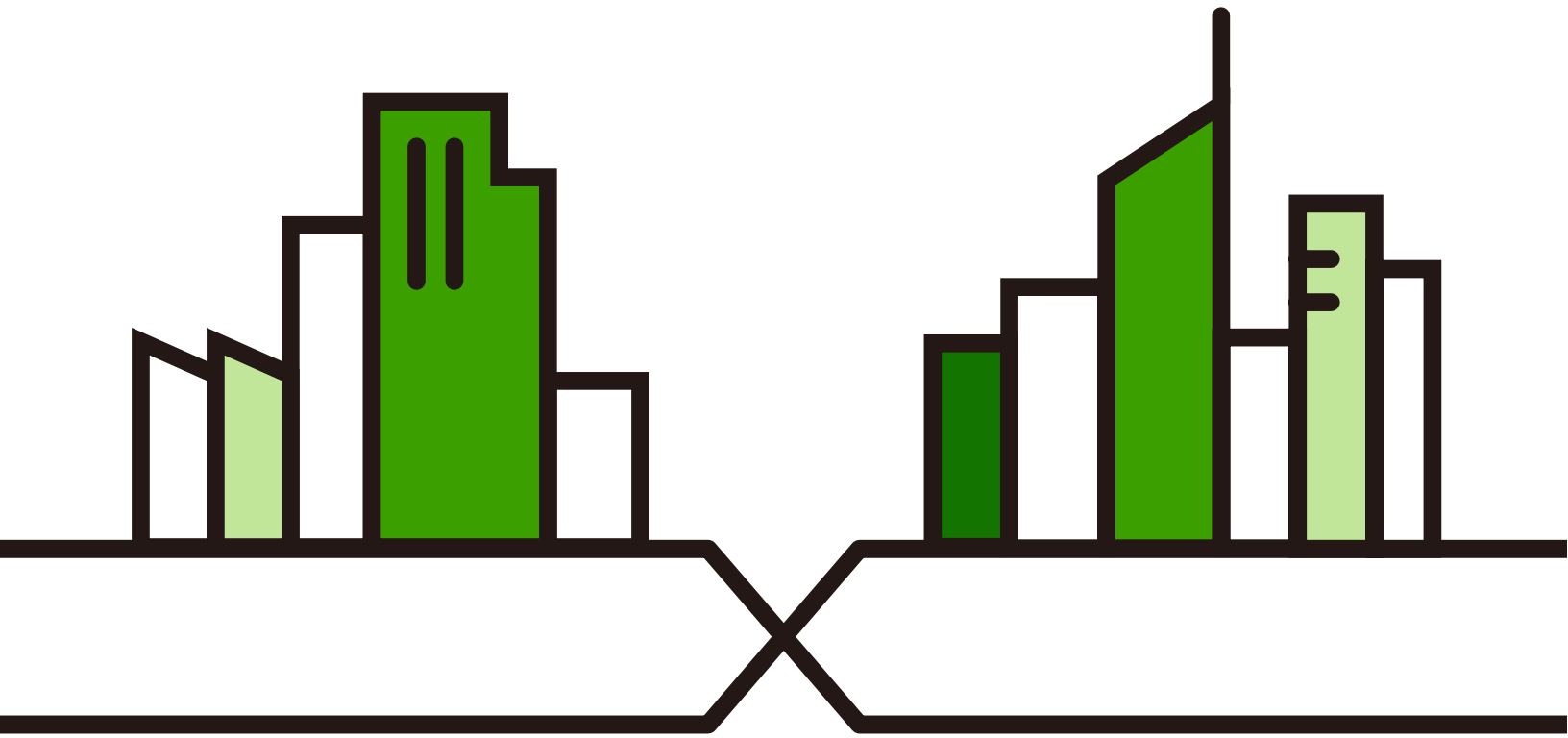
ZYXEL
NETWORKS

User's Guide

Cloud Email Security

Default Login Details	
URL	Supplied by Zyxel
User Name	Your myZyxel Email Address
Password	Supplied by Zyxel

Version 1.0 Edition 1, 9/2021



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in release versions or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

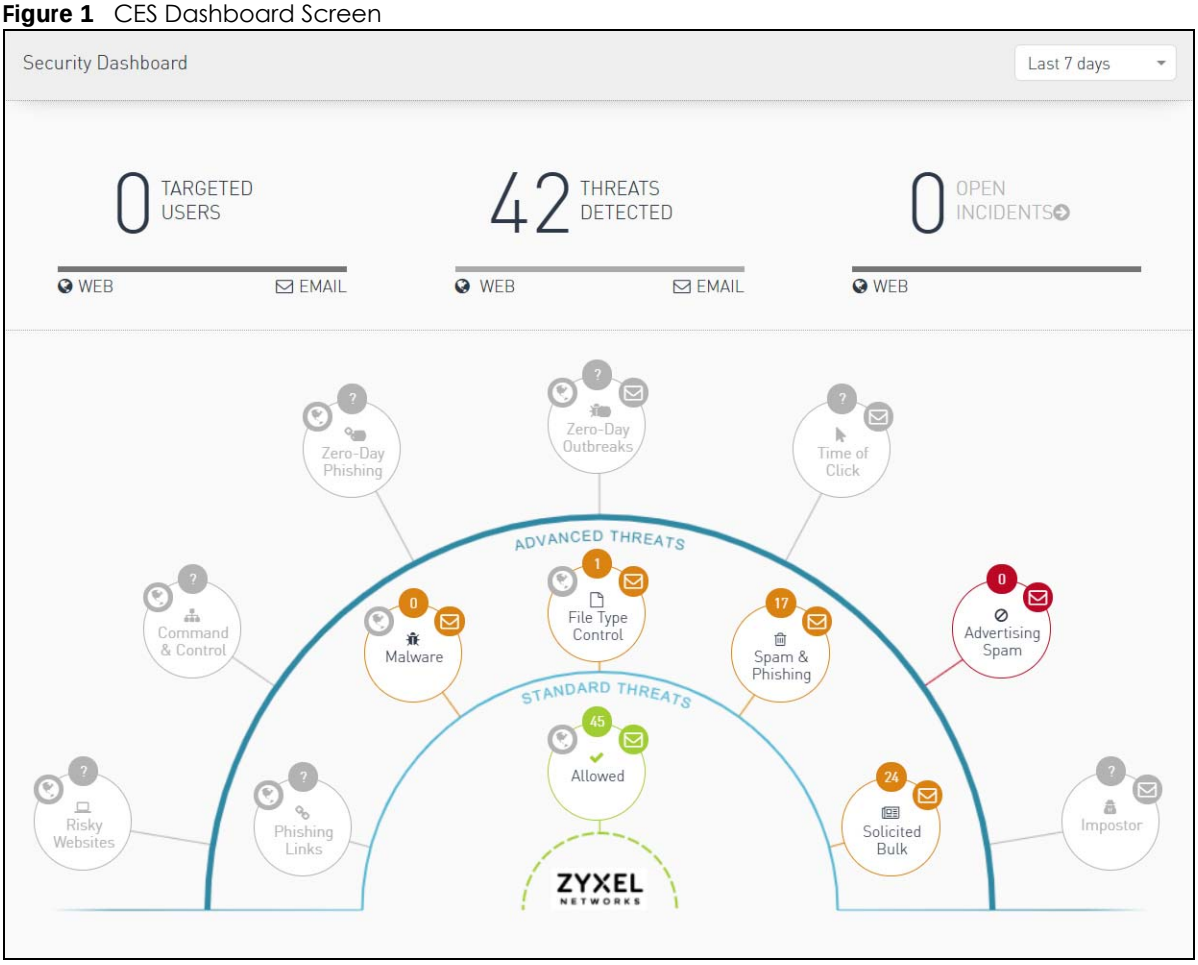
CHAPTER 1
Introduction

1.1 Overview

Cloud Email Security (CES) is a cloud-based security product that allows you to scan incoming emails for disallowed content. CES offers benefits and features such as:

- Automatically scan emails before they are arrive at your mail servers.
- Quarantine emails containing malicious content such as malware, phishing, or spam.
- Block emails that do not follow your company's email usage policies, such as emails with video attachments or blank subjects.
- View reports and receive notifications regarding scanned emails.

Figure 1 CES Dashboard Screen



Compared to the security features in the ZyWALL USGFLEX / ATP series, CES offers the following benefits:

- Scan incoming mail when your mail servers are cloud-based rather than on the premises.

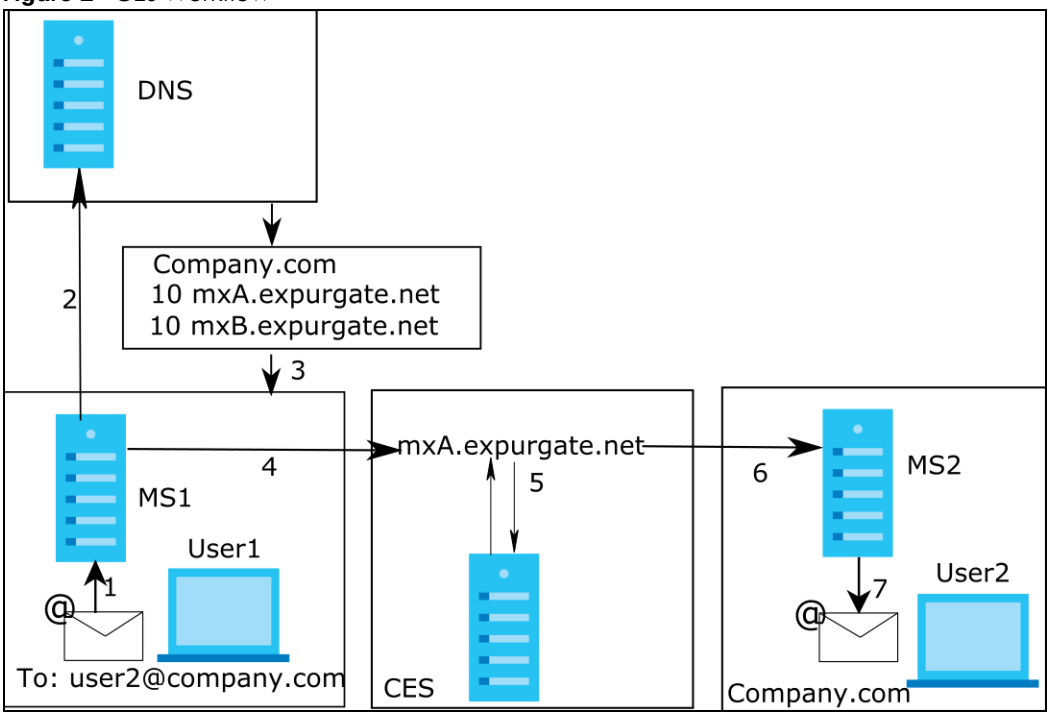
- Scan emails when your mail server is using encrypted SMTP (SMTP/TLS, SMTP/Start TLS).

1.2 CES Workflow

The following describes the workflow of the CES scanning process, using example domain company.com.

Note: The domain administrators have already configured the MX records for company.com to point to CES.

Figure 2 CES Workflow



1 User 1 in organization ABC sends an email to user2@company.com.

2 Organization ABC's mail server does a DNS lookup of the MX records for company.com.

3 The MX records of company.com point to CES. Organization ABC's mail server receives the results of the DNS lookup.

4 Organization ABC's mail server sends the email to CES.

5 CES checks the email according to the security policies configured for address user2@company.com.

6 If the incoming email passes the check, CES delivers the email to the company.com mail server.

1.3 Licensing

CES requires a license which is registered at myZyxel.

License types available at the time of writing are as follows.

Table 1 CES License Types

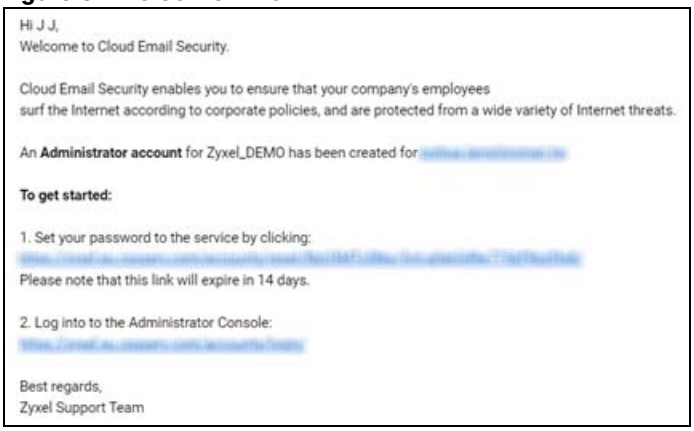
TYPE	DETAILS	VALIDITY PERIOD	NUMBER OF USERS
Trial	• Anti-Malware • Anti-Spam • Quarantine • Message Filtering • Malware Outbreak Protection.	1 month	5
Email Security Standard		3 months	5
			10
			25
			50

When registering a license, you must decide on the following:

- Organization name. This is the name of your account, and cannot be changed later.
- Number of users. This determines the maximum number of email addresses that are protected from security threats by CES. You can have unlimited email addresses in your email domain, but email addresses that are not associated with a CES user account are not scanned.

After creating an organization in myZyxel, you will receive a welcome email containing the URL that your organization must log into.

Figure 3 Welcome Email


Hi J J,
Welcome to Cloud Email Security.

Cloud Email Security enables you to ensure that your company's employees
surf the Internet according to corporate policies, and are protected from a wide variety of Internet threats.

An **Administrator account** for Zyxel_DEMO has been created for

To get started:

1. Set your password to the service by clicking:

Please note that this link will expire in 14 days.

2. Log into to the Administrator Console:

Best regards,
Zyxel Support Team

Note: If you later decide you want to add additional users, please contact customer support.

1.4 Getting Started

Follow these steps to start using CES. At the time of writing, the CES mail servers are:

- mxA.expurgate.net
- mxB.expurgate.net

1 Sign into CES as an administrator.
For details, see Section 1.4.1 on page 6.

2 Configure security settings in a policy set.
For details on modifying the default policy sets, see Section 3.2.1 on page 13.
For details on creating a new policy set, see Section 3.2.1.1 on page 13.

3 Add users to CES.
To import users from Active Directory (AD), see Section 6.3.2 on page 47.
To manually create a user, see Section 6.3.3 on page 48.

4 Optional: Organize users into groups.
To import groups from Active Directory (AD), see Section 6.3.2 on page 47.
To manually create a group, see Section 6.3.4 on page 48.

5 Apply a policy set to a set of users or groups using a rule.
For details on creating a rule, see Section 3.3.2 on page 18.

6 Ensure that your domain's mail servers accepts incoming SMTP and/or SMTP/TLS traffic from the CES mail servers.

7 Configure the CES gateway settings so that it forwards scanned emails to your domain's mail servers. To configure settings, see Section 6.4 on page 49. Wait until the **Status** changes from **Pending** to a check mark.

8 Modify your domain's MX records so that they point to the Cloud Email Security servers.
To avoid the possibility of emails not being delivered, we recommend modifying your MX records in stages:

8a Modify your domain's MX records so that they contain both the CES mail servers and your domain's mail servers. Give the CES mail servers a higher priority. Example:

```
10 mxa.expurgate.net
10 mxb.expurgate.net
20 mail1.zyyxel.com.tw
20 mail2.zyyxel.com.tw
```

8b Monitor CES for 1 to 2 weeks, to ensure that it is scanning and delivering mail correctly.

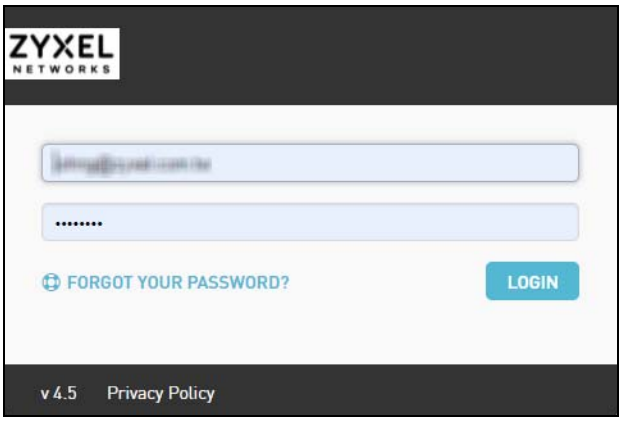
8c When you have confirmed the configuration is working correctly, remove your domain's mail servers from your domain's MX records.

