Go to **Administration** > **End User Management** > **Logon Methods**.
2. In the **Single Sign-On** section, click the toggle button to enable SSO.
3. Click **Add** to create an SSO profile.
4. Configure general information for SSO.

a. Specify an SSO profile name.

b. Specify an identifier that is globally unique at your site.

The End User Console URL is generated.

If you have to change the unique identifier due to conflict with another identifier, make sure you also change it in your identity provider configuration.

5. Select the domains to which the current profile applies:

   - **All domains**: applies this profile to all domains.

     Note

     You can create only one profile that is applied to all domains.

   - **Specified domains**: applies this profile to specified domains.

     Select domains from the **Available** pane and click **Add >** to add them to the **Selected** pane.

6. Complete identity provider configuration for SSO.

   a. Select your identity provider from the **Identity provider** drop-down list.

   b. Specify the logon and logoff URLs for your identity provider.

   Note

   Use the logon URL collected from AD FS, Microsoft Entra ID or Okta configurations.

   The logoff URL logs you off and also terminates the current identity provider logon session.

   c. (For Okta only) Click **Download Logoff Certificate** to obtain the certificate file to upload to your federation server.

   d. (Optional) Enable signature validation.

Note

A signature is returned from the identity provider server during SSO. To avoid forgery logon by attackers, the signature must be checked against the certificate file you obtained from your identity provider.

1. Click the **Signature validation** toggle button.
2. Locate the certificate file you downloaded from AD FS, Microsoft Entra ID or Okta configurations and upload it for signature validation.

e. Specify the identity claim type based on the claim you configured for AD FS, Microsoft Entra ID or Okta. For example, if you use `email` as the claim name, type `email`.

f. (Optional) Enable SSO management by group.

Note

If you enable this function, only end users with valid email addresses in the specified group can be logged on to the End User Console through SSO:

1. Click the `Group allow list` toggle button.
2. Specify the group claim type based on the group claim you configured for AD FS, Microsoft Entra ID or Okta. For example, if you use `euc_group` as the group attribute name, type `euc_group`.
3. Specify group claim values based on the group claim you configured for AD FS, Microsoft Entra ID or Okta. If your identity provider is AD FS or Okta, type group names; if your identity provider is Microsoft Entra ID, type group IDs.

7. Click **Save** to save the profile.

8. Click **Save** to save SSO settings.

   Once you have completed the configuration, an end user can log on using the End User Console URL generated in Step 4 to initiate SSO from the identity provider to the End User Console. The identity claim type and group claim type specified in Step 6 are used to get the mapping claim values from your identity provider. In this case, Trend Micro Email Security obtains the email address and user group of the logon account to verify the identity of the end user. Once verified, the end user will be successfully logged on to the End User Console.

Configuring Active Directory Federation Services

Active Directory Federation Services (AD FS) provides support for claims-aware identity solutions that involve Windows Server and Active Directory technology. AD FS supports the WS-Trust, WS-Federation, and Security Assertion Markup Language (SAML) protocols.

This section uses Windows 2016 as an example to describe how to configure AD FS as a SAML server to work with Trend Micro Email Security. Make sure you have installed AD FS successfully.

Procedure

1. Go to **Start** > **All Programs** > **Windows Administrative Tools** > **AD FS Management**.
2. On the AD FS management console, go to **AD FS**, right-click **Relying Party Trusts**, and then choose **Add Relying Party Trust**.
3. Complete settings for each screen in the Add Relying Party Trust wizard.
   a. On the **Welcome** screen, select **Claims aware** and click **Start**.
   b. On the **Select Data Source** screen, select **Enter data about the relying party manually** and click **Next**.
   c. On the **Specify Display Name** screen, specify a display name, for example, `Trend Micro Email Security End User Console`, and click **Next**.

d. On the **Configure Certificate** screen, click **Next**.

Note

No encryption certificate is required, and HTTPS will be used for communication between Trend Micro Email Security and federation servers.

e. On the **Configure URL** screen, select **Enable support for the SAML 2.0 WebSSO protocol**, type the relying party SAML 2.0 SSO service URL, and then click **Next**.

Note

Specify the SAML 2.0 SSO service URL for your region as follows:

`https://euc.<domain_name>/uiserver/euc/ssoAssert?cmpID=<unique_identifier>`

In the preceding and following URLs:

- Replace `<unique_identifier>` with a unique identifier. Record the unique identifier, which will be used when you create an SSO profile on the Trend Micro Email Security administrator console.
- Replace `<domain_name>` with any of the following based on your location:
  - North America, Latin America and Asia Pacific:

    `tmes.trendmicro.com`
  - Europe and Africa:

    `tmes.trendmicro.eu`
  - Australia and New Zealand:

    `tmes-anz.trendmicro.com`
  - Japan:

    `tmems-jp.trendmicro.com`
  - Singapore:

    `tmes-sg.trendmicro.com`
  - India:

    `tmes-in.trendmicro.com`
  - Middle East (UAE):

    `tmes-uae.trendmicro.com`

f. On the **Configure Identifiers** screen, type the identifier for the relying party trust, click **Add**, and then click **Next**.

Note

Specify the identifier for the relying party trust for your region as follows:

`https://euc.<domain_name>/uiserver/euc/ssoLogin`

g. On the **Choose Access Control Policy** screen, choose an access control policy and click **Next**.

h. Continue clicking **Next** in the wizard and finally click **Close**.

4. From the **Edit Claim Issuance Policy for Trend Micro Email Security End User Console** dialog box, click **Add Rule** in the **Issuance Transform Rules** tab.

5. Complete settings for each screen in the Add Transform Claim Rule wizard.

a. On the **Select Rule Template** screen, select **Send LDAP Attributes as Claims** for **Claim rule template** and click **Next**.

b. On the **Configure Rule** screen, specify a claim rule name and select **Active Directory** for **Attribute store**.

c. Select LDAP attributes and specify an outgoing claim type for each attribute. For example, select **E-Mail-Addresses** and type `email` as the outgoing claim type.

Important

When configuring the identity claim type for an SSO profile on Trend Micro Email Security, make sure you use the claim type specified here.

d. (Optional) Configure group claim type settings for user groups.

1. On the **Select Rule Template** screen, select **Send Group Membership as a Claim** for **Claim rule template** and click **Next**.
2. On the **Configure Rule** screen, specify a claim rule name, click **Browse** under **User's group**, and select AD groups.
3. Specify the outgoing claim type and outgoing claim values. For example, type `euc_group` and the AD group names.

Important

When configuring the group claim type for an SSO profile on Trend Micro Email Security, make sure you use the group claim type specified here.

e. Click **Finish**.

f. Click **OK** to close the wizard.

6. From **AD FS** > **Relying Party Trust**, double-click the relying party trust file you created earlier.

a. From the **Test Properties** dialog box, click the **Advanced** tab.

b. Select **SHA1** from the **Secure hash algorithm** drop-down list and click **OK**.

7. Collect the single sign-on logon and logoff URLs and obtain a certificate for signature validation from AD FS.

a. On the AD FS management console, go to **AD FS** > **Service** > **Endpoints**.

b. Look for the **SAML 2.0/WS-Federation** type endpoint and collect the URL path.

Note

The URL path will be used when you configure logon and logoff URLs on Trend Micro Email Security.

- Logon URL: <adfs_domain_name>/adfs/ls/
- Logoff URL: <adfs_domain_name>/adfs/ls/?wa=wsignout1.0

c. Go to **AD FS** > **Service** > **Certificates**.

d. Look for the **Token-signing** certificate, right-click it, and then select **View Certificate**.

e. Click the **Details** tab and click **Copy to File**.

f. Using the Certificate export wizard, select **Base-64 Encoded X.509 (.CER)**.

g. Assign a name to the file to complete the export of the certificate into a file.

Configuring Microsoft ENTRA ID

Microsoft Entra ID is Microsoft's multi-tenant cloud based directory and identity management service.

Make sure you have a valid subscription in Microsoft Entra ID that handles the sign-in process and eventually provides the authentication credentials of end users to the End User Console.

Procedure

1. On the Microsoft Entra ID management portal, select an active directory that you want to implement SSO.
2. Click **Enterprise applications** in the navigation area on the left and click **New application**.
3. On the **Browse Microsoft Entra ID Gallery (Preview)** screen, click **Create your own application**.

4. On the **Create your own application** panel that appears on the right, specify a name for your application, for example, `Trend Micro Email Security End User Console`, and click **Create**.
5. Under **Getting Started** in the overview of your application, click **1. Assign users and groups**, click **Add user/group**, select a specific user or group for this application and click **Assign**.
6. In the navigation area of your application, click **Single sign-on**.
7. Click **SAML** to configure the connection from your application to Microsoft Entra ID using the SAML protocol.
    a. Under **Basic SAML Configuration**, click **Edit**, specify the identifier and reply URL, and click **Save**.

Note

Specify the identifier for your region as follows:

`https://euc.<domain_name>/uiserver/euc/ssoLogin`

Specify the reply URL for your region as follows:

`https://euc.<domain_name>/uiserver/euc/ssoAssert?cmpID=<unique_identifier>`

In the preceding and following URLs:

- Replace <*unique_identifier*> with a unique identifier. Record the unique identifier, which will be used when you create an SSO profile on the Trend Micro Email Security administrator console.
- Replace <*domain_name*> with any of the following based on your location:
  - North America, Latin America and Asia Pacific:

    `tmes.trendmicro.com`
  - Europe and Africa:

    `tmes.trendmicro.eu`
  - Australia and New Zealand:

    `tmes-anz.trendmicro.com`
  - Japan:

    `tmems-jp.trendmicro.com`
  - Singapore:

    `tmes-sg.trendmicro.com`
  - India:

    `tmes-in.trendmicro.com`
  - Middle East (UAE):

    `tmes-uae.trendmicro.com`

Click **No, I'll test later** when you are prompted to choose whether to test single sign-on with `Trend Micro Email Security End User Console`. You are advised to perform a test after all SSO settings are complete.

b. Under **User Attributes & Claims**, click **Edit**, and specify the identity claim.

User attributes and claims are used to get the email addresses of logon accounts to authenticate their identity. By default, the source attribute **user.mail** is preconfigured to get the email addresses. If the email addresses in your organization are defined by another source attribute, do the following to add a new claim name:

Click **Add new claim**. On the **Manage claim** screen, specify the claim name, leave **Namespace** empty, select **Attribute** as **Source**, select a value from the **Source attribute** drop-down list, and click **Save**.

Important

When configuring the identity claim type for an SSO profile on Trend Micro Email Security, make sure you use the claim name specified here.

(Optional) Click **Add a group claim**. On the **Group Claims** screen, specify the groups associated with the end user, select **Group ID** as **Source attribute**, select **Customize the name of the group claim**, specify the group claim name, for example, `euc_group`, and click **Save**.