9 Configure your domain's mail servers to only accept emails from the CES mail servers. This prevents malicious mail servers from bypassing CES and sending emails directly to your users.

1.4.1 Signing into CES

Follow the steps below to sign into CES.

1 Open the URL from the welcome email in a web browser.
A login page is displayed.



2 Enter your CES username and password, and then click **LOGIN**. Your username is the same as your email address. You can set your password by clicking on the password in the welcome email.

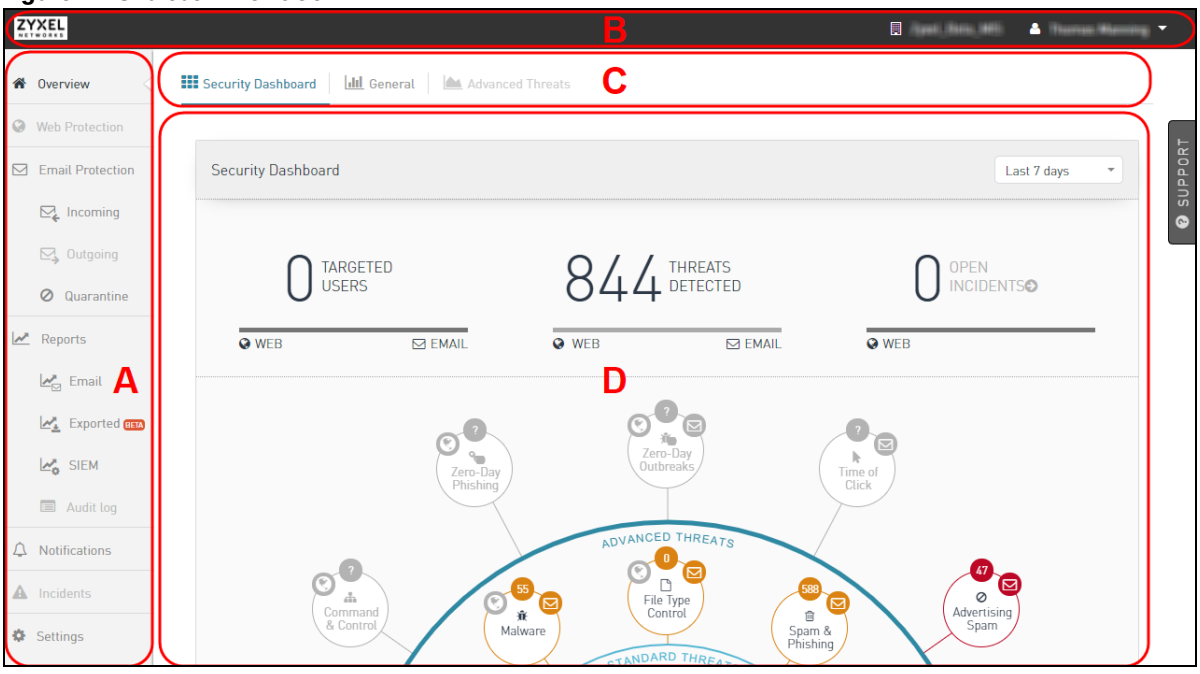
3 If you need to reset your password, click **FORGOT YOUR PASSWORD?** and then follow the instructions.

1.5 The CES User Interface

The following section describes the web user interface (UI) for Cloud Email Security.

Note: Certain Cloud Email Security features are not available for use. These features appear in the UI, but are inactive and cannot be clicked.

Figure 4 CES User Interface



The following describes the labels in this screenshot.

Table 2 CES User Interface

LABEL	DESCRIPTION
A	Navigation menu
B	Title bar
C	Tab bar
D	Main window

1.5.1 Navigation Menu

The following describes all available features in the navigation menu.

Table 3 CES: Navigation Menu

LABEL	DESCRIPTION
Overview	View a summary of scanned emails and detected security threats in the past 24 hours, 7 days, 30 days, or 90 days.
Email Protection	Configure email protection settings. As the time of writing, clicking this menu items redirects you to the **Incoming** menu.
Incoming	Configure email protection settings, including policy sets and rules, for incoming emails.
Quarantine	View, delete, or release emails that have been scanned and quarantined due to email policy sets.
Reports	Create and view reports on email detection.
Email	View detailed reports on scanned emails and detected security threats in the past 24 hours, 7 days, 14 days, or custom time period
Exported	View and re-download reports that were exported on the **Email** screen.
SIEM	Configure API access to email report data.This allows you to integrate CES with your existing Security Information and Event Management (SIEM) architecture.
Audit Log	View changes made to CES settings by administrators.
Notifications	View notifications issued by CES.
Settings	Configure general CES settings, such as the address of your network's mail servers.

1.5.2 Title Bar

The following describes all available features in the title bar.

Table 4 CES: Title Bar

LABEL	DESCRIPTION
	This is your company's logo. To customize the logo, go to **Settings > Account > Branding > Company Logo**.
	This is the name of the organization currently being managed. To manage a different organization, go to **Account > Switch organization**.
	This is the name of your user account. Click this to view account options.

Table 4 CES: Title Bar (continued)

LABEL	DESCRIPTION
Account Info	Click this to view information about your account at **Settings > Account > Account Information**.
Help	Click this to open the Zyxel documentation repository.
Switch organization	If your user account is an administrator in two or more CES organizations, then click this to manage a different organization, i
Change password	Click this to change your CES login password. The password must be at least 8 characters.
Logout	Click this to log out of CES.
Notifications	View notifications issued by CES.
Settings	Configure general CES settings, such as the address of your network's mail servers.

CHAPTER 2
Overview

2.1 Overview

The **Overview** screens allow you to view a summary of scanned emails and detected security threats.

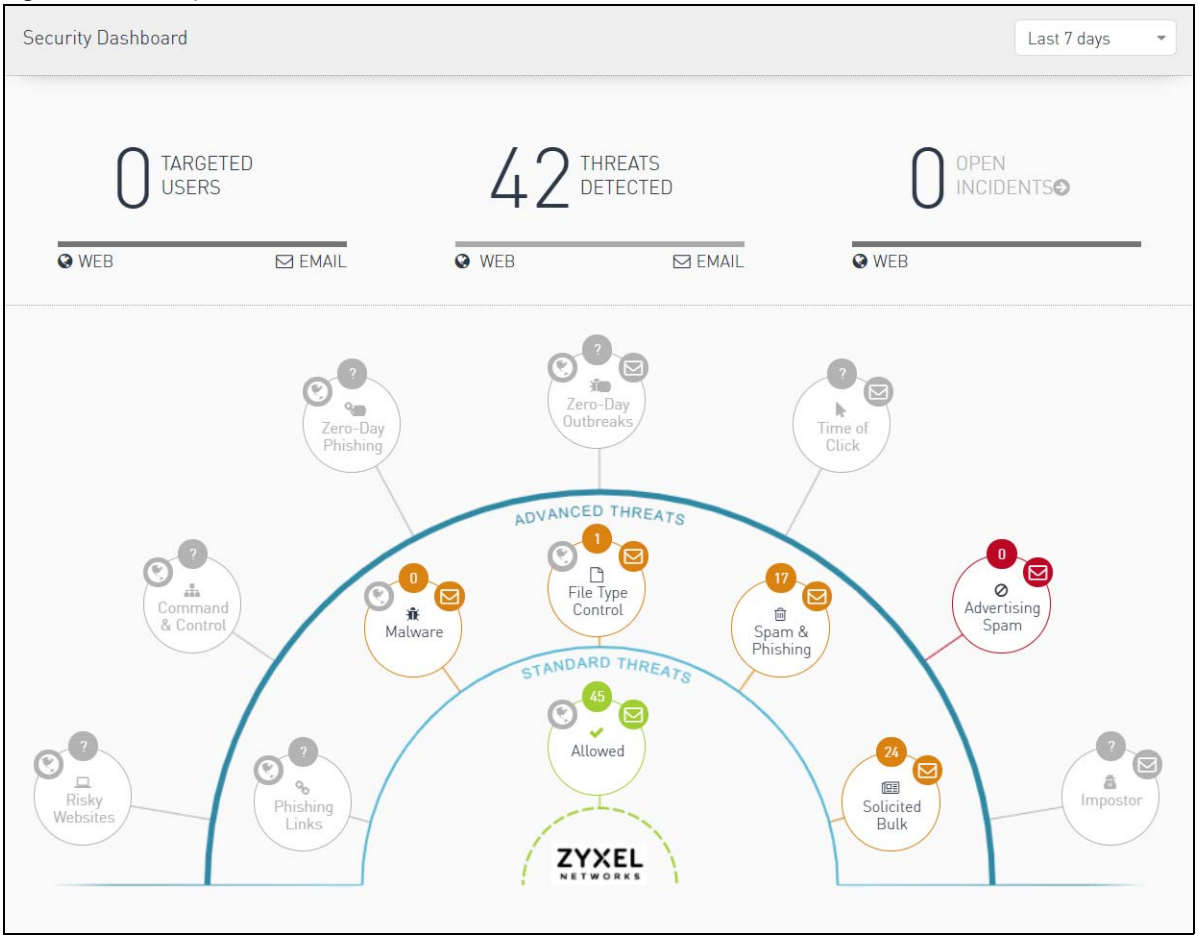
2.1.1 What You Can Do in this Chapter

Use the **Security Dashboard** screen (see Section 2.2 on page 10) to view a summary of scanned emails and detected security threats from the past 24 hours, 7 days, 30 days, or 90 days.

2.2 Security Dashboard Screen

The **Security Dashboard** screen allows you to view a summary of scanned emails and detected security threats from the past 24 hours, 7 days, 30 days, or 90 days.

Figure 5 Security Dashboard Screen



The following table describes the labels on this screen.

Table 5 CES: Security Dashboard Screen

LABEL	DESCRIPTION
Last X hours/Days	Click this to change the time period for all fields on this screen. Choices are: 24 hours, 7 days, 30 days, 90 days.
Targeted Users	This shows the number of users that have had malicious emails sent to them over the specified time period.
Threats Detected	This shows the total number of malicious emails detected by CES over the specified time period.
Open Incidents	This shows the number of open security incidents. A security incident is a potential malware infection in your network.
Advanced Threats/ Standard Threats	These sections show the total number of emails from each of the following that were detected by CES within the specified time period. Note: Only categories with an email icon are supported by CES.
Zero-Day Outbreaks	The email contained a file attachment or URL that did not match any known malware signature. However, the CES threat intelligence engine scanned and classified the file or URL as malware.
Advertising Spam	The email was classified as a semi-legitimate or unsolicited email sent to a large number of users. For example, marketing emails.

Table 5 CES: Security Dashboard Screen (continued)

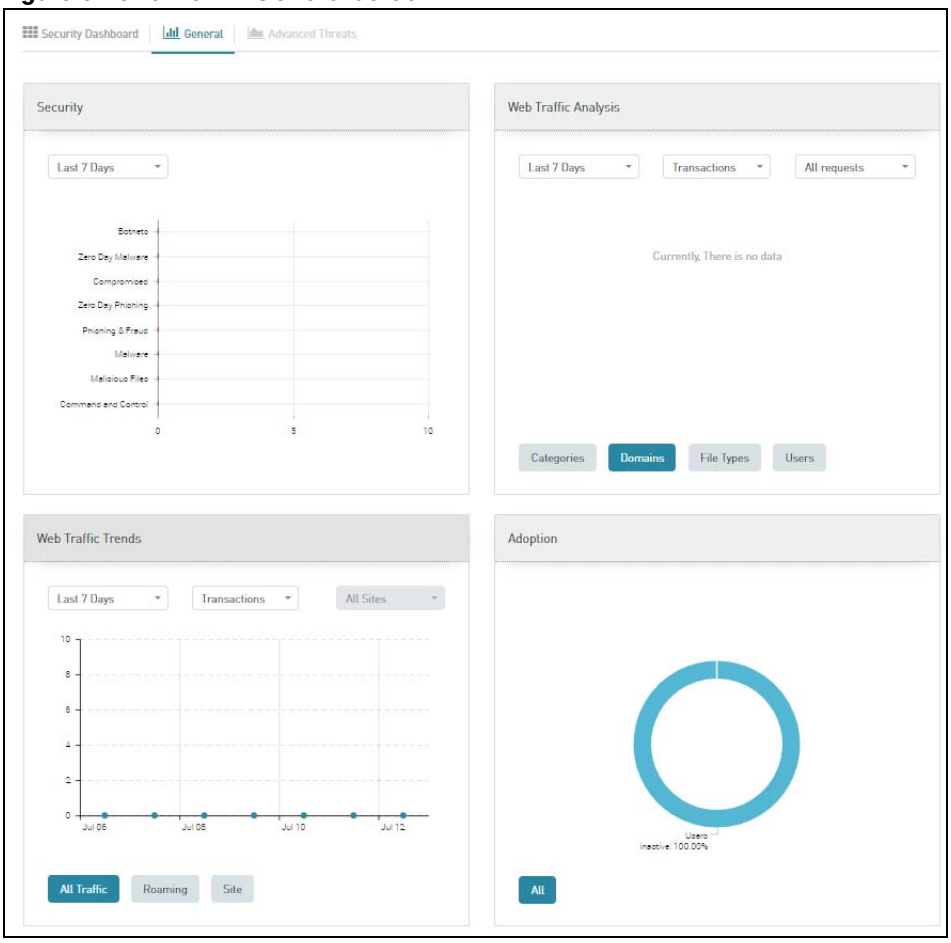
LABEL	DESCRIPTION
Impostor	The email was not from the specified sender's domain, detected using Sender Policy Framework (SPF).
Malware	The email contained a file attachment or URL that matched a known malware signature.
File Type Control	The email contained an file attachment that is disallowed according to the File Type Control filter.
Spam & Phishing	The email was classified as unwanted advertising (spam), or an email that tricks the receiver into sending confidential information (phishing).
Solicited Bulk	The email was classified as a solicited email sent to a large number of users, for example newsletters or messages sent to a mailing list messages.
Allowed	The email was scanned and contained no threats.

2.3 General Screen

The General screen allows you to view a to view a graphical summary of web protection scanning and threats.

Note: At the time of writing, web protection is not available in CES.

Figure 6 Overview > General Screen



CHAPTER 3
Email Protection

3.1 Overview

The **Overview** screens allow you to view a summary of scanned emails and detected security threats.

3.1.1 What You Can Do in this Chapter

- Use the **Incoming Email** screen (see Section 3.2 on page 13) to configure policy sets for incoming emails.
- Use the **Rules** screen (see Section 3.3 on page 17) to create and configure rules.
- Use the **Quarantine** screen (see Section 3.3 on page 17) to view and manage quarantined emails.

3.2 Incoming Email Protection

The Incoming email Protection screens allows you to configure policy sets for incoming emails.

3.2.1 Policy Sets

A policy set is a set of security settings that are applied when CES scans incoming emails. You can create a new policy set, or edit one of the following default policy sets.

Table 6 Default Policy Sets

POLICY SET	DESCRIPTION
Security	The policy set rejects emails classified as malware.
Spam protection	The policy set rejects emails classified as malware, spam, phishing, or unsolicited bulk emails.
Productivity	The policy set blocks emails classified as malware, spam, phishing, unsolicited bulk emails, or solicited bulk emails.

3.2.1.1 Creating a Policy Set

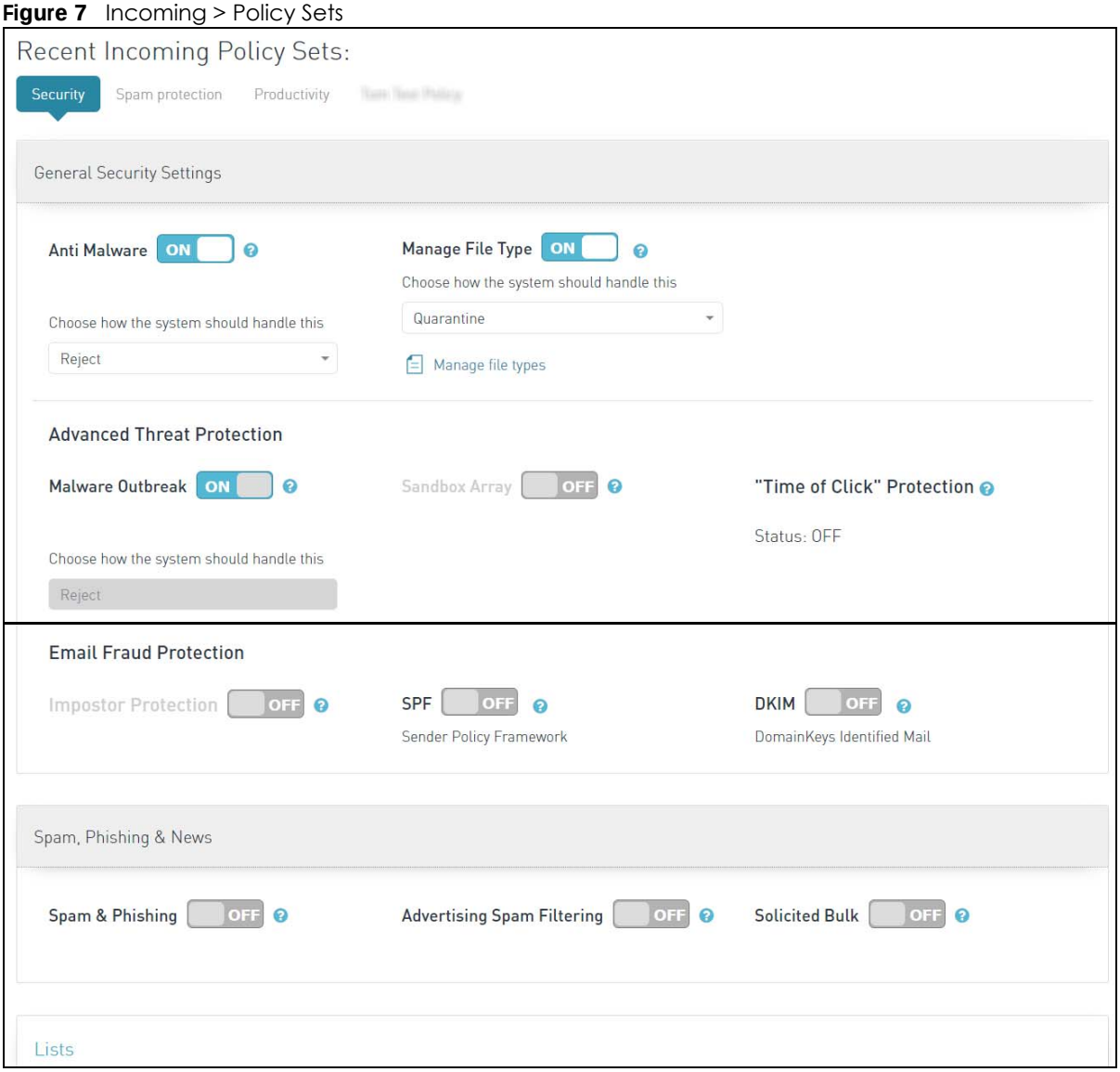
Follow the steps below to create a new policy set.

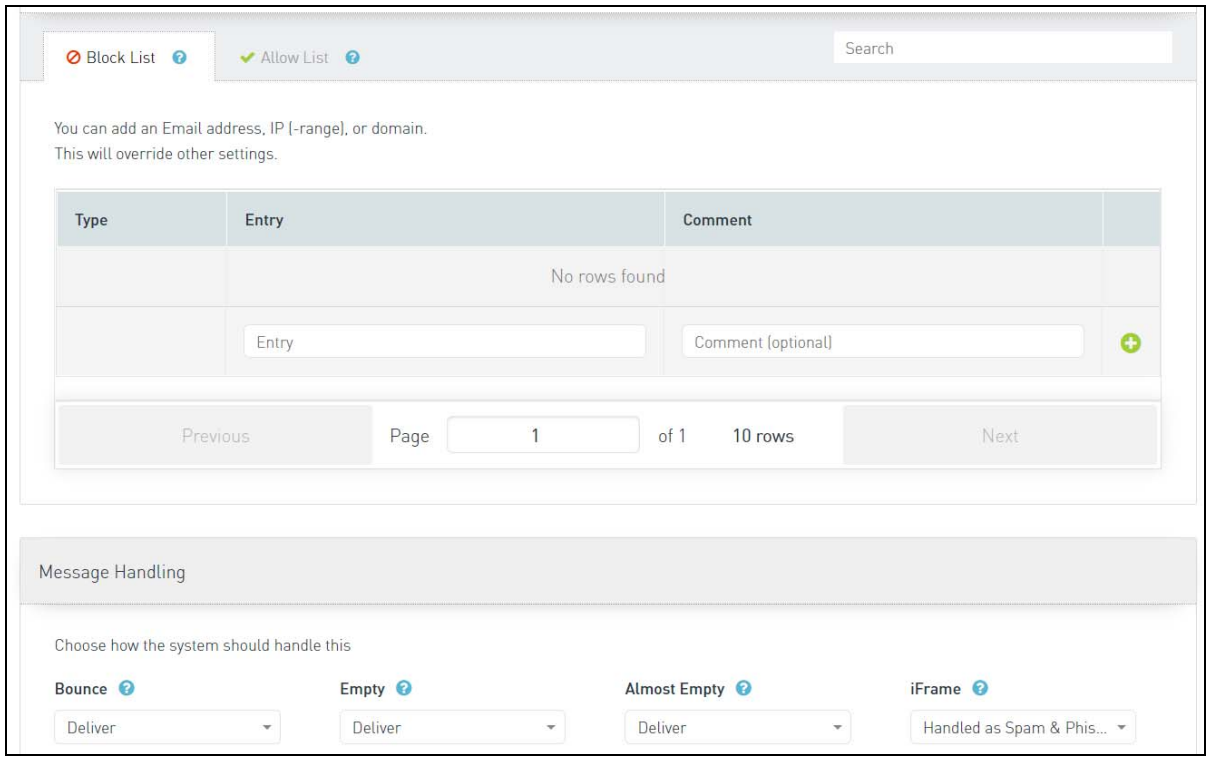
1. Click **Email Protection > Incoming > Policy Sets**.
2. At the bottom of the screen, click **+ ADD POLICY SET**.
   The **Add POLICY** window opens.
3. Enter a name for the policy set. The name can be 1–50 characters, and may consist of any combination of letters, numbers, special characters, or Unicode characters.
4. Click **ADD**.

3.2.1.2 Policy Sets Screen

This screen allows you to create and configure policy sets.

Figure 7 Incoming > Policy Sets





The following table describes the labels on this screen.

Table 7 Incoming > Policy Sets

LABEL	DESCRIPTION
Recent Incoming Policy Sets	This shows all policy sets in the current organization. Click on a policy set to configure the policy's settings.
Choose how the system should handle this	For each Policy Set setting, you can action CES takes when a match is detected. Select one of the following actions: • **Reject**: A delivery failed message is sent to the sender. CES sends the email to the recipient's spam or trash folder. • **Quarantine**: Send the email to the CES quarantine folder. The recipient receives a notification email asking them to review the quarantined email. For details, see Section 3.4 on page 19. Note: Quarantine must be enabled at **Settings > Email Services**. • **Tag and Deliver**: CES rewrites the email's subject line, and then sends the email to the recipient. You can use the following variables in the new subject line: %u: The recipient's CES username. %d: The recipient's email address domain name. %t: The email classification, such as "Clean", "Spam", or "Bulk". %s: The email's original subject line Example 1: "[%t] %s" with spam email "Download our app today!" results in "[SPAM] Download our app today!". • **Forward to**: Send the email to the specified address instead of the original recipient. • **Remove Attachment:** Remove the email's attachments and then send the email to the recipient. Each attachment is replaced with a text file containing the original filename and reason that the file was blocked.
General Security Settings	
Anti Malware	Click this to scan URLs and file attachments in the email for content that matches a known malware signature.

Table 7 Incoming > Policy Sets (continued)

LABEL	DESCRIPTION
Manage File Type	Click this to match emails with attachments of a specific file type. To choose the matched file types, click **Manage file types**.
Malware Outbreak	Click this to scan URLs and file attachments in the email using the CES threat intelligence engine. This engine detects new malware that does not match any known malware signatures.
SPF	Click this to enable Sender Policy Framework (SPF) checking. SPF is a framework for detecting forged email sender addresses. With SPF, each domain has a list of IP addresses of mail servers which are allowed to send or relay mail for the domain. This list is attached to the domain's DNS record. After enabling SPF, choose from the following two scanning options: • **SPF for all sender domains**: CES scans every email using SPF. If the domain of the sender address does not have an SPF record, then the mail is automatically passed and delivered to the recipient. • **SPF for selected sender domains**: CES scans an email only if the domain of the sender address is on the list of **Domains to be Verified**. If the domain of the sender address is not on the list or does not have an SPF record, then the mail is automatically passed and delivered to the recipient.
DKIM	Click this to enable Domain Keys Identified Mail (DKIM) checking. DKIM is a framework for detecting forged email sender addresses. With DKIM, the sending mail server adds an encrypted DKIM signature to the header of an email. The receiving mail server can verify that the email is from the sender's domain by validating the signature using a public encryption key. This encryption key is attached to the sending domain's DNS record. After enabling DKIM: • If the domain of the sender address has a public DKIM encryption key but the email does not have a matching DKIM signature, then CES flags the email as malicious and performs the specified action. • If the domain of the sender address does not a public DKIM encryption key, then the mail is automatically passed and delivered to the recipient.
Spam, Phishing, & News	
Spam & Phishing	Click this to match emails classified as unsolicited commercial mail (spam), or emails that tricks the receiver into sending confidential information (phishing).
Advertising Spam Filtering	Click this to match emails classified as a semi-legitimate or unsolicited email sent to a large number of users. For example, marketing emails.
Solicited Bulk	Click this to match emails classified as solicited mail sent to a large number of users. For example, newsletters or messages to a mailing list.
Lists	
Block List	Create a list of email addresses, server IP addresses, or domains to be blocked. The block list overrides all other settings in the policy set except for the allow list. You can block emails by adding any of the following information: • IPv4 address of the sending mail server. For example, 123.456.789.10. • IPv4 range of the sending mail server, in CIDR format. For example: 123.456.789.1/24. • Domain of the sender. For example: domain.com or sub.domain.com. To also block sub domains, add *, for example: *.domain.com. • Specific email address. For example, user@domain.com.

Table 7 Incoming > Policy Sets (continued)

LABEL	DESCRIPTION
Allow List	Create a list of email addresses, serve IP addresses, or domains to be allowed. CES passes and delivers emails that match any information on the list. The allows list overrides all settings in the policy set and block list, except for malware settings. You can allow emails by adding any of the following information: • IPv4 address of the sending mail server. For example, 123.456.789.10. • IPv4 range of the sending mail server, in CIDR format. For example: 123.456.789.1/24. • Domain of the sender. For example: domain.com or sub.domain.com. To also block sub domains, add *, for example: *.domain.com. • Specific email address. For example, user@domain.com. Note: If **Policy Set > General Security Settings > Anti Malware** is enabled, then the following classifications of email will be rejected even if they match an entry on the allow list: Dangerous Dangerous Virus Dangerous Virus Outbreak For details on email classifications, see Section 4.2.1 on page 25.
Message Handling	Select how CES handles specific types of email messages. Choose from the following actions: • **Deliver**: CES sends the email to the recipient. • **Handle as Spam & Phishing**: CES applies the action set in this policy set under **Spam, Phishing, & News > Spam & Phishing**. If **Spam & Phishing** is disabled, then no action is taken and CES sends the email to the recipient.
Bounce	Select how this policy set handles bounce emails. A bounce email is an email containing a notification that an email previously sent from your domain was not delivered.
Empty	Select how this policy set handles incoming emails that have no text in the subject line and email body.
Almost Empty	Select how this policy set handles incoming emails that have a subject line but no text in the body.
iFrame	Select how this policy set handles incoming emails that contain an HTML iFrame element. An iFrame is an HTML element that may contain a website, image, video file, audio file, or script.

3.3 Rules

A rule applies a policy set to a specific set of users or groups.

3.3.1 Rule Priority

You can create multiple rules, each with an order number. If multiple rules apply to a user, then when an email arrives for the user then CES applies the rule with the lowest order number, then the rule with the next lowest order number, and so on. If any rule applies an action to the email, then no further rules are applied to the email.

For example, you create the following rules:

Table 8 Rules Screen

ORDER	RECIPIENTS	POLICY
1	User1	Policy Set 1 Manage File Types=ON File Type=All Images Action=Tag and Delivery
2	Everyone	Policy Set 2 Spam & Phishing=ON Action=Quarantine

If User1 receives an email with an image attachment, the email is tagged and then delivered and then rule 2 is not applied. This means that User1 can receive spam emails, as long as they have an image attached.

3.3.2 Creating a Rule

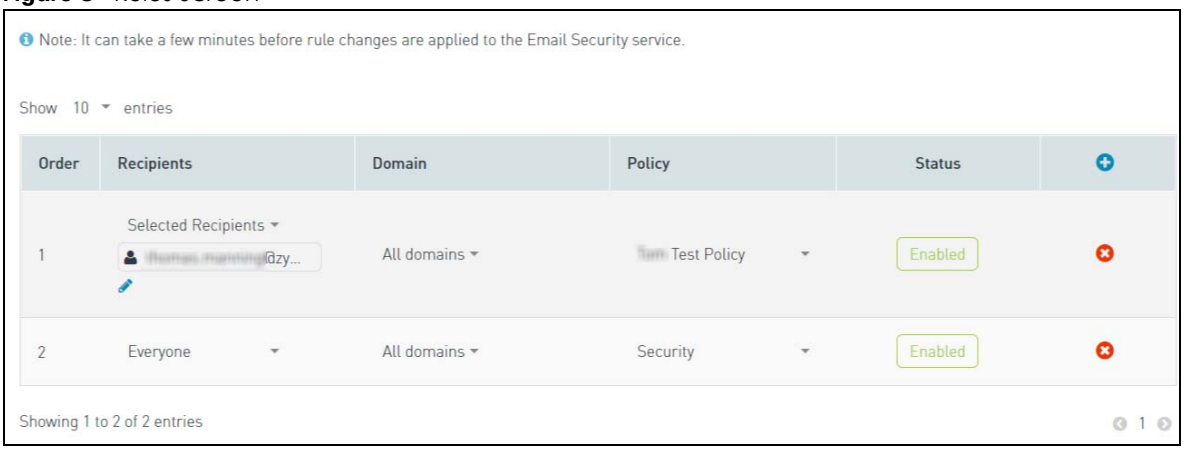
Follow the steps below to create a new rule.

1. Click **Email Protection > Incoming > Rules**.
2. Click 
   A new rule is added to row 1 of the table. The new rule has the following default settings:
   - **Recipients**: Everyone
   - **Domain**: All Domains
   - **Policy**: Security
3. Configure the **Recipients, Domain,** and **Policy** settings of the new rule by clicking on the values.
4. Drag the new rule to the correct priority position in the rules table.
5. At the bottom of the screen, click **Save**.
6. Wait 5 to 10 minutes for the new rule to take effect.

3.3.3 Rules Screen

This screen allows you to create and configure rules.

Figure 8 Rules Screen



The following table describes the labels on this screen.