Important

When configuring the group claim type for an SSO profile on Trend Micro Email Security, make sure you use the group claim name specified here.

c. Under **SAML Signing Certificate**, click **Edit**, specify an email address for **Notification Email Addresses**, and click **Save**. Click

Download next to **Certificate (Base64)** to download a certificate file for Microsoft Entra ID signature validation on Trend Micro Email Security.

d. Under **Set up Trend Micro Email Security End User Console**, record the login and logout URLs.

Configuring Okta

This section describes how to add Trend Micro Email Security as a new application and configure SSO settings on your Okta Admin Console.

Procedure

1. Navigate to the Admin Console by clicking **Admin** in the upper-right corner.

   Note

   If you are in the Developer Console, click **< > Developer Console** in the upper-left corner and then click **Classic UI** to switch over to the Admin Console.

2. In the Admin Console, go to **Applications** > **Applications**.
3. Click **Add Application**, and then click **Create New App**.

   The **Create a New Application Integration** screen appears.
4. Select **Web** as the **Platform** and **SAML 2.0** as the **Sign on method**, and then click **Create**.
5. On the **General Settings** screen, type a name for Trend Micro Email Security in **App name**, for example, `Trend Micro Email Security End User Console`, and click **Next**.
6. On the **Configure SAML** screen, specify the following:

   a. Type `https://euc.<domain_name>/uiserver/euc/ssoAssert?cmpID=<unique_identifier>` in **Single sign on URL** based on your serving site.

Note

In the preceding and following URLs:

- Replace `<unique_identifier>` with a unique identifier. Record the unique identifier, which will be used when you create an SSO profile on the Trend Micro Email Security administrator console.
- Replace `<domain_name>` with any of the following based on your location:
  - North America, Latin America and Asia Pacific:

    `tmes.trendmicro.com`
  - Europe and Africa:

    `tmes.trendmicro.eu`
  - Australia and New Zealand:

    `tmes-anz.trendmicro.com`
  - Japan:

    `tmems-jp.trendmicro.com`
  - Singapore:

    `tmes-sg.trendmicro.com`
  - India:

    `tmes-in.trendmicro.com`
  - Middle East (UAE):

    `tmes-uae.trendmicro.com`

b. Select **Use this for Recipient URL and Destination URL**.

c. Type `https://euc.<domain_name>/uiserver/euc/ssoLogin` in **Audience URI (SP Entity ID)**.

d. Select **EmailAddress** in **Name ID format**.

e. Select **Okta username** in **Application username**.

f. (Optional) Click **Show Advanced Settings**, specify the following:

This step is required only if you want to configure a logoff URL on the Trend Micro Email Security administrator console. The logoff URL is used to log you off and also terminate the current identity provider logon session.

1. Next to **Enable Single Logout**, select the **Allow application to initiate Single Logout** check box.
2. Type `https://euc.<domain_name>/uiserver/euc/sloAssert?cmpID=<unique_identifier>` in **Single Logout URL**.
3. Type `https://euc.<domain_name>/uiserver/euc/ssoLogout` in **SP Issuer**.
4. Upload the logoff certificate in the **Signature Certificate** area.

   You need to download the logoff certificate from the Trend Micro Email Security administrator console in advance. Go to **Administration** > **End User Management** > **Logon Methods**. Click **Add** in the **Single Sign-on** section. On the pop-up screen, locate the **Identity Provider Configuration** section, select **Okta** as **Identity provider** and click **Download Logoff Certificate** to download the certificate file.
5. Keep the default values for other settings.

g. Under **ATTRIBUTE STATEMENTS (OPTIONAL)**, specify `email` in **Name**, and select **Unspecified** in **Name format** and **user.email** in **Value**.

Important

When configuring the identity claim type for an SSO profile on Trend Micro Email Security, make sure you use the attribute name specified here.

h. (Optional) Under **GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**, specify `euc_group` in **Name**, select **Unspecified** in **Name format** and specify filter conditions.

Important

When configuring the group claim type for an SSO profile on the Trend Micro Email Security, make sure you use the group attribute name specified here.

i. Click **Next**.

7. On the **Feedback** screen, click **I'm an Okta customer adding an internal app**, and then click **Finish**.

   The **Sign On** tab of your newly created Trend Micro Email Security application appears.

8. Click **View Setup Instructions**, and record the URL in **Identity Provider Single Sign-On URL** and download the certificate in **X.509 Certificate**.

Email Continuity

Note

This feature is not included in the Trend Micro Email Security Standard license.

For details about different license versions, see *Available license versions on page 1-26*.

With Email Continuity, Trend Micro Email Security provides a standby email system that gives virtually uninterrupted use of email in the event of a mail server outage. If a planned or unplanned outage occurs, Trend Micro Email Security will keep your incoming email messages for 10 days. Once your email server is back online within the 10-day period, these messages will be restored to your email server.

A continuity mailbox is available instantly and automatically, providing end users the ability to read, forward, download and reply to any email messages. This enables end users to have continued email access during an outage without requiring any action from IT.

In fact, Trend Micro Email Security will scan the email messages sent from the continuity mailbox based on its default outbound policy.

Administrators can configure and manage Email Continuity records on the Trend Micro Email Security administrator console, and end users will be able to use the continuity mailbox to manage email messages on the End User Console.

Share the End User Console web address for your region with your end users:

- North America, Latin America and Asia Pacific:

  https://euc.tmes.trendmicro.com

- Europe and Africa:

  https://euc.tmes.trendmicro.eu

- Australia and New Zealand:

  https://euc.tmes-anz.trendmicro.com

- Japan:

  https://euc.tmems-jp.trendmicro.com

- Singapore:

  https://euc.tmes-sg.trendmicro.com

- India:

  https://euc.tmes-in.trendmicro.com

- Middle East (UAE):

  https://euc.tmes-uae.trendmicro.com

Adding an Email Continuity record

Add Email Continuity records for specified recipient domains to provide uninterrupted email access for end users on this domain during email server outages.

Procedure

1. Go to **Administration** > **Other Settings** > **Email Continuity**.
2. Click **Add**.

   The **Add Email Continuity Record** screen appears.
3. Select a specific recipient domain from the **Domain name** drop-down list.
4. Select **Enable Email Continuity** to apply Email Continuity to the selected domain.
5. Select **Enable Email Sending**.

   Note

   This option is disabled by default.

   This option allows you to compose and send email messages directly from the End User Console. If your domain has SPF records, make sure the following record is included:

   `spf.tmes.trendmicro.com`
6. Click **Add**.

Editing an Email Continuity record

Procedure

1. Go to **Administration** > **Other Settings** > **Email Continuity**.
2. Click the domain name of the record that you want to edit.

The **Edit Email Continuity Record** screen appears.

3. Change your setting as required.
4. Click **Save**.

Logon access control

Trend Micro Business Account can determine the clients that are allowed to access the administrator console, End User Console and resources within Trend Micro Email Security by specifying a list of approved IP addresses. The Business Account can also specify the action to take on the access request from an unapproved IP address.

With this feature enabled:

- Only administrator from the approved IP addresses can be authorized to log on to the administrator console (either through local account or SSO), verify their profiles, and complete API access.

Note

API access aims to perform operations on resources within Trend Micro Email Security and synchronize user directories via REST APIs.

For more information, refer to the *Trend Micro Email Security REST API Online Help* and *Directory Synchronization Tool User's Guide* at http://docs.trendmicro.com/en-us/enterprise/trend-micro-email-security.aspx for details.

- Only end users from the approved IP addresses can be authorized to log on to the End User Console (either through local account or SSO), activate their accounts, and perform digest inline actions.
- For the access request from an unapproved IP address, Trend Micro Email Security can allow access without IP address check, allow access but record audit logs, or block access and record audit logs, depending on your access control settings.

The **Logon Access Control** screen includes the following tabs:

- **Access Control Settings**: Displays the access control settings that you want to apply to the access requests from unapproved IP addresses.
- **Approved IP Addresses**: Lists the IP addresses from which the access to Trend Micro Email Security are always allowed.

Configuring access control settings

Procedure

1. Go to **Administration** > **Other Settings** > **Logon Access Control**.
2. On the **Access Control Settings** tab, select whether to allow access to Trend Micro Email Security from unapproved IP addresses.
   - **Administrator Console**: Select an action (**Bypass**, **Allow and log**, and **Block and log**) to take on the access request to the Trend Micro Email Security administrator console from an unapproved IP address. The default value is **Bypass**.
     - **Bypass**: The request bypasses access control check. Trend Micro Email Security allows the access without verifying the client's IP address.
     - **Allow and log**: Trend Micro Email Security allows the access but records audit logs.
     - **Block and log**: Trend Micro Email Security blocks the access and records audit logs.

     This setting also applies when administrators attempt to verify their profiles from an unapproved IP address.
   - **End User Console**: Select an action (**Bypass**, **Allow and log**, and **Block and log**) to take on the access request to the Trend Micro Email Security End User Console from an unapproved IP address. The default value is **Bypass**.

     This setting also applies when end users attempt to activate their accounts from an unapproved IP address.
   - **API Access**: Select an action (**Bypass**, **Allow and log**, and **Block and log**) to take on the access request to Trend Micro Email Security

through REST APIs from an unapproved IP address. The default value is **Bypass**.

Note

IP-based access control is enabled if you select **Allow and log** or **Block and log** for any of the drop-down lists. In this case, at least one approved IP address must be configured on the **Approved IP Addresses** tab; otherwise, IP-based access control will not take effect.

3. Optionally select **Also apply to digest inline action**.

   Selecting this check box applies the same setting configured for **End User Console** to digest inline actions.

4. Optionally specify the email addresses to receive alerts on blocked or logged access.

   a. Type one or more email addresses as the alert recipients in the **Email Address** field.

      Use semicolons (;) to separate email addresses. There is no need to add a space after a semicolon.

   b. Specify the maximum number of alerts that can be sent within 24 hours.

5. Click **Save**.

Configuring approved IP addresses

Procedure

1. Go to **Administration** > **Other Settings** > **Logon Access Control**.
2. On the **Approved IP Addresses** tab, click **Add**.
3. Specify the IP address and type a description.

   Only IPv4 addresses are supported. Private IP addresses are not supported.

4. Click **Save**.

Directory management

You can import LDAP Data Interchange Format (LDIF) or comma-separated values (CSV) files into Trend Micro Email Security. This helps Trend Micro Email Security to better filter and process messages for valid email addresses. Messages to invalid email addresses will be rejected.

Trend Micro Email Security uses user directories to help prevent backscatter (or outscatter) spam and Directory Harvest Attacks (DHA). Importing user directories lets Trend Micro Email Security know legitimate email addresses and domains in your organization.

Trend Micro Email Security also provides a synchronization tool that enables you to synchronize your current groups, email accounts and email aliases from Open LDAP, Microsoft Active Directory, Microsoft AD Global Catalog, Microsoft 365/Microsoft Entra ID and IBM Domino servers to the Trend Micro Email Security server.