Table 9 Rules Screen

LABEL	DESCRIPTION
Show X entries	Select how many rows to show in the list.
Order	This shows the priority of the rule. Drag rules up and down in the table to change their
Recipients	This shows who the rule applies to. This can be a set of users and groups, or **Everyone**. Click on the value to edit it.
Domain	This shows which email domain the rule applies to. This can be one domain, or **All Domains**.
Policy	This shows the policy set that is applied to the recipients.
Status	This shows whether the rule is enabled.
	Click this to create a new rule.
	Click this to delete a rule.

3.4 Quarantine

The quarantine folder is an isolated email folder used to temporarily store potentially malicious emails. When CES detects a malicious email, one of the actions it can take is to move the email to the isolated quarantine folder. An administrator can then log into CES, check the quarantine folder, and then decide whether to release or delete the quarantined email.

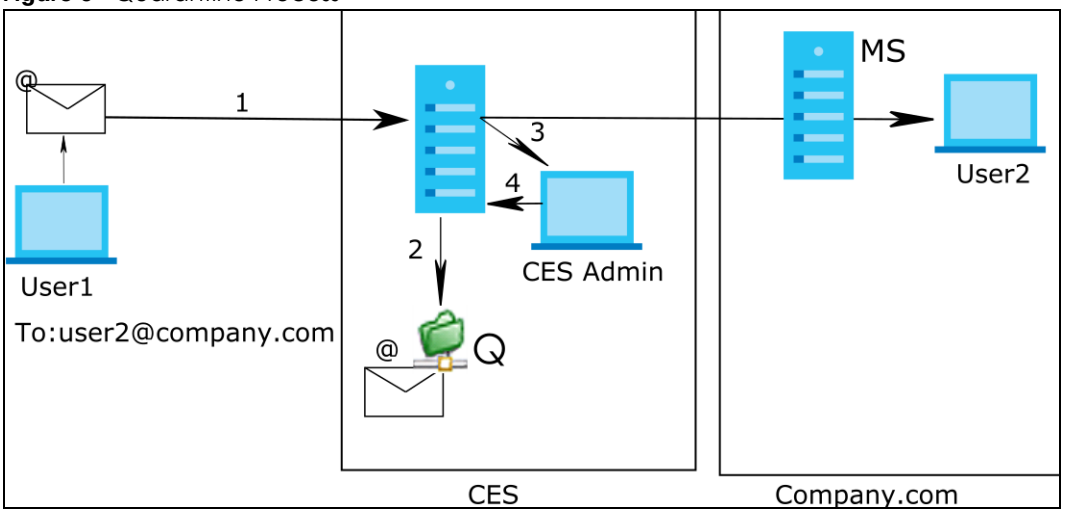
Note: To enable quarantine and configure quarantine settings, go to at **Settings > Email Services > Quarantine**.

3.4.1 Quarantine Process

The following describes the CES quarantine process, using example domain company.com.

Note: The domain administrators have already configured the MX records for company.com to point to the CES cloud servers.

Figure 9 Quarantine Process



1 A user sends an email to user2@company.com. CES receives the email.

2 CES scans the email and applies the policy set for user2@company.com. The policy does not allow image attachments. CES moves the email to the quarantine folder (**Q**).

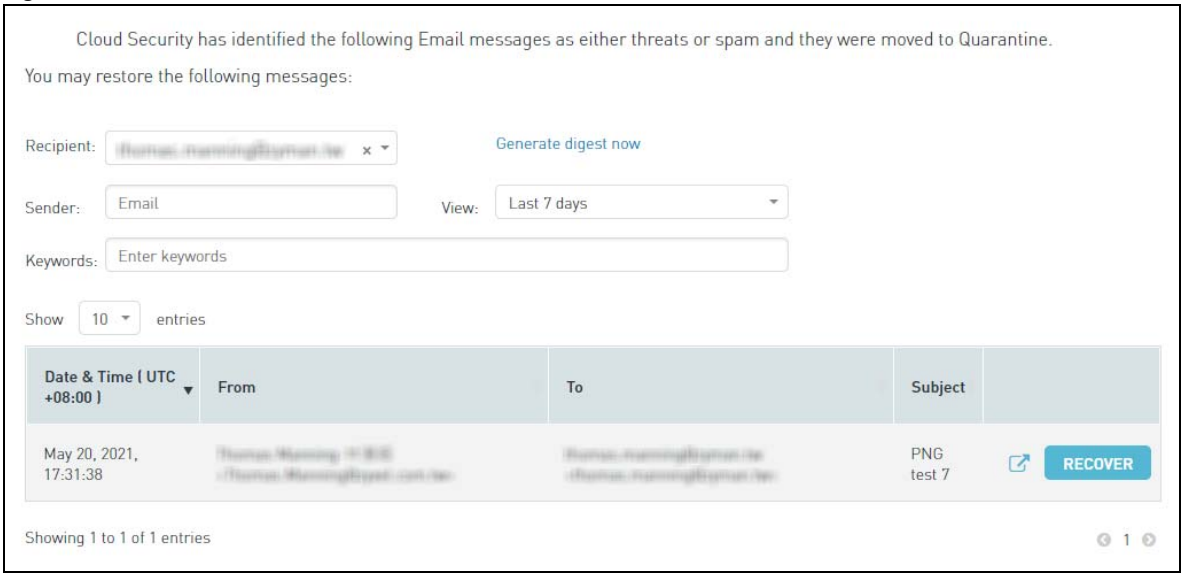
3 CES sends a notification digest email to the company.com mail server (MS) for User 2, stating that an email they were going to receive has been quarantined. CES also sends a quarantine digest email to the CES administrator, giving details of all emails that have been sent to the quarantine folder since the last quarantine digest email.

4 The administrator logs into CES, and goes to **Email Protection > Quarantine**. The administrator can see all emails in the quarantine folder and can choose to release or delete specific email. If released, CES delivers the email to the company.com mail server. If the email is not released within the time set under **Settings > Email Services > Quarantine > Retention Period**, then CES automatically deletes the email.

3.4.2 Quarantine Screen

The Quarantine screen allows you to view and manage quarantined emails. To get to this screen, go to **Email Protection > Quarantine**.

Figure 10 Quarantine Screen



The following table describes the labels on this screen.

Table 10 Quarantine Screen

LABEL	DESCRIPTION
Recipient	Select an email address to manage the address's quarantined emails.
Generate digest now	Click this to generate a quarantine digest email and send it to the selected recipient email address. The digest email contains a list of all of the recipient's quarantined emails, with the following information: • The date and time that the email was received. • The recipient's name and email address. • The sender's name, email address, domain, and X-headers. • The subject line of the email. Note: This digest is automatically generated and send by CES within 24 hours each time an email is quarantined.
Sender	Enter a sender name or email address to filter the list of emails using the From field.
View	Select a time period to filter the list of emails by received date and time.
Keywords	Enter one or more keywords to filter the list of emails by their subject line.
Show X entries	Select how many emails to show in the email list.
Email List	
Date & Time	This shows when the email was received. The date and time format is determined by the timezone specified at **Settings > Account > Account Information > Default Time Zone supported for reports.**
From	This shows the email sender's name and email address.
To	This shows the email recipient's name and email address.
Subject	This shows the email's subject line text.

Table 10 Quarantine Screen (continued)

LABEL	DESCRIPTION
	Click this to view the email in a new window. The body is displayed in a RAW text format, which includes all header information and unformatted HTML tags.
Recover	Click this to release the email from quarantine and send it to the original recipient with all of its attachments.

CHAPTER 4
Reports

4.1 Overview

The **Reports** screens allow you to view and download detailed reports about emails, users, and security threats.

4.1.1 What You Can Do in this Chapter

- Use the **Tracking Log** screen (see Section 4.2 on page 23) to view how CES handled each incoming email.
- Use the **Email Security** screen (see Section 4.3 on page 26) to view a graphical summary of scanned emails and threats.
- Use the **Email Summary Dashboard** screen (see Section 4.4 on page 27) to view total users, the most targeted users, and a detailed summary of the average number of malware hits per day.
- Use the **Exported Reports** screen (see Section 4.5 on page 30) to view and download reports exported from a dashboard
- Use the **Scheduled Reports** screen (see Section 4.6 on page 32) to view and edit scheduled reports
- Use the **SIEM Integration** screen (see Section 4.7 on page 35) to create API-accessible feeds which can be used to read and search for data from your email logs.
- Use the **Audit Log** screen (see Section 4.8 on page 37) to view changes made to CES settings by administrators

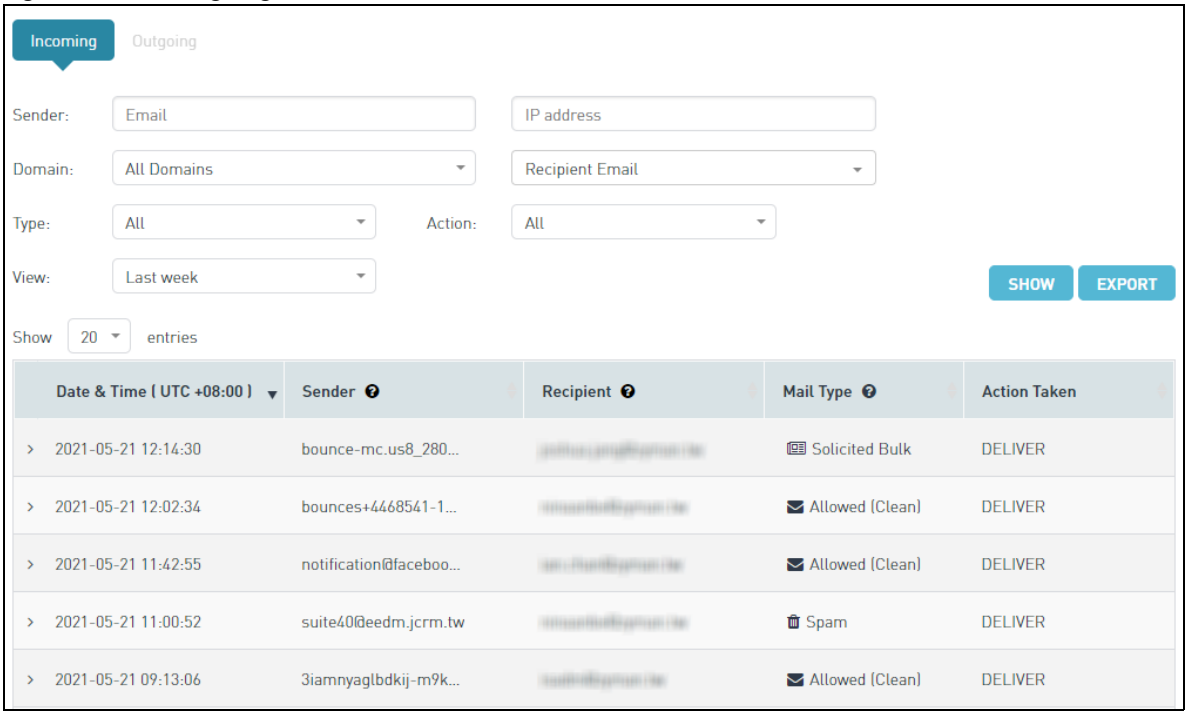
4.2 Tracking Log Screen

The **Tracking Log** screen allows you to view how CES handled each incoming email, including how each email was classified and what action was taken. To get to this screen, go to **Reports > Email > Tracking Log**.

Note: Incoming means emails sent from an external mail server to your mail servers.

Outgoing means emails sent from your mail servers to an external mail server.

Figure 11 Tracking Log Screen



The following table describes the labels on this screen.

Table 11 Tracking Log Screen

LABEL	DESCRIPTION
Use the following fields to filter incoming email logs.	
Sender	Enter a sender email address to filter using the From field.
IP address	Enter the IP address of the sender's mail server.
Domain	Select the domain of the recipient email address.
Recipient Email	Select how many emails to show in the quarantined email list.
Type	Select an email classification given to each email by CES.
Action	Select the action performed on the email by CES.
View	Select a time period to filter the list of emails by received date and time.
SHOW	Click this to apply the specified filtering options to the email list.
EXPORT	Click this to export the email list to a CSV file. The file is then automatically downloaded to your computer and opens in your web browser. Note: To export, the filters must be set to display less than 1,000 emails in the email list. To export a report containing more than 1,000 emails, see Section 4.5.1 on page 31.
Show X entries	Select how many rows to show in the list.
Email List	
Date & Time	This shows when the email was received. The date and time is determined by the timezone specified at **Settings > Account > Account Information > Default Time Zone supported for reports.**
Sender	This shows the email sender's email address.
Recipient	This shows the email recipient's email address.

Table 11 Tracking Log Screen (continued)

LABEL	DESCRIPTION
Mail Type	This shows the classification that CES gave to the email. For a description of each email classification, see Section 4.2.1 on page 25.
Action Taken	This shows the action that CES performed on the email, as determined by its classification.

4.2.1 Email Types

CES scans and then assigns a type to each incoming email. The following table describes each email type.

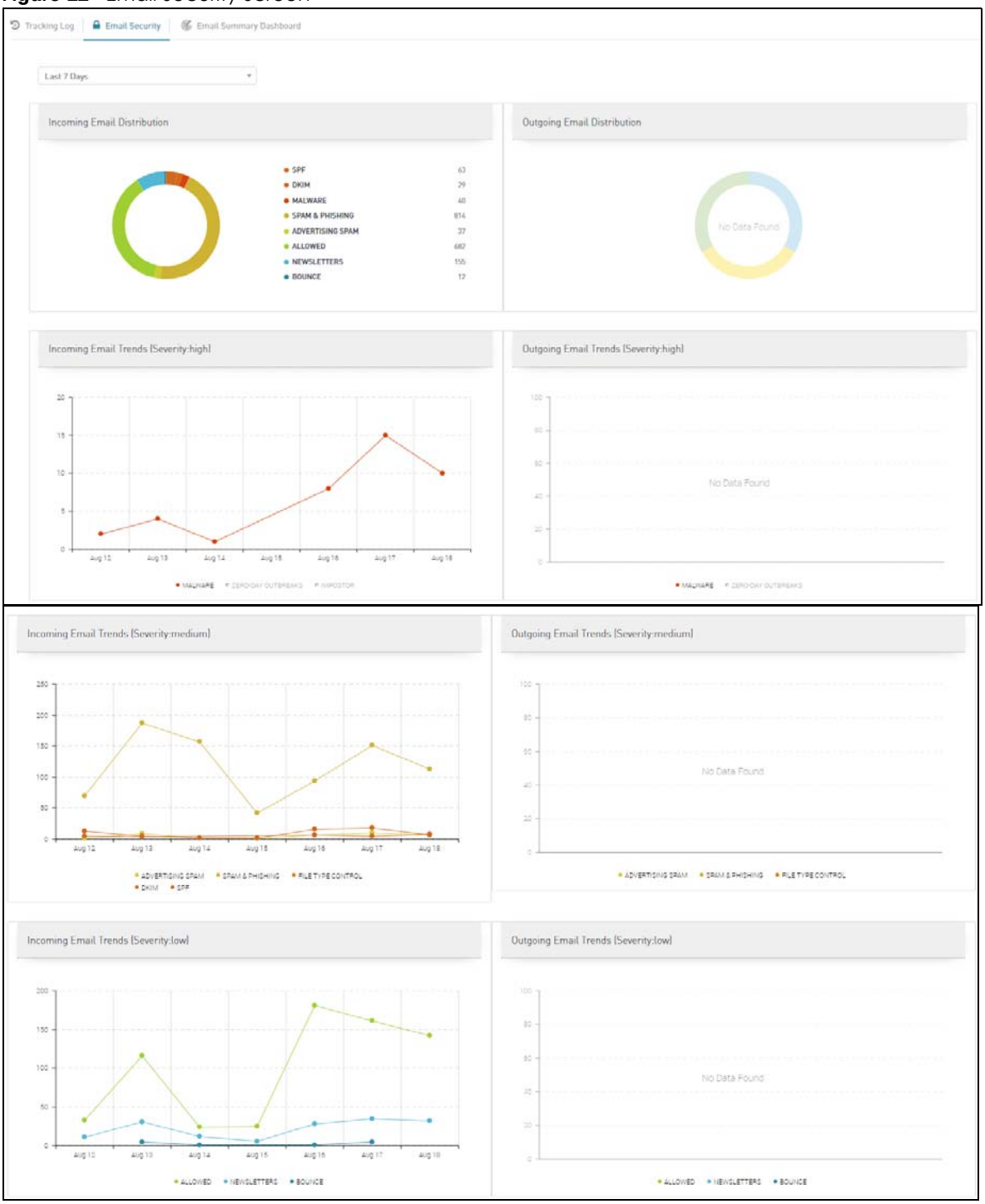
Table 12 Email Types

LABEL	DESCRIPTION
Clean	These are emails with no suspicious features.
Clean Empty	These are emails that have no text in the subject line and email body.
Clean Almost Empty	These are emails that contain fewer than 12 readable characters in the message body (not including tags for display such as HTML tags).
Clean Empty Body	These are emails that have a subject line but no text in the body.
Clean Bounce	These are emails returned back to sender due to an error.
Iframe	These are emails using the iframe feature.
Spam & Phishing	These are emails definitively identified as Spam or phishing e-mail.
Unwanted Attachment	These are emails with attachments that match a file type in the Manage File Type filter of a policy set.
Solicited Bulk	These are mass mails such as newsletters.
Bulk Advertising	These are advertising emails that are not typical Spam, but are usually deemed to be a nuisance.
Bulk Porn	These are emails containing pornographic material, but which are not Spam (for example, pornographic newsletters)
Dangerous	These are emails which may include dangerous self-executing code or attachments with these features.
Dangerous Virus	These are emails containing a virus.
Dangerous Code	These are emails containing potential dangerous content. For example, references to local files.
Dangerous Attachment	These are emails containing attachments such as exe, zip files that may contain viruses.
Dangerous Virus Outbreak	These are emails, that are most likely to contain a new virus not yet recognized by virus detection due to the newness of their debut.
Recipient Validation	These are emails that failed a Recipient Validation check. For details, see Section 6.4 on page 49.
Email Fraud Protection	These are emails that failed a Sender Policy Framework (SPF) or Domain Keys Identified Mail (DKIM) check.
Impostor	These are emails where the sender is trying to impersonate someone within your organization.
SPF	These are emails that failed a Sender Policy Framework (SPF) check. For details, see Section 3.2.1.2 on page 14.
DKIM	These are emails that failed a Domain Keys Identified Mail (DKIM) check. For details, see Section 3.2.1.2 on page 14.

4.3 Email Security Screen

The **Email Security** screen allows you to view a graphical summary of scanned emails and threats. To get to this screen, go to **Reports > Email > Email Security**.

Figure 12 Email Security Screen



The following table describes the labels on this screen.

Table 13 Tracking Log Screen

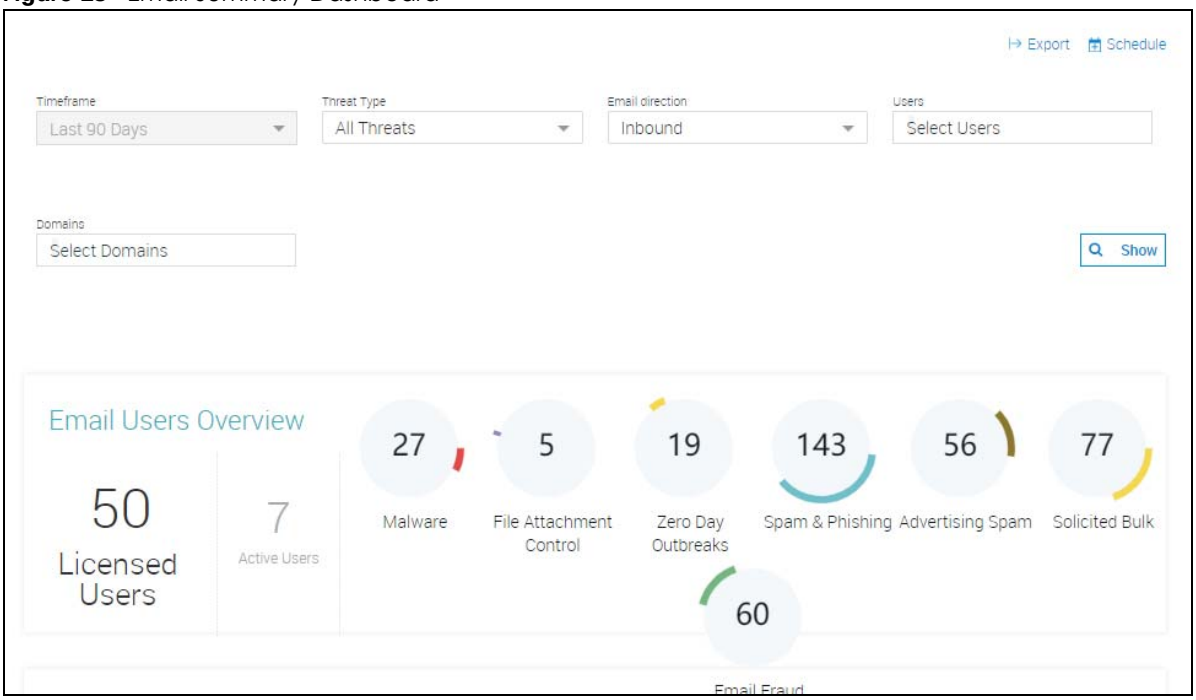
LABEL	DESCRIPTION
Timeframe	Select a time period to filter the graphs on this page.
Incoming Email Distribution	This shows the top classifications of incoming email.
Incoming Email Trends (Severity:high)	This shows a graph of incoming emails classified as a severe threat, such as malware or impostor.
Incoming Email Trends (Severity:medium) email	This shows a graph of incoming emails classified as a medium threat, such as spam and advertising.
Incoming Email Trends (Severity:low)	This shows a graph of incoming emails classified as a low threat, such as bounce and solicited bulk.

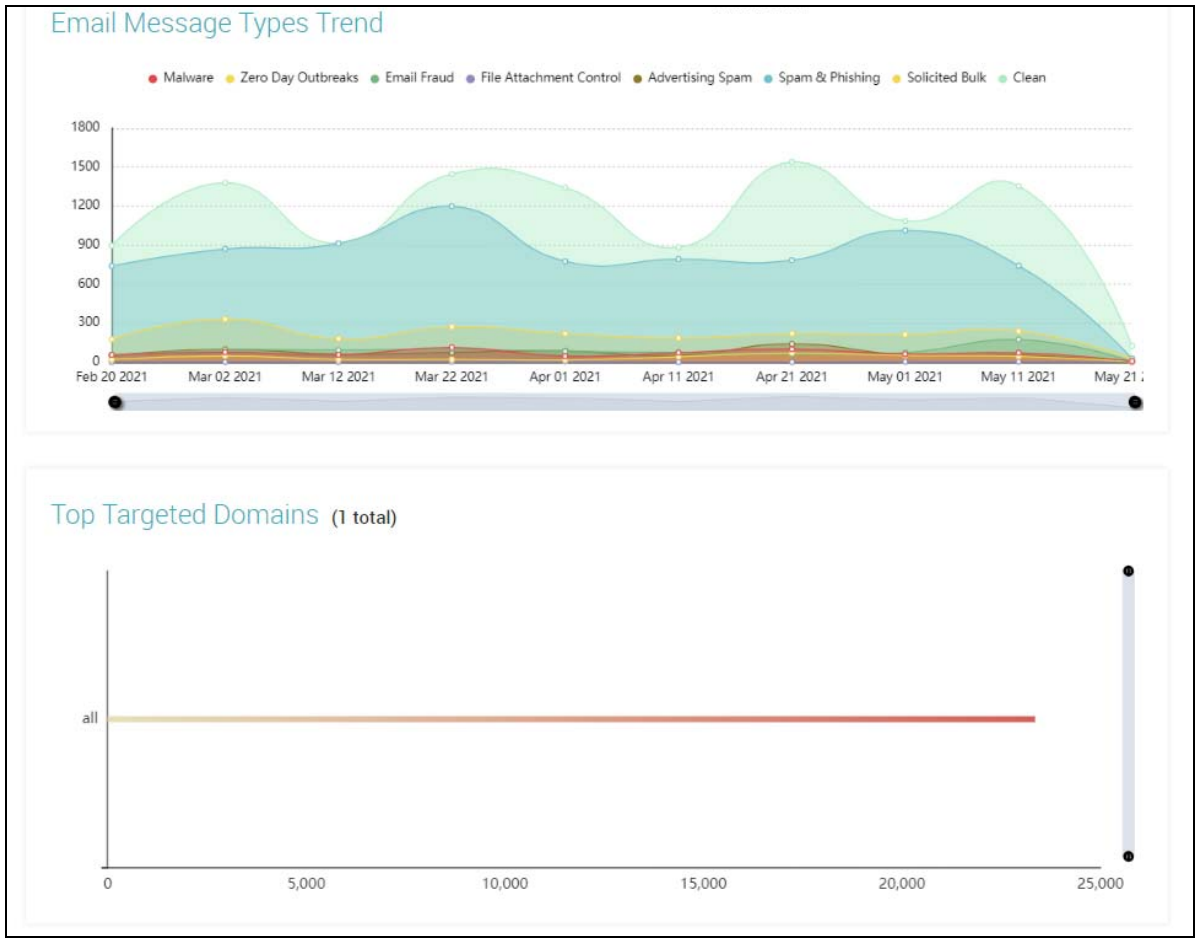
4.4 Email Summary Dashboard Screen

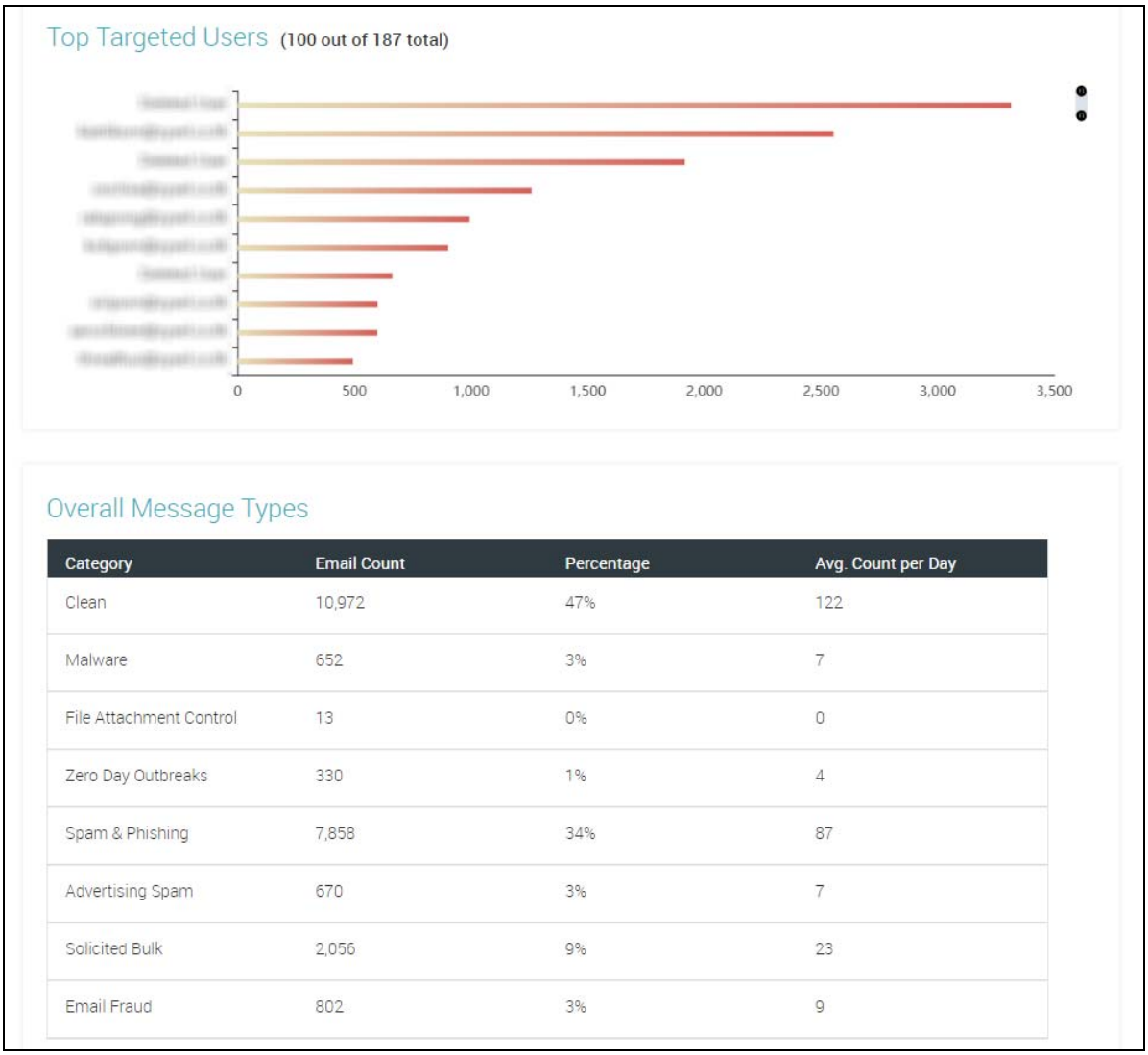
The **Email Summary Dashboard** screen allows you to view total users, the most targeted users, and a detailed summary of the average number of malware hits per day.

To get to this screen, go to **Reports > Email > Email Summary Dashboard**.

Figure 13 Email Summary Dashboard




Email Message Types Trend
Malware
Zero Day Outbreaks
Email Fraud
File Attachment Control
Advertising Spam
Spam & Phishing
Solicited Bulk
Clean
1800
1500
1200
900
600
300
0
Feb 20 2021
Mar 02 2021
Mar 12 2021
Mar 22 2021
Apr 01 2021
Apr 11 2021
Apr 21 2021
May 01 2021
May 11 2021
Top Targeted Domains (1 total)
all
0
5,000
10,000
15,000
20,000
25,000



The following table describes the labels on this screen.

Table 14 Email Summary Dashboard Screen

LABEL	DESCRIPTION
Export	Select this to immediately export the current dashboard as a report. CES exports each section of the dashboard to a separate PDF or CSV file, and then adds each file to a ZIP file. The export process runs as a background task and might take a long time. You can download the final ZIP file at **Reports > Exported > Exported Reports**.
Schedule	Select this to export the current dashboard as a report, according to a schedule. CES exports each section of the dashboard to a separate PDF or CSV file, and then adds each file to a ZIP file. The export process runs as a background task and might take a long time. You can download the final ZIP file at **Reports > Exported > Exported Reports**. For details on creating scheduled reports, see Section 4.6.1 on page 33.
Timeframe	Select a time period for the reports on this screen.
Threat Type	Select the classifications of threat to show on this screen.