The **Directory Management** screen includes the following tabs:

- **Directory Synchronize**
  - **Downloads**: Displays the download paths or links to the Directory Synchronization Tool, Directory Synchronization Tool User's Guide, REST API Client, and REST API Online Help.
  - **Synchronization Summary**: Displays the total number of email aliases, groups, and valid recipients last synchronized from all directory sources.
  - **Synchronization History**: Displays the number of email aliases, groups, and valid recipients synchronized each time.
- **Directory Import**
  - **Import User Directory**: Selections for importing a new user directory file.
  - **Imported User Directory History**: The current user directory file(s) that Trend Micro Email Security is using.

- **Export**
  - **Valid recipients**: Exports the existing valid recipients to a CSV file.
  - **Groups**: Exports the existing groups to a CSV file.
  - **Email aliases**: Exports the existing email aliases to a CSV file.

Synchronizing user directories

The **Directory Synchronize** tab displays downloads, synchronization summary, and synchronization history. This screen consists of the following sections:

- **Downloads**: Displays the download paths for the Directory Synchronization Tool and Directory Synchronization Tool User's Guide.
- **Synchronization Summary**: Displays the total number of email aliases, groups, and valid recipients last synchronized from all directory sources.
- **Synchronization History**: Displays the number of email aliases, groups, and valid recipients synchronized each time.

Element	Description
Timestamp	Time when a synchronization happened
Sync Objects	Objects that have been synchronized, such as email aliases, groups, and valid recipients **Note** Since version 2.0.10088 of the Directory Synchronization Tool, the number of email aliases, groups, and valid recipients synchronized every time has also been recorded here.

Element	Description
Sync Tool Location	Information about the machine where the synchronization tool is installed, including its IP address, FQDN or host name
Result	Whether the synchronization is successful or unsuccessful, or whether any groups, email aliases or policies were added or removed

Importing user directories

You can import LDAP Data Interchange Format (LDIF) or comma-separated values (CSV) files into Trend Micro Email Security. This helps Trend Micro Email Security to better filter and process messages for valid email addresses. Messages to invalid email addresses will be rejected.

Important

Before you import an LDIF or CSV directory file, note the following:

- Trend Micro Email Security only recognizes ANSI-encoded LDIF (with the extension `.ldf`) and ANSI or UTF-8-encoded CSV (with the extension `.csv`) files. Do not include blank lines or other irrelevant data in the file that you import. Use caution when creating a file.
- When importing user directory files, Trend Micro Email Security replaces all records for a managed domain at once. If any email addresses for a managed domain are imported, all other email addresses for that domain are removed. Newly imported email addresses for that domain, and records for other managed domains, will be kept. If you import an updated user directory file that does not have any information for one of your domains, the entries for those domains remain the same and are not overwritten.

  Every time you import a directory file, it overwrites the old version. If you import an updated directory file that has information for one of your domains, all entries for those domains are overwritten. Use caution when importing a directory.
- You can only see the directories that are associated with your administrator account. If you are sharing your Trend Micro Email Security service with another administrator (for example, a value-added reseller) who logs on with his/her specific account information, Trend Micro Email Security will not show the directories for that account.
- Every time you add more users to your network, you must import your updated user directories; otherwise, Trend Micro Email Security will reject email from newly added users.

WARNING!

Trend Micro strongly suggests that you do not import more than 24 directories in a day. Doing so could overwhelm system resources.

Temporarily disable all valid recipients before import a file. When you are confident that all entries are correct, re-enable all valid recipients. To disable or enable valid recipients, go to **Inbound Protection** > **Connection Filtering** > **Recipient Filter** and click **Disable All** or **Enable All**.

Procedure

1. Next to **Format**, select the format type:
   - **LDIF**
   - **CSV**

Note

If you create a CSV file, divide the records into fields for `email_address` and `Firstname Lastname` and separate them using a comma and optional quotation marks. Use of spaces or other delimiters is not supported. Use one record per line.

For example:

VALID
`bob@example.com,Bob Smith` `sally@example.com,Sally Jones`
`"bob@example.com","Bob Smith"` `"sally@example.com","Sally Jones"`

NOT VALID
`bob@example.com,Bob Smith,sally@example.com,Sally Jones`

Microsoft Excel will save a two column chart as a CSV using valid formatting.

2. Next to **Name**, type a descriptive name for the file.
3. Next to **File location**, type the file directory path and filename or click **Choose File** and select the `.ldf` or `.csv` file on your computer.
4. Click **Verify File** to read the file and show a summary of how many email addresses were found.

   After the progress bar completes, a summary screen appears showing the following:

   - **Import Summary**: A summary of the information above
   - **Domains and Number of Users to Replace Current Users**: The domains that you specified when you subscribed to the Trend Micro Email Security service

- **Unauthorized Domains**: Any domains that are included in your directory file, but are not officially registered with your Trend Micro Email Security service

Note

Trend Micro Email Security does not provide service for these domains and their corresponding email addresses.

5. Click **Import**.

   This will import and then enable the email address list.

Exporting user directories

You can export valid recipients, groups and email aliases to a comma-separated values (CSV) file.

Procedure

1. Choose to export valid recipients, groups or email aliases and do the following:
   - Select a domain from the **Valid recipients** drop-down list and click **Export to CSV**.
   - Select a group from the **Groups** drop-down list and click **Export to CSV**.
   - Next to **Email aliases**, click **Export to CSV**.

Note

In the exported file, the primary email alias displays at the beginning of each line.

Installing the directory synchronization tool

The Directory Synchronization Tool automates the import of directory files for valid recipient email addresses, user groups and email aliases. The

Directory Synchronization Tool provides functionality similar to the **Import User Directory** feature on the **Directory Import** screen.

Procedure

1. Go to **Administration** > **Service Integration**.
2. On the **API Access** tab, click **Add** to generate a key.

   The API Key is the global unique identifier for your Directory Synchronization Tool to authenticate its access to Trend Micro Email Security. It must be used together with the administrator account that created it. A new API Key is enabled by default.

   If you want to change your API Key later on, click **Add** to generate a new key and use the new key in your requests. You can click the toggle button under **Status** to disable the old key or delete it if both of the following conditions are met:

   - Requests can be sent successfully with the new key.
   - The old key is not used by any other applications that have access to Trend Micro Email Security.

   A maximum of two API Keys are allowed at a time.

   Important

   The API Key allows your Directory Synchronization Tool to communicate with Trend Micro Email Security. Keep the API Key private.

3. In the **Downloads** list, click download to download the desired items.

   - **Directory Synchronization Tool**: Provided for synchronizing accounts and groups between local directories and the Trend Micro Email Security server.
   - **Directory Synchronization Tool User's Guide**: Available for more information on using the synchronization tool.

4. Save the tool on a local drive.

5. Follow the installation steps to install the tool.

Co-branding

Trend Micro Email Security enables you to display a service banner, for example, your company logo, on the top banner of the Trend Micro Email Security administrator console and End User Console. This is a cost-effective way to promote your company and brand awareness.

After configuring co-branding settings, provide your customers with the web address to access their co-branded administrator console or End User Console if you are a reseller. The web address may vary for different regions.

TABLE 10-10. Administrator Console Addresses

ACCOUNT TYPE	CONSOLE ADDRESS
Customer Licensing Portal accounts and Licensing Management Platform accounts	For these accounts, the web addresses of the administrator console still remain unchanged. For detailed web addresses, see *Accessing the Trend Micro Email Security administrator console on page 2-2*.

Account Type	Console Address

Local subaccounts added by the administrator	Append `/co-brand/` and the Trend Micro Email Security account name to the base URL.
	
	For example, to access the co-branded administrator console for the account named “adminB”, type the following address for your region:
	
	• North America, Latin America and Asia Pacific:
	
	`https://ui.tmes.trendmicro.com/co-brand/adminB`
	
	• Europe and Africa:
	
	`https://ui.tmes.trendmicro.eu/co-brand/adminB`
	
	• Australia and New Zealand:
	
	`https://ui.tmes-anz.trendmicro.com/co-brand/adminB`
	
	• Japan:
	
	`https://ui.tmems-jp.trendmicro.com/co-brand/adminB`
	
	• Singapore:
	
	`https://ui.tmes-sg.trendmicro.com/co-brand/adminB`
	
	• India:
	
	`https://ui.tmes-in.trendmicro.com/co-brand/adminB`
	
	• Middle East (UAE):
	
	`https://ui.tmes-uae.trendmicro.com/co-brand/adminB`

SSO accounts	For these accounts, the console address is the URL generated in Step 4 in *Configuring single sign-on on page 10-42*.

TABLE 10-11. End User Console Addresses

ACCOUNT TYPE	CONSOLE ADDRESS

Local accounts	Append `/euc-co-brand/` and the Trend Micro Email Security managed domain to the base URL.
	
	For example, to access the co-branded End User Console for the managed domain "example.com", type the following address for your region:
	
	• North America, Latin America and Asia Pacific:
	
	`https://euc.tmes.trendmicro.com/euc-co-brand/example.com`
	
	• Europe and Africa:
	
	`https://euc.tmes.trendmicro.eu/euc-co-brand/example.com`
	
	• Australia and New Zealand:
	
	`https://euc.tmes-anz.trendmicro.com/euc-co-brand/example.com`
	
	• Japan:
	
	`https://euc.tmems-jp.trendmicro.com/euc-co-brand/example.com`
	
	• Singapore:
	
	`https://euc.tmes-sg.trendmicro.com/euc-co-brand/example.com`
	
	• India:
	
	`https://euc.tmes-in.trendmicro.com/euc-co-brand/example.com`
	
	• Middle East (UAE):
	
	`https://euc.tmes-uae.trendmicro.com/euc-co-brand/example.com`

SSO accounts	For these accounts, the console address is the URL generated in Step 4 in *Configuring single sign-on on page 10-65*.

Service integration

Currently, Trend Micro Email Security integrates with the following Trend Micro products:

- Apex Central

  For more information about Apex Central, see *Apex Central on page 1-32*.

- Remote Manager

  For more information about Remote Manager, see *Remote Manager on page 1-34*.

Furthermore, Trend Micro Email Security supports API openness to allow integration with external systems via APIs. For example, Trend Micro Email Security opens REST APIs to allow customers to query domains; query, add, replace, and delete directory users; and retrieve policy event logs and mail tracking logs for the purpose of third-party SIEM application integration.

API access

Trend Micro Email Security allows connection from the Directory Synchronization Tool to automate the import of directory files for valid recipient email addresses, user groups and email aliases. Also, Trend Micro Email Security provides programmatic access through REST APIs, allowing customers to perform create, read, update and delete operations on resources within Trend Micro Email Security.

To use these features, API Keys are required to authenticate the external systems' access to Trend Micro Email Security.

The **API Access** tab lets you obtain and manage your API Keys.