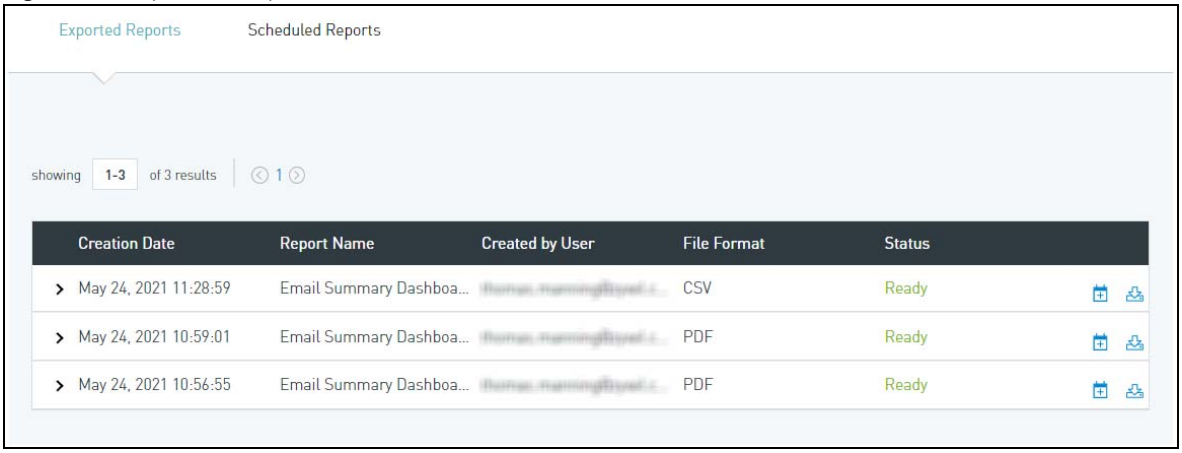
Table 14 Email Summary Dashboard Screen (continued)

LABEL	DESCRIPTION
Email direction	Select incoming or outgoing emails. Note: At the time of writing, only incoming emails are supported.
Users	Select one or more users to filter the reports on this screen by user.
Email Users Overview	
Licensed Users	This shows the maximum number of users allowed to be added to CES, according to your current license.
Active Users	This shows number of users that have received emails within the specified time period.
Malware	This shows the number of emails that were classified as malware. For details on classifications, see Section 4.2.1 on page 25.
File Attachment Control	This shows the number of emails that were classified as Unwanted Attachment.
Zero Day Outbreaks	This shows the number of emails that were classified as Dangerous Virus Outbreak.
Spam	This shows the number of emails that were classified as spam
Advertising Spam	This shows the number of emails that were classified as Bulk Advertising.
Solicited Bulk	This shows the number of emails that were classified as Solicited Bulk.
Email fraud	This shows the number of emails that were classified as Email Fraud Protection.
Email Message Types Trend	This shows the number of emails of each classification received over the specified time period.
Top Targeted Domains	This shows the number of emails for each of your managed domains over the specified time period.
Top Targeted Users	This shows th users that received the most malicious emails over the specified time period.
Overall Message Types	This shows the total number of emails, the percentage of total emails, and the average number of emails per day for each classification over the specified time period.

4.5 Exported Reports Screen

The **Exported Reports** screen allows you to view and download reports exported from a dashboard. Typically, these reports include information about total scanned items, threats detected, and users targeted within a specific time period. To get to this screen, go to **Reports > Exported > Exported Reports**.

Figure 14 Exported Reports Screen



The following table describes the labels on this screen.

Table 15 Exported Reports Screen

LABEL	DESCRIPTION
Showing X of Y results	Click this X to set how many reports are displayed in the table. Y shows the total number of reports.
>	Click this to show and hide the details of the report.
Creation Date	This shows the time and date the report was created. The date and time format is determined by the timezone specified at **Settings > Account > Account Information > Default Time Zone supported for reports.**
Report Name	This shows the name of the screen that the report was created from.
Created by User	This shows the username of the user account that created the report.
File Format	This shows whether the report is in CSV or PDF format.
Status	This shows whether the report is ready to be downloaded (**Ready**) or still being generated (**In Progress**).
	Click this to periodically create this report on a schedule. For details, see Section 4.6.1 on page 33.
	Click this to download the report to your computer, as a ZIP file. This button is only available if status is **Ready**.
Report Details	
Included Reports	This shows all of the sections of the dashboard that were exported into the ZIP file. Note: You cannot choose which sections are exports.
Filters	This shows the filters that are applied to the report, such as time period and users.
Password Protected?	This shows whether the report requires a password to open it.

4.5.1 Creating a Report

Follow the steps below to a create a report.

1 Go to a dashboard screen that has an export button at the top right. For example, **Reports > Email > Email Summary Dashboard.**

2 Configure the filters for the report. For example, you might want to set the report to only cover a specific time period or set of users.

3 Move the pointer over **Export**, and then select a report format. Choose from the following options:

- **CSV**: The report is a set of CSV files containing RAW data points. There is one file for each section of the dashboard screen.
- **PDF**: The report is a set of PDF files containing data in formated graphs and tables. There is one file for each section of the dashboard screen.

  After clicking the format a message appears, saying that the report in being generated.

4 Go to **Reports > Exported > Exported Reports**. Locate the report, and then wait for the report's status to change from I**n Progress** to **Ready**. If the report has a large number of data points, then this might take a long time.

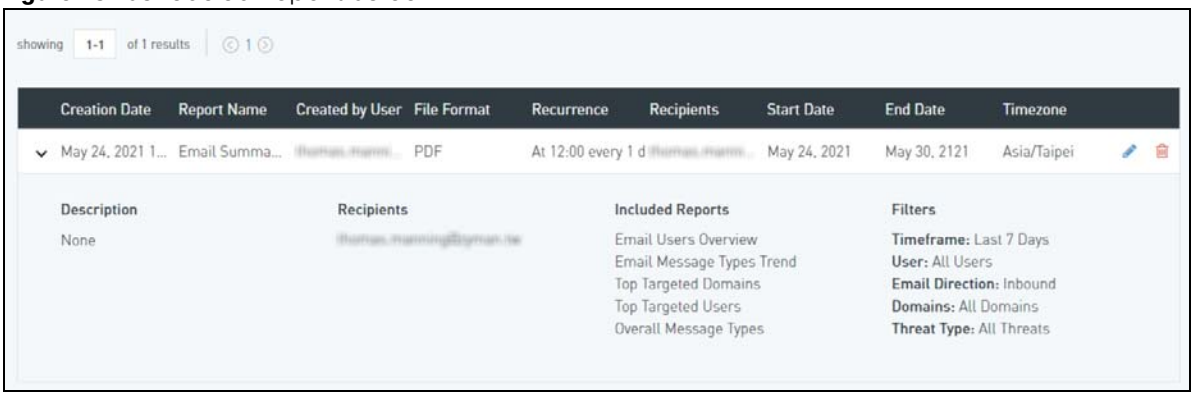
5 Click  to download the report to your computer as a ZIP file.

4.6 Scheduled Reports Screen

The **Scheduled Reports** screen allows you to view and edit scheduled reports. To get to this screen, go to **Reports > Exported > Scheduled Reports**.

A scheduled report is an exported report that is created periodically on a schedule, and then sent by email to one or more CES administrators. This is useful if you want to use the exported reports feature to regularly check the status of CES without logging in.

Figure 15 Scheduled Reports Screen



The following table describes the labels on this screen.

Table 16 Scheduled Reports Screen

LABEL	DESCRIPTION
Showing X of Y results	Click this X to set how many reports are displayed in the table. Y shows the total number of reports.
>	Click this to show and hide the details of the report.
Creation Date	This shows the time and date the report was created.
Report Name	This shows the name of the screen that the report was created from.
Created by User	This shows the username of the user account that created the report.

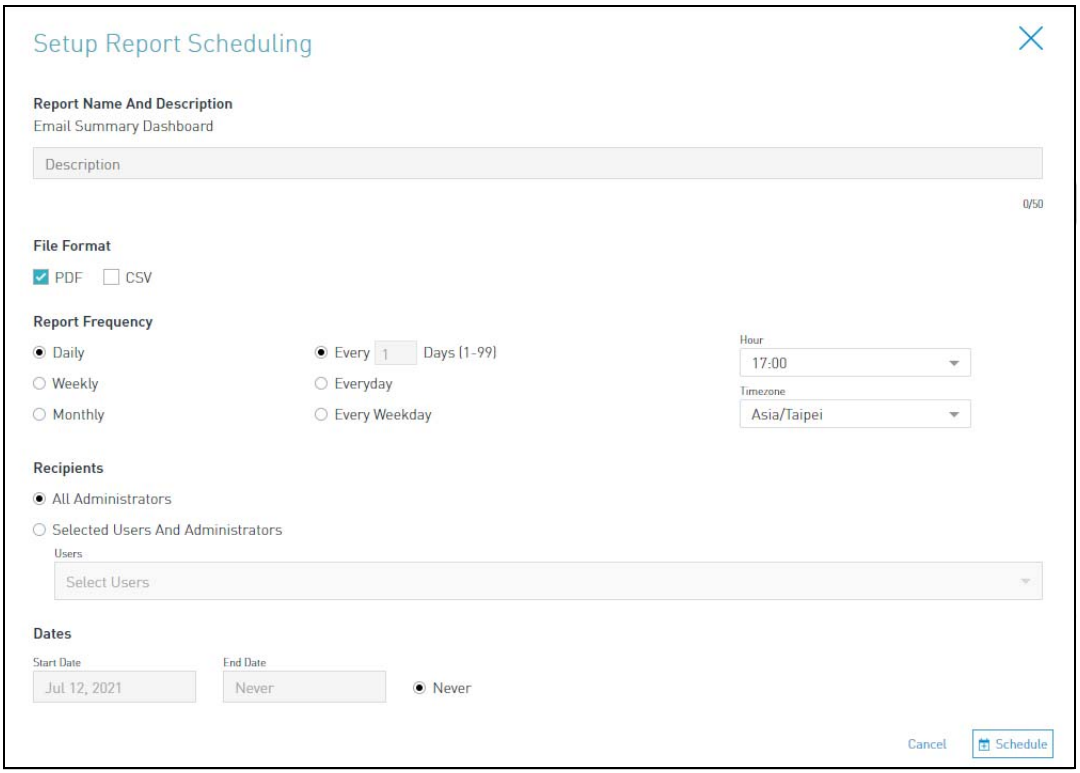
Table 16 Scheduled Reports Screen (continued)

LABEL	DESCRIPTION
File Format	This shows whether the report is in CSV or PDF format.
Recurrence	This shows the report's schedule. For example "At 23:00 every 2 days".
Recipients	This shows a list of the email addresses that receive the report after it is created.
Start Date	This shows the date on which the schedule becomes active.
End Date	This shows the date on which the schedule becomes inactive.
Timezone	This shows the timezone that the schedule is following.
Status	This shows whether the report is ready to be downloaded (**Ready**) or still being generated (**In Progress**).
	Click this to edit the report.
	Click this to delete the report.
Report Details	
Description	This shows a description of the report, set by a CES administrator.
Recipients	This shows a list of the email addresses that receive the report after it is created.
Included Reports	This shows all of the sections of the dashboard that were exported into the ZIP file.
Filters	This shows the filters that are applied to the report, such as time frame and users.

4.6.1 Creating a Scheduled Report

Follow the steps below to a create a report.

1. Go to a dashboard screen that has an export button at the top right. For example, **Reports > Email > Email Summary Dashboard.**
2. Configure the filters for the report. For example, you might want to set the report to only cover a specific time period or set of users.
3. At the top-right of the screen, click **Schedule**. The **Setup Report Scheduling** window opens.



4 Enter a description of up to 50 characters for the report. This description should tell other administrators what the report is for.

5 Select a report format. Choose from the following options:

- **CSV**: The report is a set of CSV files containing RAW data points. There is one file for each section of the dashboard screen.
- **PDF**: The report is a set of PDF files containing data in formated graphs and tables. There is one file for each section of the dashboard screen.

6 Select how frequently the report will be generated. For example, you can set once a week, or every X days.

Select what time the report will be generated, and what timezone this time is in.
You can create reports for different timezones if your company has offices in multiple countries. You can set a default timezone in **Settings > Account > Account Information > Default Time Zone supported for reports.**

7 Set the recipients for the report. You can select all administrators, or a specific group of users and administrators.

8 Select a start date. CES will start generating reports according to the schedule on this date.

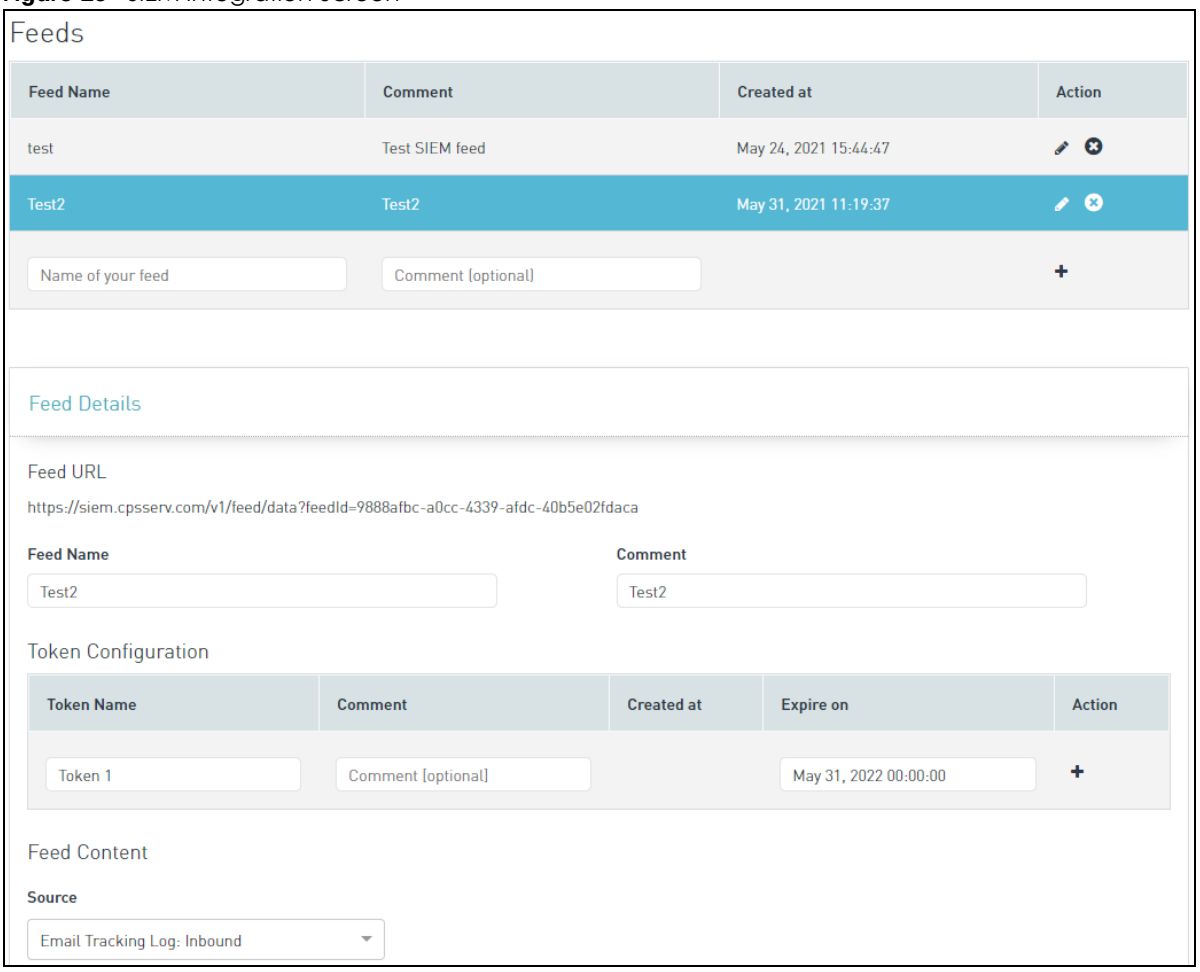
9 Select an end date. CES will stop generating reports according to the schedule on this date. Select **Never** to generate reports indefinitely.

10 Click **Schedule**.
The scheduled report is created and displayed at **Reports > Exported > Exported Reports**.

4.7 SIEM Integration Screen

The **SIEM Integration** screen allows you to create API-accessible feeds which can be used to read and search for data from your email logs. You can use these feeds to integrate CES into your existing Security Information and Event Management (SIEM) architecture. To get to this screen, go to **Reports > SIEM**.

Figure 16 SIEM Integration Screen



The following table describes the labels on this screen.

Table 17 SIEM Integration Screen

LABEL	DESCRIPTION
Feed name	This displays the name of the feed, as set by the administrator who created it.
Comment	This shows a description of the feed, as set by a CES administrator.
Created at	This shows the time and date the feed was created.
Action	Click one of the icons to perform an action on the feed.
	Click this to edit the feed.
	Click this to delete the feed. Note: After deleting a feed, you must click **Save** at the bottom of the screen to save the change.