Obtaining an API key

Procedure

1. Go to **Administration** > **Service Integration**.
2. On the **API Access** tab, click **Add** to generate a key.

The API Key is the global unique identifier for your application to authenticate its access to Trend Micro Email Security. It must be used together with the administrator account that created it. A new API Key is enabled by default.

If you want to change your API Key later on, click **Add** to generate a new key and use the new key in your requests. You can click the toggle button under **Status** to disable the old key or delete it if both of the following conditions are met:

- Requests can be sent successfully with the new key.
- The old key is not used by any other applications that have access to Trend Micro Email Security.

A maximum of two API Keys are allowed at a time.

Important

The API Key allows your application to communicate with Trend Micro Email Security. Keep the API Key private.

Log retrieval

The **Log Retrieval** tab allows you to decide whether to retrieve policy event logs and mail tracking logs via REST APIs for third-party SIEM application integration.

To retrieve the logs, you must enable the log retrieval function first.

For more information about log retrieval via REST APIs, refer to the Trend Micro Email Security REST API Online Help.

Apex Central

Trend Micro Apex Central consolidates your organization's suspicious object information and synchronizes the suspicious objects among integrated managed products. After Trend Micro Email Security is registered to Apex Central, Apex Central automatically synchronizes the suspicious URLs, file SHA-1 hashes, and file SHA-256 hashes with Trend Micro Email Security at a

scheduled time interval. In addition to its own scanning mechanism, Trend Micro Email Security cancan leverage the suspicious objects to detect known or potentially malicious files and URLs during scanning.

For more information about how Apex Central manages suspicious object lists, see the Apex Central Administrator's Guide.

Configuring suspicious object settings

Trend Micro Apex Central consolidates and synchronizes the Virtual Analyzer and user-defined suspicious object lists with Trend Micro Email Security. Enable this feature to implement the lists during scanning.

Before you begin configuring this feature, make sure that:

- You have installed Apex Central, and your Apex Central has a serving Deep Discovery product, which can be a Deep Discovery Inspector, Deep Discovery Email Inspector, or Deep Discovery Analyzer.
- Your Trend Micro Email Security has been registered to a required Trend Micro Apex Central.
- You have enabled Web Reputation settings in the spam policy you want to apply the suspicious URL list to.

Procedure

1. Go to **Administration** > **Other Settings** > **Service Integration**.
2. Click **Apex Central**.
3. Enable **Check for suspicious objects during scanning**.
4. Under **Security Level for Files**, specify the security level to determine whether to take actions on messages when suspicious files are detected during virus scanning.

   The actions to take are defined in the virus policy.

Note

Trend Micro Email Security classifies all files and URLs in the user-defined suspicious object lists as the "High" risk.

5. Under **Security Level for URLs**, make sure your specify the security level for Web Reputation in your spam policy to determine whether to take actions on messages when suspicious URLs are detected during spam scanning.

   The actions to take are defined in the spam policy.

6. Check additional information about suspicious object synchronization from the Apex Central.

7. Click **Save**.

Trend Vision One

Important

This is a "Pre-release" feature and is not considered an official release. Please review the *Pre-release disclaimer on page xiii* before using the feature.

Trend Vision One consolidates suspicious object information based on input from different sources and synchronizes the suspicious objects with integrated products. Once integrated, Trend Micro Email Security automatically synchronizes suspicious URLs, file SHA-1 hashes, and file SHA-256 hashes from Trend Vision One upon integration and later whenever these types of suspicious objects are updated. In addition to its own mechanism, Trend Micro Email Security can leverage the suspicious objects to detect known or potentially malicious files, URLs, and sender addresses during scanning.

For more information about how Trend Vision One manages suspicious objects, see the "Threat Intelligence" > "Suspicious Object Management" in Trend Vision One Online Help.

Configuring suspicious object settings

Before you start, make sure you meet the following requirements:

- You have integrated Trend Micro Email Security with Trend Vision One.

Note

To integrate, go to **Service Management** > **Product Instance** in the Trend Vision One console.

- You have enabled virus policies. Suspicious file SHA-1/SHA-256 hashes apply during virus scanning.
- You have enabled spam policies with Web Reputation turned on. Suspicious URLs apply during Web Reputation scanning.

Procedure

1. Go to **Administration** > **Other Settings** > **Service Integration**.
2. Click **Trend Vision One**.
3. Enable **Check for suspicious files and URLs**.

   For files or URLs that match the suspicious objects from both Trend Vision One and Apex Central, the settings for the suspicious objects from Trend Vision One take precedence.
4. Enable **Check for suspicious sender addresses**.

   Trend Micro Email Security synchronizes only the sender addresses configured with the “Block/Quarantine” action in Trend Vision One and blocks messages from these senders.
5. Under **Security Level for Files**, specify the security level to determine whether to take actions on messages when suspicious files are detected during virus scanning.

   The actions to take are synchronized from Trend Vision One along with the suspicious objects.
6. For **Security Level for URLs**, make sure your specify the security level for Web Reputation in your spam policy to determine whether to take actions on messages when suspicious URLs are detected during spam scanning.

   The actions to take are synchronized from Trend Vision One along with the suspicious objects.

7. Check additional information about suspicious object synchronization from Trend Vision One.
8. Click **Save**.

Remote Manager

The **Remote Manager** tab shows the settings you must configure to integrate with Remote Manager.

To enable Trend Micro Remote Manager to monitor and manage Trend Micro Email Security:

1. Contact your reseller administrator to add Trend Micro Email Security as a managed product on the Remote Manager web console and obtain the authorization key generated by Remote Manager.
2. Go to **Administration** > **Other Settings** > **Service Integration** and click **Remote Manager**.
3. Type your authorization key you obtained and click **Connect**.

To prevent Trend Micro Remote Manager from managing Trend Micro Email Security:

1. Go to **Administration** > **Other Settings** > **Service Integration** and click **Remote Manager**.
2. Click **Discontinue**.
3. After you get a confirmation message, click **OK**.

Phishing simulation

The **Phishing Simulation** tab lets you decide whether to bypass inbound protection scans for Trend Micro phishing simulation emails.

Trend Micro provides phishing simulations to enhance information security awareness of your employees against the latest threats and educate them to quickly and efficiently spot attacks. Trend Micro phishing simulations enable you to test what could happen to your organization before the hackers try.

Procedure

1. Go to **Administration** > **Other Settings** > **Service Integration** and click **Phishing Simulation**.
2. Enable the **Bypass scans for Trend Micro phishing simulations** toggle to let Trend Micro Email Security skip scans for incoming emails sent from Trend Micro phishing simulation IP addresses.

Note

You can check the **Trend Micro phishing simulation IP addresses** in the screen.

Email reporting add-in for Outlook

The Email Reporting Add-in for Outlook provides an easy way for your users to report false positives and false negatives to Trend Micro Email Security, which uses the reported data to improve threat detection for your Exchange email service.

Note

This feature is not available at the Japan site.

The add-in is compatible with the following Exchange environments:

- Server side:
  - Microsoft 365 Apps
  - Exchange Server 2016
  - Exchange Server 2019
- Client side:
  - Microsoft 365 Apps
  - Outlook on the web in Microsoft 365 (Supported on Microsoft Edge, Google Chrome, and Mozilla Firefox)

If you are using the Microsoft 365 Apps at the server side, follow the instructions below to use the Email Reporting Add-in for Outlook.

Action	Description
Deploy the add-in	Deploy the add-in to your users' Outlook mailboxes in the Microsoft 365 admin center. For details, see *Deploying the add-in in the Microsoft 365 admin center on page 10-107*.
Configure the add-in	Configure whether your users can report false positives and false negatives to Trend Micro Email Security. 1. Log on to the Trend Micro Email Security console, and go to **Administration** > **Other Settings** > **Email Reporting Add-in for Outlook**. 2. Turn on the toggle allow your users to report emails as spam, phishing, or not a risk to Trend Micro Email Security. **Note** • Reporting an email also sends a copy of the email to Trend Micro. However, this action does not move or delete the email. • End users can report emails that are received over the last 30 days and are protected by Trend Micro Email Security. For example, internal emails, emails in the Sent Items folder, and emails for unprotected domains cannot be reported.
Update the add-in	Update the add-in to the latest version. Trend Micro Email Security will make announcements when a new version is available. For details, see *Updating the add-in in the Microsoft 365 admin center on page 10-109*

Action	Description
Remove the add-in	Remove the add-in when it is no longer used in your organization. 1. Log on to the Microsoft 365 admin center with your Global Administrator account. 2. Go to **Settings** > **Integrated apps**, and locate and click **Report Email**. 3. On the **Report Email** screen, click **Remove app** under **Actions**. 4. On the **Remove apps** screen, check **Yes, I'm sure I want to remove the app and associated data**, and click **Remove**. According to Microsoft, it can take up to 24 hours for an add-in removal to apply at your users' side.

If you are using Exchange Server 2016 or 2019 at the server side, follow the instructions below to use the Email Reporting Add-in for Outlook.

Action	Description
Deploy the add-in	Deploy the add-in to your users' Outlook mailboxes in the Exchange admin center. For details, see *Deploying the add-in in the Exchange admin center on page 10-108*

Action	Description
Configure the add-in	Configure whether your users can report false positives and false negatives to Trend Micro Email Security. 1. Log on to the Trend Micro Email Security console, and go to **Administration** > **Other Settings** > **Email Reporting Add-in for Outlook**. 2. Turn on the toggle allow your users to report emails as spam, phishing, or not a risk to Trend Micro Email Security. **Note** Reporting an email also sends a copy of the email to Trend Micro. However, this action does not move or delete the email.
Update the add-in	Update the add-in to the latest version. 1. Remove the existing Email Reporting Add-in. For details, see "Remove the add-in" in this table. 2. Deploy the latest Email Reporting Add-in. For details, see *Deploying the add-in in the Exchange admin center on page 10-108*. According to Microsoft, it can take up to 72 hours for the update of an add-in to apply at your users' side.
Remove the add-in	Remove the add-in when it is no longer used in your organization. 1. Log on to the Exchange admin center with an administrator account. 2. Go to **organization** > **add-ins**. 3. In the add-in list on the **add-ins** screen, select **Report Email** and click the delete button. According to Microsoft, it can take up to 72 hours for the removal of an add-in to apply at your users' side.

Deploying the add-in in the Microsoft 365 admin center

Procedure

1. Log on to the Trend Micro Email Security console, go to **Administration** > **Other Settings** > **Email Reporting Add-in for Outlook**, and copy the **Link to manifest file**.

   The link uploads the add-in in the Microsoft 365 admin center.

2. Log on to the Microsoft 365 admin center with your Global Administrator account.

3. Go to **Settings** > **Integrated apps** and click **Upload custom apps**.

4. On the **Upload Apps to deploy** screen, click **Provide link to manifest file**, paste the link to the add-in manifest file you copied in step 1, and click **Validate**.