Table 17 SIEM Integration Screen (continued)

LABEL	DESCRIPTION
+	Click this to create a new feed.
Feed Details	
Feed URL	This shows the URL used to access the feed. A token is also required to read data from the URL.
Feed Name	Enter the name of the feed. This can consist of up to 255 characters.
Comment	Enter a description of the feed. This can consist of up to 1024 characters.
Token Configuration	A token is a private key that allows you to authenticate with CES and access a specific feed. A feed can have multiple tokens, each with separate expiry dates. This is useful if you have multiple SIEM platforms, as each platform can have its own token.
Token Name	This shows the name of the token.
Comment	This shows a description of the token, as set by a CES administrator.
Created at	This shows the time and date the token was created.
Expire on	This shows the time and date the token expires.
Action	Click one of the icons to perform an action on the token.
	Click this to edit the token.
+	Click this to create a new token. Note: You must copy and save the token during creation. You cannot view the token again later.
Source	Click this to select incoming or outgoing mail. Note: At the time of writing, CES only supports inbound mail.

4.7.1 Creating a Feed

Follow the steps below to a create an API-accessible feed.

1 Go to **Reports > SIEM.**

2 Locate a blank row, and then enter a name for the feed.

3 Enter a descriptive comment for the feed, and then click +.
The feed details section opens.

4 Under Token Configuration, enter a token name, comment, and expiry date. Then click +.
The token is created and opens in a new window.

5 Copy and save the token.

Note: You cannot view the token again later

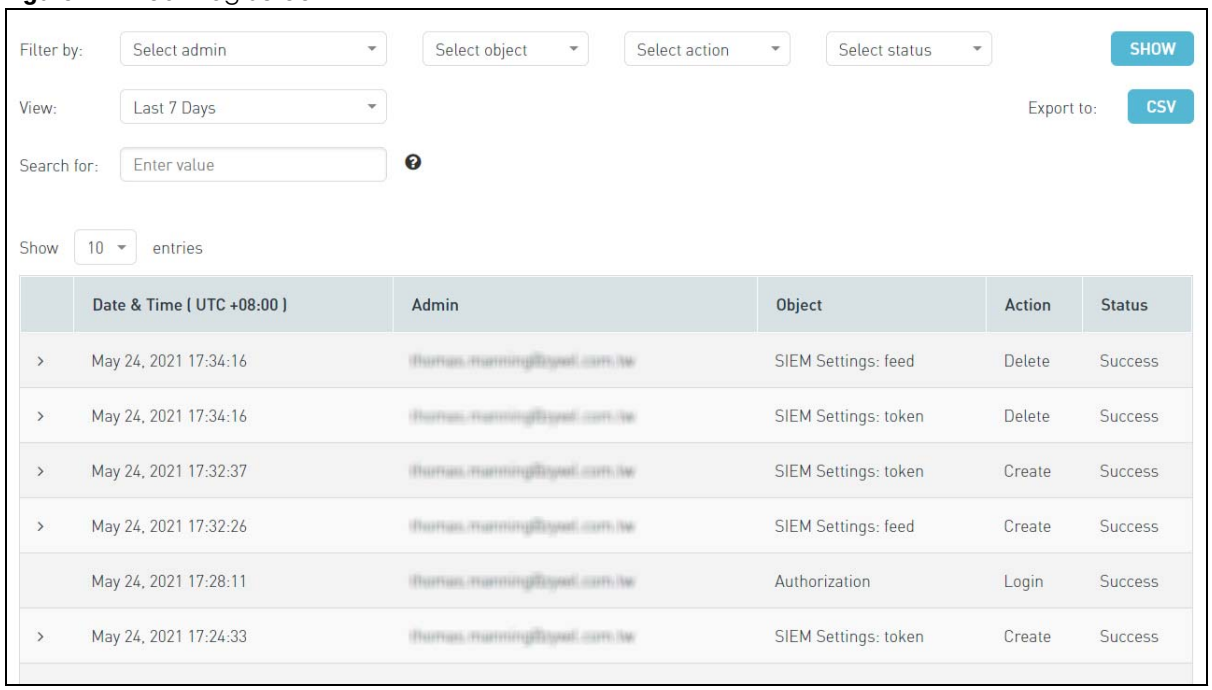
6 Click + and then repeat the above steps to create additional tokens.
You can have one token for each SIEM platform.

The feed is can now be accessed using the created tokens.

4.8 Audit Log Screen

The **Audit Log** screen allows you to view changes made to CES settings by administrators. To get to this screen, go to **Reports > Exported > Exported Reports**.

Figure 17 Audit Log Screen



The following table describes the labels on this screen.

Table 18 Audit Log Screen

LABEL	DESCRIPTION
Filter by	Click this to filter the audit log by the CES administrator.
Select object	Click this to filter the audit log by the modified setting or object.
Select action	Click this to filter the audit log by action taken on the setting or object. For example, delete.
Select status	Click this to filter audit log by whether the action was successful or failed.
Show	Click this to apply the current filter settings.
Export to	Click this to export the audit log to a CSV file, and then open the file in your web browser.
Search for	Enter one or more keywords to search the audit log.
Log Message Table	
Showing X results	Click X to set how many log messages are displayed in the table.
>	Click this to show details of the settings change, such as the new setting values.
Date & Time	This shows the time and date the log message was created. The date and time format is determined by the timezone specified at **Settings > Account > Account Information > Default Time Zone supported for reports.**
Admin	This shows the CES administrator that made the setting change.
Object	This shows the modified setting or object, such as a user or feed.
Action	This shows the action taken on the setting or object. For example, delete.
Status	This shows whether the action was successful or failed.

CHAPTER 5
Notifications

5.1 Overview

The **Notifications** screens allow you to view and delete notifications.

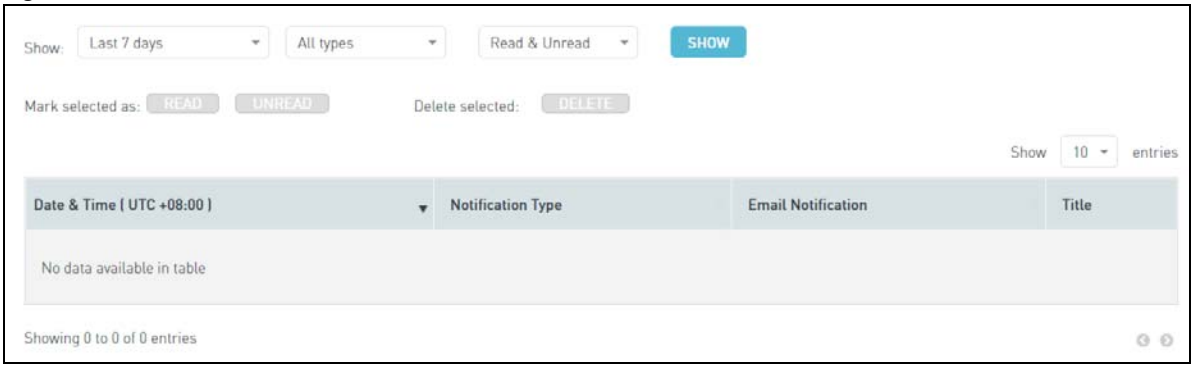
5.1.1 What You Can Do in this Chapter

Use the **Notifications** screen (see Section 5.2 on page 38) to view and delete notifications

5.2 Notifications Screen

The Notifications screen allows to view and delete notifications about detected security threats or CES. To get to this screen, go to **Menu > Notifications**.

Figure 18 Notifications Screen



The following table describes the labels on this screen.

Table 19 Notifications Screen

LABEL	DESCRIPTION
Show (time period)	Select a time period for the notifications on this screen.
All types	Click this to filter the notifications by type.
Read & Unread	Click this to filter the notifications by read or unread status.
Show	Click this to apply the current filter settings.
Read	Click this to set the selected notifications as read.
Unread	Click this to set the selected notifications as unread.
Delete	Click this to delete the selected notifications.
Notification Table	

Table 19 Notifications Screen

LABEL	DESCRIPTION
Date & Time	This shows the time and date the notification was created. The date and time format is determined by the timezone specified at **Settings > Account > Account Information > Default Time Zone supported for reports.**
Notification Type	This shows the type of notification issued.
Email Notification	This shows whether the notification email has been delivered yet.
Title	This shows the severity level of the notification, which can be low, medium, or high.
Details	Click this to go the related CES screen where the notification was issued.

CHAPTER 6
Settings

6.1 Overview

The **Settings** screen allow you to configure general settings for CES.

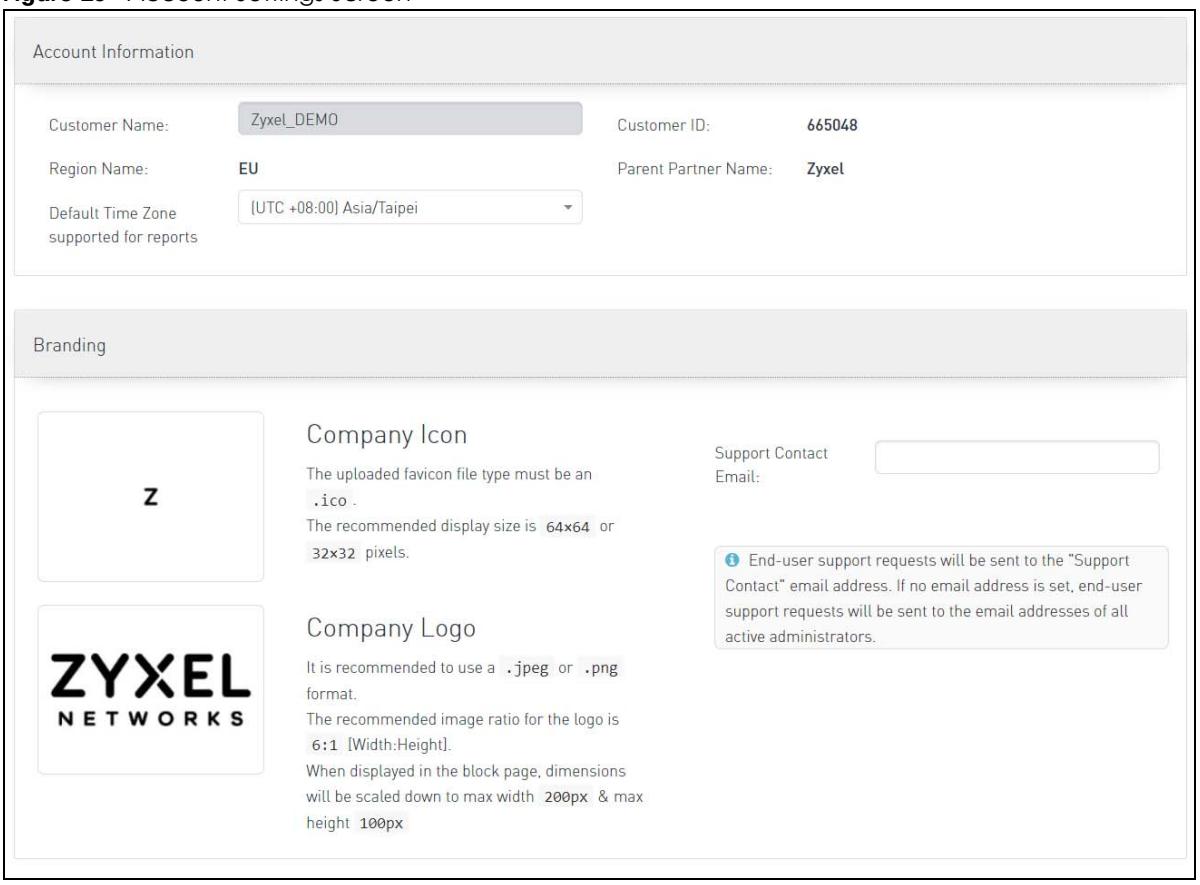
6.1.1 What You Can Do in this Chapter

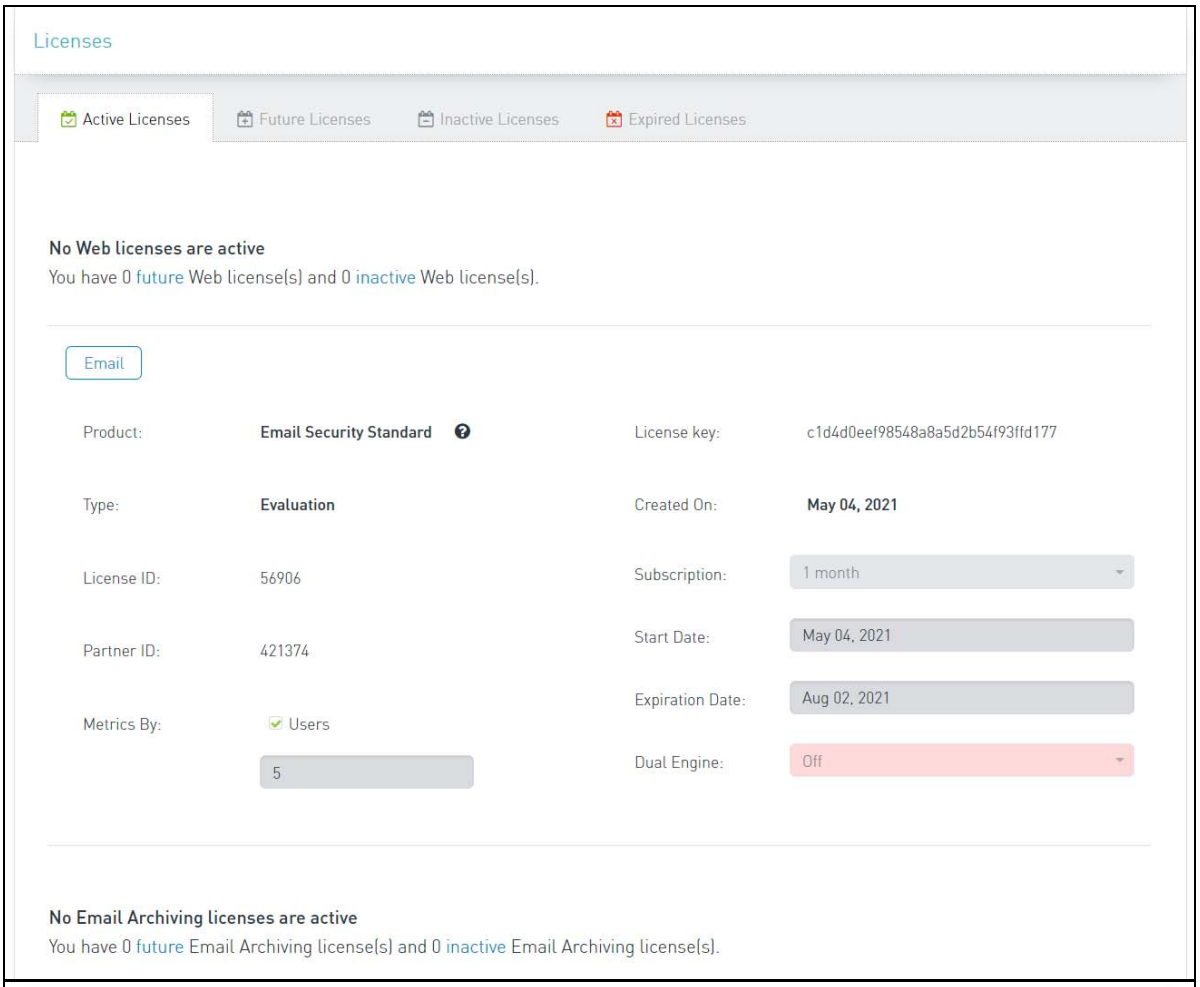
- Use the **Account Screen** screen (see Section 6.2 on page 40) to configure settings related your CES organization, such as timezone, licensing information, branding, and administrators.
- Use the **Users** screen (see Section 6.3 on page 45) to add, remove, and edit user accounts and groups.
- Use the **Email Services** screen (see Section 6.4 on page 49) to configure email settings such as mail servers, quarantine, and recipient validation.
- Use the **Notification Settings** screen (see Section 6.5 on page 51) to configure notification settings.