5. Wait until the validation is completed and click **Next**.

6. On the **Add users** screen, select an option under **Assign users**, and click **Next**.

   Note

   This add-in works only for Exchange users protected by Trend Micro Email Security.

7. On the **Accept permissions requests** screen, review the app permissions and capabilities, and click **Next**.

8. On the **Review and finish deployment** screen, review the information and click **Finish deployment**.

   Wait a few minutes for the deployment to complete.

9. Click **Done**.

   According to Microsoft, it can take up to 24 hours for a newly deployed add-in to appear on the app ribbon in your users' Outlook mailboxes.

Your users may need to relaunch Office to view the add-in icon on the app ribbon.

Deploying the add-in in the Exchange admin center

Procedure

1. Log on to the Trend Micro Email Security console, go to **Administration** > **Other Settings** > **Email Reporting Add-in for Outlook**, and copy the **Link to manifest file**.

   The link uploads the add-in in the Exchange admin center.

2. Log on to the Exchange admin center with an administrator account.
3. Go to **organization** > **add-ins**.
4. Click the add icon (+) and click **Add from URL**.
5. In the **URL** text box on the **Add from URL** dialog box, paste the link you copied in step 1, and click **install**.
6. In the add-in list on the **add-ins** screen, double-click **Report Email**.
7. On the **Report Email** dialog box, select **Make this add-in available to users in your organization**, and then specify user defaults.
   - **Optional, enabled by default**: Enable the add-in by default and allow your users to turn off the add-in.
   - **Optional, disabled by default**: Disable the add-in by default and allow your users to turn on the add-in.
   - **Mandatory, always enabled. Users can't disable this add-in**: Enable the add-in by default and do not allow your users to turn off the add-in.
8. Click **Save**.

   According to Microsoft, it can take up to 72 hours for a newly deployed add-in to appear on the app ribbon in your users' Outlook mailboxes.

Your users may need to relaunch Office to view the add-in icon on the app ribbon.

Updating the add-in in the Microsoft 365 admin center

Procedure

1. Log on to the Trend Micro Email Security console, go to **Administration** > **Other Settings** > **Email Reporting Add-in for Outlook**, and copy the **Link to manifest file**.
2. Log on to the Microsoft 365 admin center with your Global Administrator account.
3. Go to **Settings** > **Integrated apps**.
4. Locate and click **Report Email**.
5. On the **Report Email** screen, click **Update app** under **Actions**.
6. On the **Update file** screen, click **Provide link to manifest file**, paste the link you copied in step 1, and click **Validate**.
7. Wait until the validation is completed and click **Next**.
8. Click **Accept and update** and click **Done**.

   According to Microsoft, it can take up to 72 hours for the update of an add-in to apply at your users' side.

License information

The **License Information** screen provides a summary of the following:

- **Purchased version**: Displays the product license version you purchased.
- **Activation code**: Displays the activation code.
- **Expiration date**: Displays the date on which your license expires.
- **Grace end date**: Displays the end date of the grace period granted after the expiration of your license.

- **License type**: Displays either “Full” or “Trial” version.
- **Seat count**: Displays the total number of seats assigned to your license.

Immediately after your license expires, it will go through a grace period, wherein the service continues as expected. After the grace period, your service will be suspended, and your data will be permanently deleted. To prevent unnecessary disruptions to your email service, please renew your license or change your MX records before the grace end date.

If you have two valid licenses (namely, Trend Micro Email Security Standard and Trend Micro Email Security Advanced), both of them display on this screen and Trend Micro Email Security Advanced applies by default. After the grace period of Trend Micro Email Security Advanced expires, your license will automatically downgrade to Trend Micro Email Security Standard.

There are two ways to manage your licenses:

- From the Licensing Management Platform

  The Licensing Management Platform allows partners to self-provision and auto-renew licenses. Contact your reseller or MSP to add, renew or extend your licenses.

- From the Customer Licensing Portal

  Visit the Customer Licensing Portal website at https://clp.trendmicro.com and activate, register and manage your products on the portal. For details, see the supporting documentation at:

  http://docs.trendmicro.com/en-us/smb/customer-licensing-portal.aspx

If you want to convert a trial license into a full license or upgrade from Trend Micro Email Security Standard to Trend Micro Email Security Advanced, do the following:

1. Log on to the Customer Licensing Portal website (https://clp.trendmicro.com).
2. From the Customer Licensing Portal page, click **Provide Key**.
3. Provide your activation code and click **Continue**.

Activating Sandbox as a Service

To activate Sandbox as a Service, obtain the Activation Code from your Trend Micro sales representative or reseller and provide the Activation Code on the Customer Licensing Portal.

Note

If you have not activated the license for Sandbox as a Service or your license expires, all your Virtual Analyzer settings in virus and spam policies cannot take effect.

Procedure

1. Log on to the Customer Licensing Portal using your Trend Micro account and password.
2. Click the **My Products/Services** menu tab.
3. Click **Provide Key**.

   The **License Key** screen appears.
4. Type your Activation Code.
5. Click **Continue**.

   The **My Products/Services** screen appears and displays the updated license information.
6. Log on to the Trend Micro Email Security administrator console.
7. Check whether the license activation is successful.

   Wait for some time because the license activation may take as long as 20 minutes to finish. If you keep seeing the error message about the Sandbox as a Service license after that, contact technical support for assistance.

Migrating data from IMSS or IMSVA

If you are a customer of InterScan Messaging Security Suite (IMSS) or InterScan Messaging Security Virtual Appliance (IMSVA) and want to switch to Trend Micro Email Security, Trend Micro Email Security allows you to migrate your existing data from IMSS 9.1 or IMSVA 9.1.

Data that will be migrated

All settings in IMSS or IMSVA will be migrated to Trend Micro Email Security completely or partially except those listed in *Data that will not be migrated on page 10-119*. Among the settings that are partially migrated, some are modified to adapt to Trend Micro Email Security due to the feature differences between IMSS or IMSVA and Trend Micro Email Security. Therefore, you need to confirm or fix these settings according to the on-screen instructions after migration.

The following table lists some examples of the settings that will be partially migrated and describes the feature differences.

Note

For details about all the settings that are completely or partially migrated, see the data migration report downloaded from the Trend Micro Email Security administrator console when the migration completes.

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
Policy > **Policy List**	The following settings on the **Step 1: Select Recipients and Senders** screen: • Sender • Recipient	The following submenus under the **Inbound Protection** and **Outbound Protection** menus:	The following settings in the **Senders** section of the **Recipients and Senders** tab: • Sender	LDAP users in IMSS or MISVA are migrated as static email addresses in Trend Micro Email Security.

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
	• Sender to recipient exception	• **Virus Scan** • **Spam Filtering** • **Content Filtering** • **Data Loss Prevention** > **Data Loss Prevention (DLP) Policy**	• Recipient • Sender to recipient exception	
	Condition match settings on the **Step 2: Select Scanning Conditions** screen	• **Inbound Protection** > **Content Filtering** • **Outbound Protection** > **Content Filtering**	Condition match settings in the **Advanced** section of the **Scanning Criteria** tab	Only content filtering supports **all condition matched (AND)**.
	True file type settings in the **Attachment** section of the **Step 2: Select Scanning Conditions** screen	• **Inbound Protection** > **Content Filtering** • **Outbound Protection** > **Content Filtering**	True file type settings in the **Advanced** section of the **Scanning Criteria** tab	Trend Micro Email Security does not support MSI, PNG, 7-Zip, or Microsoft Windows shortcuts.
	Global DKIM Enforcement rule	**Inbound Protection** > **Domain-based Authentication** > **DomainKeys**	Settings in the **Default (for unspecified domains)** policy (including the	Trend Micro Email Security uses both the header sender address and envelope sender

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
		Identified Mail (DKIM) Verification	action and **Enforced Peers**)	address instead of only the header sender address for matching the list of enforced peers.
Policy > **Approved List**	The settings of the following approved lists: • DKIM approved list • Web reputation approved list • URL keyword list	• **Inbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Verification** • **Administration** > **Policy Objects** > **Web Reputation Approved List** • **Administration** > **Policy Objects** > **URL Keyword Exception List**	The settings of the following approved lists: • DKIM approved list (**Ignored Peers** section in the **Default (for unspecified domains)** policy) • Web reputation approved list • URL keyword exception list	Trend Micro Email Security uses the envelope sender address instead of the header sender address for matching the list of ignored peers.

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
Policy > **Policy Objects** > **Address Groups**	Name and address settings of an address group	**Administration** > **Policy Objects** > **Address Groups**	Name and address settings of an address group	Trend Micro Email Security supports wildcard domains (for example, *@*.example.com) in hybrid address groups, and does not support wildcard domains in internal address groups. If an address group is used as senders (or sender exceptions) in outbound policies or recipients (or recipient exceptions) in inbound policies and the group contains email addresses from unmanaged domains, Trend Micro Email Security will create a copy of the address group, delete those email addresses from the copy, and suffix the copy name with " - internal".
Policy > **Policy Objects** >	Match settings of a keyword or expression	**Administration** > **Policy Objects** >	Match settings of a keyword or expression	None

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
Keywords & Expressions		**Keywords and Expressions**		
Policy > **Policy Objects** > **Policy Notification**	Variables list in the settings of a policy notification	**Administration** > **Policy Objects** > **Notification**	Variables list in the settings of a policy notification	Trend Micro Email Security does not support the following variables: • %RULETYPE% • %ENTITY% • %QUARANTINE_PATH% • %QUARANTINE_AREA% • %PROTOCOL% • %HOSTNAME% • %MAILCHARSET% • %SUSPICIOUS_URL%
Sender Filtering > **Approved List**	The following settings of an approved list: • IP addresses • Groups of computers	**Inbound Protection** > **Connection Filtering** > **IP Reputation** > **Approved IP Addresses**	IP address settings in the **IP addresses** section	Trend Micro Email Security does not support the following settings: • IP addresses resolved from domains • Private IP addresses • IP addresses in disabled approved lists

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
	 **Note** Trend Micro Email Security migrates IP addresses and groups of computers from IMSVA only if the **Email Reputation and IP Profiler** check box to the right of **Apply to** is selected. This restriction does not apply to IMSS			

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
Sender Filtering > **Blocked List**	The following settings of a blocked list: • IP addresses • Groups of computers **Note** Trend Micro Email Security migrates only IP addresses and groups of computers whose **Action** is **Block Permanently**.	**Inbound Protection** > **Connection FilteringIP Reputation** > **Blocked IP Addresses**	IP address settings in the **IP addresses** section	Trend Micro Email Security does not support the following settings: • IP addresses resolved from domains • Private IP addresses • IP addresses in disabled blocked lists
Sender Filtering > **DMARC**	DMARC settings	**Inbound Protection** > **Domain-based Authentication**	DMARC settings	Trend Micro Email Security uses both the header sender address and

Navigation in IMSS or IMSVA	Source Settings	Navigation in Trend Micro Email Security	Destination Settings	Feature Differences
	Note DMARC settings are available only in IMSVA.	> **Domain-based Message Authentication, Reporting and Conformance (DMARC)**		envelope sender address instead of only the header sender address for matching the list of enforced peers.
Administration > **IMSVA Configuration** > **DKIM Signature**	Advanced settings of DKIM signatures **Note** DKIM signatures are available only in IMSVA.	**Outbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Signing**	Advanced settings of DKIM signatures	Trend Micro Email Security does not support exempt domains.

Data that will not be migrated

The following table lists the settings on the IMSS or IMSVA management console that will not be migrated to Trend Micro Email Security and describes the reason. All settings on the EUQ management console will not be migrated.

Note

For details about all the settings that are not migrated, see the data migration report downloaded from the Trend Micro Email Security administrator console when the migration completes.

Navigation in IMSS or IMSVA	Settings	Remarks
Dashboard	All settings	The dashboard is a statistical summary of past mail traffic and scanning results. Trend Micro Email Security provides a more powerful dashboard feature.
System Status	All settings	Trend Micro Email Security is a cloud-based product. It is unnecessary to display system status information.
Cloud Pre-Filter	All settings	Trend Micro Email Security is a cloud-based product. It is unnecessary to display cloud pre-filter information.

Navigation in IMSS or IMSVA	Settings	Remarks

Policy > **Policy List**	• Settings on the **Step 1: Select Recipients and Senders** screen
	  • **POP3** option of the **This rule will apply to** drop-down list
	• Settings on the **Step 2: Select Scanning Conditions** screen
	  • **C&C email settings** check box in the **C&C Email** section
	  • **Received time range** check box in the **Others** section
	  • **Unable to decrypt messages** check box in the **Others** section
	  • **Spoofed internal messages** check box in the **Others** section
	• Settings on the **Step 3: Select Actions** screen
	  • **Postpone delivery to** check box in the **Modify** section
	  • **Archive modified to** check box in the **Monitor** section
		Trend Micro Email Security does not support these settings.

Navigation in IMSS or IMSVA	Settings	Remarks
Policy > **Scanning Exceptions**	All settings	Trend Micro Email Security provides more powerful scan exception configuration, which is different from the configuration in IMSS or IMSVA. You need to manually configure scan exception settings in Trend Micro Email Security.
Policy > **Policy Objects** > **DLP Compliance Templates**	Predefined DLP compliance templates	Trend Micro Email Security already provides predefined DLP compliance templates.
Policy > **Policy Objects** > **DLP Data Identifiers**	Predefined expressions, file attributes, and keyword lists	Trend Micro Email Security already provides predefined DLP data identifiers.
Policy > **Scan Engine**	All settings	**Advanced Threat Scan Engine** is enabled automatically in Trend Micro Email Security.
Policy > **Internal Addresses**	All settings	IMSS or IMSVA uses the **Internal Addresses** menu to determine mail traffic direction in policy configuration. This is unnecessary in Trend Micro Email Security.
Policy > **Smart Protection**	All settings	**Smart Protection** is enabled automatically in Trend Micro Email Security.
Policy > **Encryption Settings**	All settings	These settings are designed for on-premise products. Trend Micro Email Security completes all encryption settings on the cloud server automatically.

Navigation in IMSS or IMSVA	Settings	Remarks
Sender Filtering > **Overview**	All settings	Trend Micro Email Security provides block traffic details under **Logs** > **Mail Tracking**.
Sender Filtering > **Rules**	All settings	Trend Micro Email Security does not support this feature.
Sender Filtering > **Suspicious IP**	All settings	Trend Micro Email Security does not support this feature.
Reports	All settings	Trend Micro Email Security provides a more powerful report feature.
Logs	All settings	Trend Micro Email Security provides a more powerful log query feature.
Mail Areas & Queues	All settings	Trend Micro Email Security provides a more powerful quarantine query feature. Other mail queue management is not supported by Trend Micro Email Security.
Administration	All settings except DKIM signatures	These features provided by IMSS or IMSVA are mainly for on-premise products while Trend Micro Email Security is a cloud-based product.

Prerequisites for data migration

Before migrating data from IMSS 9.1 or IMSVA 9.1, make sure the following has been done:

- Add, provision, and verify the domains you want to manage through Trend Micro Email Security.

  For details, see *Adding a domain on page 4-4*.

- Synchronize with LDAP servers using the Directory Synchronization Tool if IMSS or IMSVA has enabled LDAP settings.

  The Directory Synchronization Tool is available under **Administration** > **Other Settings** > **Directory Management**.

  For details, refer to Directory Synchronization Tool User's Guide.

- Enable IMSS or IMSVA to support Trend Micro Email Security migration by doing the following:

  1. On the IMSS or IMSVA management console, go to **Administration** > **Updates** > **System & Applications** and check the build number.

     If the build number does not meet the following requirements, install the latest service pack and hotfix.

     - IMSS 9.1.0.1357 or later
     - IMSVA 9.1.0.2011 or later

  2. Enable the hidden key in the IMSS or IMSVA admin database by running the following SQL statements:

     Note

     IMSS and IMSVA use the same configuration file `imss.ini`.

     ```
     insert into tb_global_setting (section, name, value,
     inifile)

     values ('imp_exp', 'enable_ems_migrate', '1',
     'imss.ini');
     ```

- Export configuration files from the IMSS or IMSVA management console under **Administration** > **Import/Export**.

Migrating data to Trend Micro Email Security

Procedure

1. Go to **Administration** > **Other Settings** > **IMSS/IMSVA Migration Tool**.
2. Read the on-screen instructions, and click **Get Started**.
3. On the pop-up screen, click **Choose File...**, select the configuration file you exported, select **Overwrite** or **Merge**, and click **Next**.

   Trend Micro Email Security begins to create a migration task, analyze the configuration file, and generate a data analysis report.

   Note

   This process may take several minutes, depending on the size of the configuration file.

4. At Step 2 on the pop-up screen, view pre-migration check results to determine which settings will be migrated to Trend Micro Email Security and which will not.

   a. Select an option from the **Show** drop-down list to show the settings in a specific state.

      - **Not supported**: Settings in this state are not supported in Trend Micro Email Security and will not be migrated. If you need these settings, you have to add them in Trend Micro Email Security manually.
      - **Error**: There are some critical issues about the settings in this state, but the settings will still be migrated to Trend Micro Email Security. During migration, some improper settings may be removed or modified. The settings in Trend Micro Email Security may be unexpected after migration, and the corresponding policies will be disabled temporarily. You need to fix these error settings and enable the policies manually after migration.
      - **Warning**: There are some minor issues about the settings in this state, and the settings will be automatically handled by

Trend Micro Email Security. You only need to confirm these warning settings after migration.

- **Successful**: Settings in this state will be migrated to Trend Micro Email Security without any issue.

b. View the detailed description of the settings in the table.

c. Click **Download Report** to download the data analysis report.

d. (Optional) If the data analysis report contains too many error settings, click **Cancel**, modify the settings, and restart migration.

Clicking **Cancel** at this step will not import the settings into Trend Micro Email Security.

5. Click **Next** to proceed with the migration.

Trend Micro Email Security begins to analyze the configuration file, import settings in the configuration file, and generate a data migration report.

Note

This process may take several minutes, depending on the size of the configuration file.

6. At Step 3 on the pop-up screen, view the migration results to find which settings are migrated to Trend Micro Email Security and which are not.

a. Select an option from the **Show** drop-down list to show the settings in a specific state.

- **Not supported**: Settings in this state are not supported in Trend Micro Email Security and are not migrated. If you need these settings, you have to add them in Trend Micro Email Security manually.
- **Error**: There are some critical issues about the settings in this state, but the settings are still migrated to Trend Micro Email Security. During migration, some improper settings may be removed or modified. The settings in Trend Micro Email Security may be unexpected after migration, and the

corresponding policies are disabled temporarily. You need to fix these error settings and enable the policies manually after migration.

- **Warning**: There are some minor issues about the settings in this state, and the settings are automatically handled by Trend Micro Email Security. You only need to confirm these warning settings after migration.
- **Successful**: Settings in this state are migrated to Trend Micro Email Security without any issue.

b. View the detailed description of the settings in the table.

c. Click **Download Report** to download the data migration report.

7. Click **Finish**

Under **Inbound Protection** and **Outbound Protection**, you will find that the **Migration status** drop-down list and **Migration Status** column are added on the policy list screens. Deselect the **Show migration status** check box in the migration tool if you do not want Trend Micro Email Security to show the **Migration status** drop-down list and **Migration Status** column any more.

You still need to verify the migrated data after the migration. For details, see *Verifying data after migration on page 10-127*.

Verifying data after migration

To ensure your organization achieves effective email security protection, Trend Micro Email Security recommends you perform the following tasks after data migration:

Procedure

1. Verify migrated policy data under **Inbound Protection** and **Outbound Protection**.

a. Go to the following locations respectively:

- **Virus Scan**
- **Spam Filtering**
- **Correlated Intelligence** > **Correlated Intelligence Policy**
- **Content Filtering** > **Content Policy**
- **Data Loss Prevention** > **Data Loss Prevention (DLP) Policy**

Note

After migration, policy rules are categorized into the following types: virus scan, spam filtering, Correlated Intelligence, content filtering, and DLP.

b. Select **Error** or **Warning** from the **Migration status** drop-down list.

c. Follow the on-screen instructions in the **Migration Status** column to fix error settings or confirm warning settings and enable the corresponding policies.

d. Reorder policy rules.

You can manually reorder the policy rules in each domain after migration if they do not meet your requirements. For details, see *Reordering policy rules on page 6-9*.

2. Verify other migrated data.

a. Go to **Inbound Protection** > **Connection Filtering** > **IP Reputation** > **Settings** to verify email reputation settings.

b. Go to the following locations respectively to verify approved and blocked IP addresses:

- **Inbound Protection** > **Connection Filtering** > **IP Reputation** > **Approved IP Addresses**
- **Inbound Protection** > **Connection Filtering** > **IP Reputation** > **Blocked IP Addresses**

c. Go to **Inbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Verification** to verify the Global DKIM Enforcement rule.

d. Go to **Inbound Protection** > **Domain-based Authentication** > **Domain-based Message Authentication, Reporting and Conformance (DMARC)** to verify DMARC settings.

e. Go to **Inbound Protection** > **Spam Filtering** > **Time-of-Click Protection** to verify time-of-click protection settings.

f. Go to **Outbound Protection** > **Domain-based Authentication** > **DomainKeys Identified Mail (DKIM) Signing** to verify DKIM signature settings.

g. Go to **Administration** > **Policy Objects** to verify policy object settings.

Email Recovery

Enable Trend Micro Email Security to retain and restore emails that were previously marked for deletion.

Trend Micro Email Security provides Email Recovery to retain emails that were deleted due to policy rule matches. This allows for restoration of emails that were mistakenly deleted before they are permanently purged and become unrecoverable. With Email Recovery, Trend Micro Email Security helps ensure your business continuity and reduce the risk of data loss.

When enabled, Trend Micro Email Security retains deleted emails for 14 days and manages the recovery process. Automatic email recovery may take place in instances where certain conditions, such as system updates, lead to a higher number of false positives. In such cases, Trend Micro Email Security utilizes specialized tools to restore all affected emails. If you prefer not to have your email data retained in Trend Micro Email Security, disable this feature.

Important

Only Trend Micro Email Security can restore deleted emails. This functionality is not available at your discretion through the administrator console. If you wish to gain control over restoring emails, Trend Micro recommends that you change the action configured in your policies from **Delete** to **Quarantine**.

Procedure

1. Go to **Administration** > **Other Settings** > **Email Recovery**.
2. Enable or disable Email Recovery.
3. Click **Save**.

   Restored emails can be located in the mail tracking logs. In the **Mail Tracking Details** dialog of a restored email, the **Policies Evaluated** field indicates that the email was delivered by Trend Micro.

Appendix A

FAQs and instructions

TABLE A-1. Frequently Asked Questions (FAQs)

QUESTION	ANSWER
What is Trend Micro Email Security?	Trend Micro Email Security provides always-up-to-the-minute email security with no maintenance required by IT staff to stop spam, viruses and other malware before they reach your network. Trend Micro Email Security is a cloud service that can benefit any size organization. We provide the hardware, software, and messaging expertise to cleanse your email messages of spam, viruses, worms, Trojans, and phishing (identity theft) attacks. The cleaned email messages are sent directly to your MTA for final delivery to your end users. Trend Micro Email Security can also use LDAP directories to help prevent backscatter (or outscatter) spam and Directory Harvest Attacks (DHA).
What are the advantages of Trend Micro Email Security?	As a cloud service, Trend Micro Email Security can stop attacks before they get a chance to reach your network. In addition to stopping spam, viruses, worm, Trojans, and other malware, Trend Micro Email Security can protect your network from attacks that: • Attempt to block your Internet connection (Denial of Service) • Steal your email addresses for spammers (Directory Harvest Attacks)

Question	Answer
How can I upgrade?	Trend Micro Email Security is a cloud service and so there is no need to buy additional hardware or software. The service is managed by security professionals, relieving your IT staff of the burden of installing, maintaining, and fine-tuning a complex email security system.
How can I migrate configurations from the trial Trend Micro Email Security management console to the production management console after purchasing Smart Protection Complete with a full license?	Attach the Customer Licensing Portal account you created with the Trend Micro Email Security trial license to your Smart Protection Complete full license first. 1. Log on to Customer Licensing Portal (https://clp.trendmicro.com) using your account credentials. 2. Go to **My Products/Services** and click **Provide Key**. 3. On the **License Key** screen, type your registration key, not the activation code, in the **Provide your Activation Code or product key** text box, and then click **Continue**. 4. Select the check box and click **Continue** to finish the process. After you re-log on to the Trend Micro Email Security production management console, all configurations are migrated and your license is updated.
How much does the service cost?	Trend Micro Email Security is priced on a per user basis under an annual contract. The cost per user drops as the number of users increases. There is no set-up fee or additional support costs from Trend Micro. There may be a small fee (unlikely) associated with changing your MX record. Contact your web-hosting service to review their pricing policies.
Is Trend Micro Email Security confidential? Who reads my mail?	All messages are processed automatically and transparently. Many messages are rejected before they are even received based on the reputation of the IP that is attempting to send the message. Messages that are received are processed through a multi-layered spam and virus filtering system that does not include any human intervention. Messages are never stored unless your MTA becomes unavailable.

Question	Answer
What do I need in order to access the administrator console?	To use this service you only need to have an existing Internet gateway or workgroup email connection and a web browser for accessing the online reporting and administrator console. To access the console through Trend Micro Licensing Management Platform, you need the service web address and account information.
How do I get started using Trend Micro Email Security?	To get started using Trend Micro Email Security, do the following: 1. Submit account activation information 2. Log on to the Trend Micro Email Security administrator console 3. Provision a Trend Micro Business Account 4. Configure the domain you added and add additional domains if needed 5. Import user directories that will be applied by policies 6. Configure policies to design your organizational protection solution For details, see *Getting started with Trend Micro Email Security on page 2-1*.

Question	Answer
How do I redirect my mail exchanger record (MX record)?	Before redirecting your MX record to the service, make sure you have added and configured your domain to your Trend Micro Email Security. To redirect your MX record: 1. For details about adding an MX record for the Trend Micro Email Security server, see step 1 in *Configuring a domain on page 4-6*. 2. Check Trend Micro Email Security welcome email message, which contains the specific MX record information. 3. Do one of the following: • Manual configuration If you manage your own DNS, you can manually edit your MX record (this applies to self-managed, smaller accounts). • Through a support technician If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider's (ISP) help desk or your Domain Name Service (DNS) technician for assistance. If your DNS is managed by a third-party or ISP, either they can do this for you or they may have a simple Web interface allowing you to make the change yourself. It can take up to 48 hours for any changes to propagate throughout the system. After making the modifications to the MX record, Trend Micro Email Security becomes the point of entry of messages for your domain. After the DNS record modifications take effect (up to 48 hours), all inbound email traffic is routed through Trend Micro Email Security. **Tip** After the modifications take effect, test the message route by sending messages from another email service provider (for example, Yahoo! Mail or Gmail) to a recipient in your domain. If you receive the message from that email service provider, the MX record is configured correctly.

Question	Answer
Where can I locate the instruction to redirect the MX record to point to Trend Micro Email Security?	The MX record determines the message routing for all email messages sent to your domain. The Trend Micro Email Security welcome email message from Trend Micro specifically provides details about where to redirect your MX record.
How do I accept email messages from the service?	To ensure that you are able to receive email messages processed by the service: • Configure your firewall to accept traffic from Trend Micro Email Security IP addresses • Configure your MTA to accept transactions from these IP addresses
Can I try Trend Micro Email Security on a limited number of email addresses?	Yes. **Tip** Trend Micro recommends that you use a test domain for trial purposes. Doing so allows you to experience the service and test how it functions for different types of users.
Does Trend Micro Email Security store or archive email messages?	Trend Micro Email Security does not store or archive email messages by default. All messages are processed and immediately passed through to the customer's MTA. Messages are not spooled or stored in memory unless your MTA becomes unavailable. However, if you create a policy to quarantine messages (spam for example) these email messages will be stored at our data center for up to 30 days. With Email Continuity enabled by default, Trend Micro Email Security provides a standby email system that gives virtually uninterrupted use of email in the event of a mail server outage. If an outage occurs, Trend Micro Email Security will keep your incoming email messages for 10 days. Once your email server is back online within the 10-day period, these messages will be restored to your email server.

Question	Answer
How do I reset or resend an End User Console password?	When your users lost or cannot remember their password, they can go to the logon screen of the Trend Micro Email Security End User Console and click **Forgot your password** to reset their passwords. It is not necessary for you to reset end users' passwords.
What does the service do when my MTA is unavailable?	If your MTA becomes unavailable for whatever reason, your message stream is automatically queued for up to ten (10) days or until such time that your server comes back online. You should not lose any of your valuable email messages due to hardware or software failure, power outages, network failure or simple human error.
Where does outgoing mail go?	By default, your outbound email messages are handled directly by your own MTA and passed out to other networks as it is currently handled. However, with Trend Micro Email Security (full version) you can choose to redirect your outbound email traffic through Trend Micro Email Security services. Opting for Outbound Filtering: When you activate Trend Micro Email Security, you will be informed of what MTA to send your outbound messages to if you choose to utilize outbound filtering. For complete instructions on enabling outbound filtering, see *Configuring a domain on page 4-6*.
What happens when my license expires?	Immediately after your license expires, it will go through a grace period, wherein the service continues as expected. After the grace period, however, your service will be suspended and your data will be permanently deleted. To prevent unnecessary disruptions to your email service, please renew your license before it expires.
How does Trend Micro Email Security implement the Transport Layer Security (TLS) protocol?	Trend Micro Email Security is configured in Opportunistic Transport Layer Security (TLS) mode. In this mode, the MTA servers will initially check if the sending or receiving MTA can perform SMTP transaction in TLS mode. If so, the entire session and process will be done in TLS mode.

FAQs and instructions

TABLE A-2. Frequently Asked Questions (FAQs)

QUESTION	ANSWER
What is Trend Micro Email Security?	Trend Micro Email Security provides always-up-to-the-minute email security with no maintenance required by IT staff to stop spam, viruses and other malware before they reach your network. Trend Micro Email Security is a cloud service that can benefit any size organization. We provide the hardware, software, and messaging expertise to cleanse your email messages of spam, viruses, worms, Trojans, and phishing (identity theft) attacks. The cleaned email messages are sent directly to your MTA for final delivery to your end users. Trend Micro Email Security can also use LDAP directories to help prevent backscatter (or outscatter) spam and Directory Harvest Attacks (DHA).
What are the advantages of Trend Micro Email Security?	As a cloud service, Trend Micro Email Security can stop attacks before they get a chance to reach your network. In addition to stopping spam, viruses, worm, Trojans, and other malware, Trend Micro Email Security can protect your network from attacks that: • Attempt to block your Internet connection (Denial of Service) • Steal your email addresses for spammers (Directory Harvest Attacks)
How can I upgrade?	Trend Micro Email Security is a cloud service and so there is no need to buy additional hardware or software. The service is managed by security professionals, relieving your IT staff of the burden of installing, maintaining, and fine-tuning a complex email security system.

Question	Answer
How can I migrate configurations from the trial Trend Micro Email Security management console to the production management console after purchasing Smart Protection Complete with a full license?	Attach the Customer Licensing Portal account you created with the Trend Micro Email Security trial license to your Smart Protection Complete full license first. 1. Log on to Customer Licensing Portal (https://clp.trendmicro.com) using your account credentials. 2. Go to **My Products/Services** and click **Provide Key**. 3. On the **License Key** screen, type your registration key, not the activation code, in the **Provide your Activation Code or product key** text box, and then click **Continue**. 4. Select the check box and click **Continue** to finish the process. After you re-log on to the Trend Micro Email Security production management console, all configurations are migrated and your license is updated.
How much does the service cost?	Trend Micro Email Security is priced on a per user basis under an annual contract. The cost per user drops as the number of users increases. There is no set-up fee or additional support costs from Trend Micro. There may be a small fee (unlikely) associated with changing your MX record. Contact your web-hosting service to review their pricing policies.
Is Trend Micro Email Security confidential? Who reads my mail?	All messages are processed automatically and transparently. Many messages are rejected before they are even received based on the reputation of the IP that is attempting to send the message. Messages that are received are processed through a multi-layered spam and virus filtering system that does not include any human intervention. Messages are never stored unless your MTA becomes unavailable.
What do I need in order to access the administrator console?	To use this service you only need to have an existing Internet gateway or workgroup email connection and a web browser for accessing the online reporting and administrator console. To access the console through Trend Micro Licensing Management Platform, you need the service web address and account information.

Question	Answer
How do I get started using Trend Micro Email Security?	To get started using Trend Micro Email Security, do the following: 1. Submit account activation information 2. Log on to the Trend Micro Email Security administrator console 3. Provision a Trend Micro Business Account 4. Configure the domain you added and add additional domains if needed 5. Import user directories that will be applied by policies 6. Configure policies to design your organizational protection solution For details, see *Getting started with Trend Micro Email Security on page 2-1*.

Question	Answer
How do I redirect my mail exchanger record (MX record)?	Before redirecting your MX record to the service, make sure you have added and configured your domain to your Trend Micro Email Security. To redirect your MX record: 1. For details about adding an MX record for the Trend Micro Email Security server, see step 1 in *Configuring a domain on page 4-6*. 2. Check Trend Micro Email Security welcome email message, which contains the specific MX record information. 3. Do one of the following: • Manual configuration If you manage your own DNS, you can manually edit your MX record (this applies to self-managed, smaller accounts). • Through a support technician If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider's (ISP) help desk or your Domain Name Service (DNS) technician for assistance. If your DNS is managed by a third-party or ISP, either they can do this for you or they may have a simple Web interface allowing you to make the change yourself. It can take up to 48 hours for any changes to propagate throughout the system. After making the modifications to the MX record, Trend Micro Email Security becomes the point of entry of messages for your domain. After the DNS record modifications take effect (up to 48 hours), all inbound email traffic is routed through Trend Micro Email Security. **Tip** After the modifications take effect, test the message route by sending messages from another email service provider (for example, Yahoo! Mail or Gmail) to a recipient in your domain. If you receive the message from that email service provider, the MX record is configured correctly.

Question	Answer
Where can I locate the instruction to redirect the MX record to point to Trend Micro Email Security?	The MX record determines the message routing for all email messages sent to your domain. The Trend Micro Email Security welcome email message from Trend Micro specifically provides details about where to redirect your MX record.
How do I accept email messages from the service?	To ensure that you are able to receive email messages processed by the service: • Configure your firewall to accept traffic from Trend Micro Email Security IP addresses • Configure your MTA to accept transactions from these IP addresses
Can I try Trend Micro Email Security on a limited number of email addresses?	Yes. **Tip** Trend Micro recommends that you use a test domain for trial purposes. Doing so allows you to experience the service and test how it functions for different types of users.
Does Trend Micro Email Security store or archive email messages?	Trend Micro Email Security does not store or archive email messages by default. All messages are processed and immediately passed through to the customer's MTA. Messages are not spooled or stored in memory unless your MTA becomes unavailable. However, if you create a policy to quarantine messages (spam for example) these email messages will be stored at our data center for up to 30 days. With Email Continuity enabled by default, Trend Micro Email Security provides a standby email system that gives virtually uninterrupted use of email in the event of a mail server outage. If an outage occurs, Trend Micro Email Security will keep your incoming email messages for 10 days. Once your email server is back online within the 10-day period, these messages will be restored to your email server.

Question	Answer
How do I reset or resend an End User Console password?	When your users lost or cannot remember their password, they can go to the logon screen of the Trend Micro Email Security End User Console and click **Forgot your password** to reset their passwords. It is not necessary for you to reset end users' passwords.
What does the service do when my MTA is unavailable?	If your MTA becomes unavailable for whatever reason, your message stream is automatically queued for up to ten (10) days or until such time that your server comes back online. You should not lose any of your valuable email messages due to hardware or software failure, power outages, network failure or simple human error.
Where does outgoing mail go?	By default, your outbound email messages are handled directly by your own MTA and passed out to other networks as it is currently handled. However, with Trend Micro Email Security (full version) you can choose to redirect your outbound email traffic through Trend Micro Email Security services. Opting for Outbound Filtering: When you activate Trend Micro Email Security, you will be informed of what MTA to send your outbound messages to if you choose to utilize outbound filtering. For complete instructions on enabling outbound filtering, see *Configuring a domain on page 4-6*.
What happens when my license expires?	Immediately after your license expires, it will go through a grace period, wherein the service continues as expected. After the grace period, however, your service will be suspended and your data will be permanently deleted. To prevent unnecessary disruptions to your email service, please renew your license before it expires.
How does Trend Micro Email Security implement the Transport Layer Security (TLS) protocol?	Trend Micro Email Security is configured in Opportunistic Transport Layer Security (TLS) mode. In this mode, the MTA servers will initially check if the sending or receiving MTA can perform SMTP transaction in TLS mode. If so, the entire session and process will be done in TLS mode.

About mx records and Trend Micro Email Security

Important

Make sure the MX record is entered exactly as provided in the Trend Micro Email Security welcome email message.

An MX record (DNS mail exchanger host record) determines the message routing for all messages sent to a domain. To route messages destined for your domain through the Trend Micro Email Security MTA, you must point your MX record to the fully qualified domain name (FQDN) provided in the welcome email message that Trend Micro sent you after you registered.

To disable Trend Micro Email Security, point your MX record to route all inbound SMTP traffic to your own mail server.

If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider or your DNS technician.

The following external links to MX record configuration help pages are provided for your convenience:

- GoDaddy

  http://support.godaddy.com/help/article/680/managing-dns-for-your-domain-names

- Network Solutions

  http://www.networksolutions.com/support/mx-records-mail-servers-2/

- Enom

  http://www.enom.com/help/hostinghelp.asp?displaymenu=ok&hosthelp=9

- DreamHost

  http://wiki.dreamhost.com/MX_record

About mta-sts records for inbound protection

To use MTA-STS to protect SMTP connections sending emails to your domains, you need to add a DNS record and publish a policy for each of the domains. Optionally, you can add a TLS reporting DNS record for each domain to receive reports from TLS peers protected by MTA-STS.

- The following is an example of the DNS record for MTA-STS:

```
_mta-sts.example.com. 3600 IN  TXT v=STSv1; id=20220831012215;
```

- The following is an example of the MTA-STS policy for the "example.com" domain, which needs to be published at `https://mta-sts.example.com/.well-known/mta-sts.txt`:

```
version: STSv1
mode: enforce
mx: *.in.tmes.trendmicro.com
mx: *.tmes.trendmicro.com
max_age: 604800
```

Note

Set **mx** based on your serving site.

SERVING SITE	MX VALUE
North America, Latin America and Asia Pacific	• *.in.tmes.trendmicro.com • *.tmes.trendmicro.com
Europe and Africa	• *.in.tmes.trendmicro.eu • *.tmes.trendmicro.eu
Australia and New Zealand	• *.in.tmes-anz.trendmicro.com • *.tmes-anz.trendmicro.com
Japan	• *.in.tmems-jp.trendmicro.com • *.tmems-jp.trendmicro.com
Singapore	• *.in.tmes-sg.trendmicro.com • *.tmes-sg.trendmicro.com
India	• *.in.tmes-in.trendmicro.com • *.tmes-in.trendmicro.com
Middle East (UAE)	• *.in.tmes-uae.trendmicro.com • *.tmes-uae.trendmicro.com

- The following is an example of the DNS record for TLS reporting:

```
_smtp._tls.example.com. 3600 IN TXT
v=TLSRPTv1;rua=mailto:reports@example.com
```

Feature limits and capability restrictions

The following table outlines the limits on both inbound and outbound messages.

TABLE A-3. Message Limits

PER MESSAGE	LIMIT
Size	• Trend Micro Email Security Standard license: 50 MB • Trend Micro Email Security Advanced license: 150 MB
Number of recipients	• Inbound message: 500 recipients • Outbound message: 500 recipients

The following table details the limits on End User Console settings.

TABLE A-4. End User Console Limits

PER SEAT	LIMIT
Approved sender list entries	500 entries
Blocked sender list entries	500 entries
Retention period for quarantined messages	30 days

The following table shows message retention information.

TABLE A-5. Retention Schedule

ITEM	RETENTION PERIOD
Quarantined email messages (all regions)	30 days
Message tracking information	90 days
Message queue when customer MTA is unavailable	Up to 10 days

Viewing your service level agreement

Trend Micro provides a Service Level Agreement (SLA) for Trend Micro Email Security that is intended to help your organization receive secure, uninterrupted email service.

The Service Level Agreement covers availability, latency, spam blocking, false positives, antivirus, and support. Specific service-level guarantees are

included in the most current version of the Trend Micro Email Security Service Level Agreement, which you can view or download from this screen.

Important

Provisions of the Service Level Agreement may vary among regions, so be sure to select your region and language when using this screen. Trend Micro reserves the right to modify the service at any time without prior notice. The current version of the Trend Micro Email Security service level agreement is available for review by paid customers and by customers conducting a trial.

To view the Service Level Agreement for your region:

Procedure

1. In the Trend Micro Email Security administrator console, click the **Resource Center** icon in the bottom left corner.
2. Click **Service Level Agreement**.

   The **Service Level Agreement** screen appears.
3. From the drop-down list, select your language/region.

   Tip

   Disable any pop-up blockers for your browser in order to download the Service Level Agreement.

   Trend Micro Email Security displays an Adobe Reader (PDF) document of the Service Level Agreement for the language and region that you selected.

Appendix B

Technical support

Learn about the following topics:

Contacting support

Depending on how you subscribed to your Trend Micro SaaS offering, the method of obtaining additional assistance differs. Refer to the following table to better understand how to contact your support representative.

Purchase Channel	Contact Method
Trend Micro direct purchase	Use the online Support Portal to file a case with Trend Micro support representatives. For more information, see *Using the support portal on page B-2*.
Service Provider offering	Contact your service provider directly if you have questions about the service or are experiencing problems. Service Providers have more information about your specific environment and may be able to address your concerns quickly. Most product consoles include a support link that should provide the necessary contact information.

Using the support portal

The Trend Micro Business Success Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://success.trendmicro.com/.
2. Click the search icon () to search for available solutions or keywords.
3. Click the **All Products** dropdown menu and select your product.
4. If no solution is found, click **Contact Support** and select the type of support needed.

Tip

Alternatively, you can file a support case by logging in to your MySupport account and clicking **New Case**.

Speeding up the support call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending suspicious content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://servicecentral.trendmicro.com/en-us/ers/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/en-US/solution/KA-0001177

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/en-US/solution/KA-0002449

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Troubleshooting resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Threat encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Download center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

https://docs.trendmicro.com/en-us/survey.aspx

Index

T

W

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736

www.trendmicro.com

Item Code: APEM09974/250113