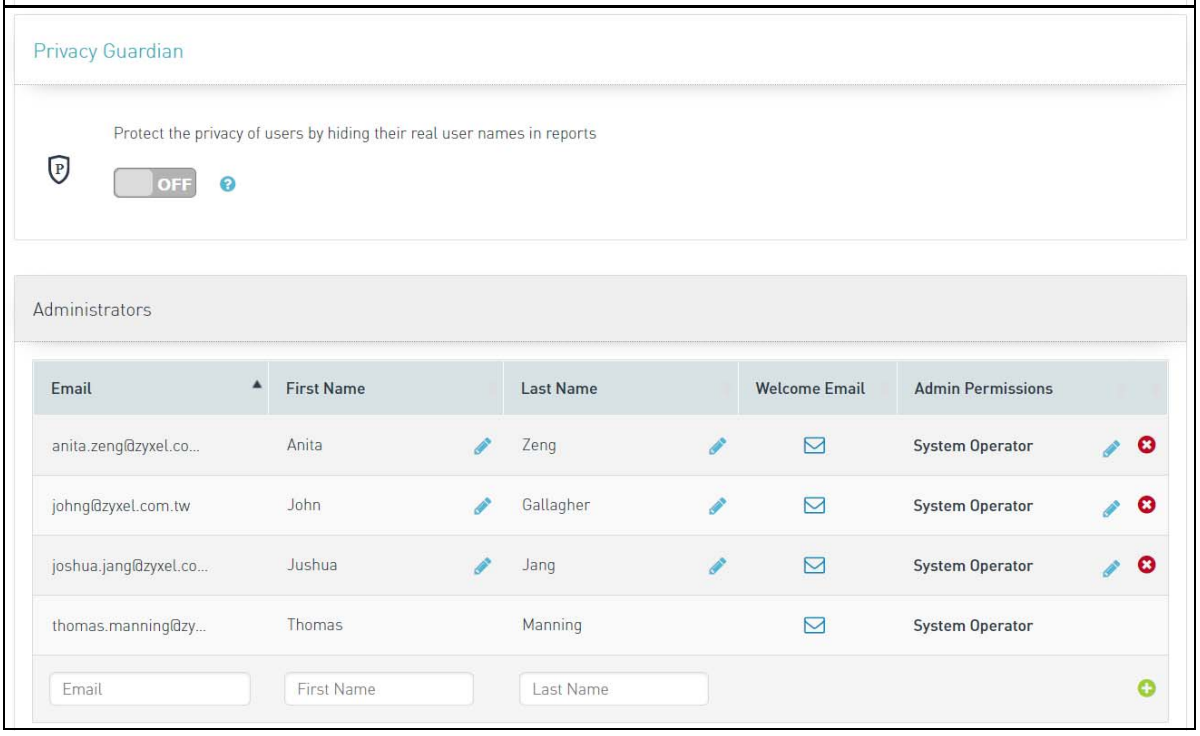
6.2 Account Screen

Use the **Account** screen to configure settings related your CES organization, such as timezone, licensing information, branding, and administrators. To get to this screen, go to **Settings > Account**.

Figure 19 Account Settings Screen




Licenses
Active Licenses
Future Licenses
Inactive Licenses
Expired Licenses
No Web licenses are active
You have 0 future Web license(s) and 0 inactive Web license(s).
Email
Product:
Email Security Standard
License key:
c1d4d0eef98548a8a5d2b54f93ffd177
Type:
Evaluation
Created On:
May 04, 2021
License ID:
56906
Subscription:
1 month
Partner ID:
421374
Start Date:
May 04, 2021
Expiration Date:
Aug 02, 2021
Metrics By:
Users
5
Dual Engine:
Off
No Email Archiving licenses are active
You have 0 future Email Archiving license(s) and 0 inactive Email Archiving license(s).

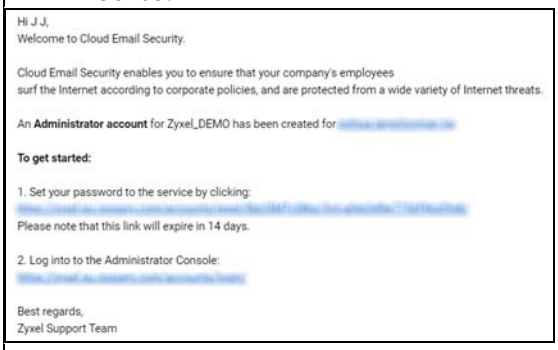

Privacy Guardian
Protect the privacy of users by hiding their real user names in reports
OFF
Administrators
Email
First Name
Last Name
Welcome Email
Admin Permissions
anita.zeng@zyxel.co...
Anita
Zeng
System Operator
johng@zyxel.com.tw
John
Gallagher
System Operator
joshua.jang@zyxel.co...
Jushua
Jang
System Operator
thomas.manning@zy...
Thomas
Manning
System Operator
Email
First Name
Last Name

The following table describes the labels on this screen.

Table 20 Account Settings Screen

LABEL	DESCRIPTION
Account Information	
Customer Name	This shows the name of your organization. This was set when you activated the license.
Customer ID	This shows your customer ID, which is linked to your license.
Region Name	This shows the region that the CES is running, and cannot be changed.
Parent Partner Name	This shows Zyxel.
Default Time Zone supported for reports	Click this configure the default time format used in reports and on most screens in CES.
Branding	Branding allows you to add your organization's logos to CES. Note: Branding, including Company Icon, Company Logo and Support Contact Email is for CES web security service only and is not supported at the time of writing.
Company icon	Click this to upload your organization's favicon icon. The favicon icon is displayed in web browser tabs and browser bookmarks when you open CES in a web browser. • The favicon icon must be an ICO file. • The favicon icon should be 32x32 or 64x64 pixels.
Company Logo	Click this to upload a your organization's logo. The logo is displayed in the title bar. • The logo should be a JPEG or PNG file. • The recommended image ratio is 6:1 width to height.
Support Contact Email	Enter an email address to receive web security support requests. This is used when a user clicks the Support link on the right side of the CES window, and then fills out a support query.
Licenses	Please check myZyxel for the most up-to-date license information.
Active Licenses	This tabs shows the CES license that your organization is currently using.
Future Licenses	This tabs shows licenses that are active but not currently being used.
Inactive Licenses	This tabs shows licenses that were added to myZyxel but have not been activated yet. Note: At the time of writing, this licensing type is not supported by CES.
Expired Licenses	This tabs shows licenses that your organization previously used but have now expired.
Product	This shows the name of the license. Note: At time of writing, CES only supports **Email Security Standard**.
Type	This shows the license type, such as production or evaluation (trial).
License ID	This shows the unique identifying number of the license.
Partner ID	This shows the unique identifying the partner running CES, which in this case is Zyxel.
Metrics By	This shows the number of users allowed to use CES by the license.
License Key	This shows the license key, as entered on myZyxel.
Created on	This shows the time and date that the license was added to myZyxel.
Subscription	This shows the duration of the license, in days, months, or years.
Start Date	This shows the time and date that the license was activated, or will be activated if it is a future license.

Table 20 Account Settings Screen (continued)

LABEL	DESCRIPTION
Expiration Date	On the **Active Licenses** page, this shows the time and date that the license will expire (future). On the **Expired Licenses** page, this shows the time and date that the license expired (past).
Privacy Guardian	
Protect the privacy of users by hiding their real user names in reports	When enabled, exported reports, log pages, and security incidents contain anonymized names and email addresses to protect the user's privacy. CES administrators who have Privacy Guardian permissions are still able to view real names and email addresses. Privacy Guardian permission are automatically assigned to the administrator that enabled this setting, and can also be assigned at **Settings > Account > Administrators**.
Administrators	Administrators are special users that can view and configure CES settings.
Email	This shows the email address of the administrator. This does not need to be an address from one of the email domains being managed by CES.
First Name	This shows the given name of the administrator.
	Click the Edit icon to modify the field.
Last Name	This shows the family name of the administrator.
Welcome Email	Click this to send a welcome email to the administrator. The email contains: • A welcome message, stating that they are now a CES administrator. • The URL of CES. • A link that they can click to set their CES password, if they have not set a password yet. Note: The first administrator receives a welcome email after purchasing a CES license.  Hi J J, Welcome to Cloud Email Security. Cloud Email Security enables you to ensure that your company's employees surf the Internet according to corporate policies, and are protected from a wide variety of Internet threats. An **Administrator account** for Zyxel_DEMO has been created for [redacted] **To get started:** 1. Set your password to the service by clicking: [redacted] Please note that this link will expire in 14 days. 2. Log into to the Administrator Console: [redacted] Best regards, Zyxel Support Team
Admin Permissions	This shows the role and permissions that the administrator has. For details, see Section 6.2.2 on page 45.
	Click the Delete delete the administrator. You must click **Save** to save the changes.
	Click the Add icon to crate a new administrator.

6.2.1 Adding an Administrator

Follow the steps below to add an administrator to CES.

1 Go to **Settings > Account > Administrator**, and then locate a blank row.

2 In the blank row enter the administrator's email address, first name, and last name, and then click Add. The new administrator is added to the table, with a default role of system administrator.

3 In the **Admin Permissions** column, click Edit. The **Roles & Permissions** window open.

4 Select a role for the administrator. For details, see Section 6.2.2 on page 45.

5 (Optional) Grant the administrator Privacy Guardian permissions. With these permissions, the administrator is able to see real names and email in reports. To modify this setting, **Privacy Guardian** must be enabled at **Setting > Account > Privacy Guardian** and your account must have Privacy Guardian permissions.

6 Click Save. The **Roles & Permissions** window closed.

7 Click the email Welcome Email icon to send the new administrator a welcome email.

6.2.2 Administrator Roles

The following describes the different CES administrator roles.

Table 21 Account Settings Screen

ROLE	PERMISSIONS
System Operators	These accounts can configure all CES settings. They can add, remove, and edit administrators.
Web Security	These accounts can only edit web security features. Note: At time of writing, this role is not supported in CES.
Email	These accounts can configure all CES settings, and can view but not add, remove, nor edit administrators.
Configuration Operators	These accounts can configure the system, but cannot view reports. They have full permissions over the **Email Protection** and **Settings** menus, but cannot access the **Reports**, **Notifications**, nor **Overview** menus,
Basic Operators	These accounts have read-only permissions on all screens.

6.3 Users

User accounts are required to use CES.

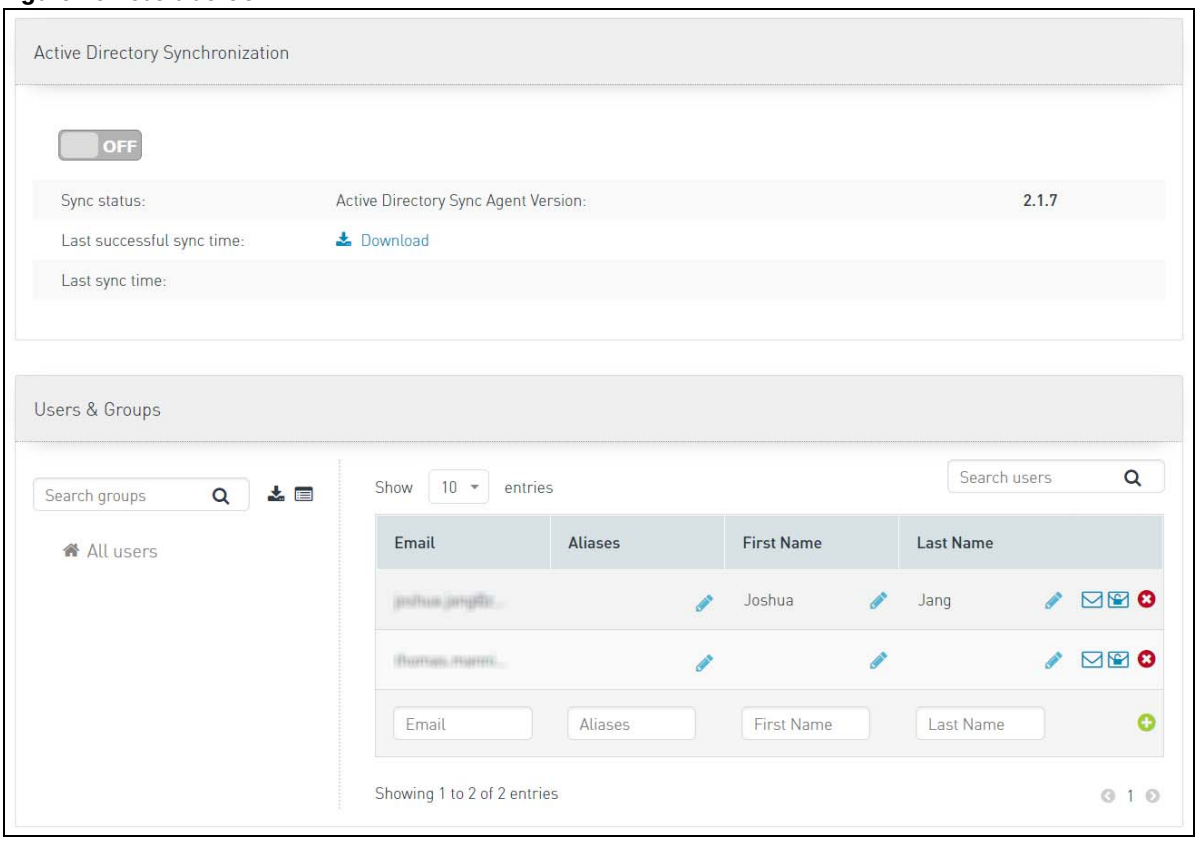
- When an email is sent to an email address associated with a user account, CES scans the email according to the rule set for the user.
- When an email arrives for an email address not associated with a user account, by default CES delivers the email to the final mail sever without scanning the email.

Note: The number of users you can add depends on your license. For details, see Section 1.3 on page 5.

6.3.1 Users Screen

Use the **Users** screen to add, remove, and edit user accounts and groups. You can add users and groups manually, or synchronize them from Active Directory.

Figure 20 Users Screen 1



The following table describes the labels on this screen.

Table 22 Users Screen

LABEL	DESCRIPTION
Active Directory Synchronization	You can synchronize users and groups from Windows Active Directory, by installing AD Sync Agent on one of your AD servers. For details, see Section 6.3.2 on page 47.
On/Off	Enable or disable synchronizing users and groups from Active Directory.
Sync status:	When an Active Directory synchronization job is in progress, this shows the percentage comped. When a job is not in progress, this shows **Idle**.
Last successful sync time:	This shows the time and date that an Active Directory synchronization job successfully ran.
Last sync time:	This shows the time and date that an Active Directory synchronization job ran. It may have been successfully or failed.
Active Directory Sync Agent Version:	This shows the version of the AD Sync Agent that is available for download.
Download	Click this to download AD Sync Agent.

Table 22 Users Screen (continued)

LABEL	DESCRIPTION
Users & Groups	
Group List	
Search Groups	Enter a keyword to filter the list of groups.
	Click the Download icon to export users an groups to a CSV file, which then opens in your web browser.
	Click the View icon to view the groups as a flat list (**List View**) or hierarchy (**Tree View**).
Users List	
Show X entries	Select how many entries to show in the list.
Email	This shows the email address of the user.
Aliases	This shows any alternative email addresses the user has.
	Click this to edit the current field.
First Name	This shows the user's first name.
Last Name	This shows the user's last name.
	Click the Welcome Email icon to send a link for the web security initiation process. Note: This is for CES web security service only and is not supported at the time of writing.
	Click the Password Reset icon to send a password reset email to web security users. Note: This is for CES web security service only and is not supported at the time of writing.
	Click the Remove icon to delete the user.
	Click the Add icon to create a new user. For details, see Section 6.3.3 on page 48.

6.3.2 Setting up Active Directory Synchronizing

Follow the steps below to synchronize users and groups from your existing Windows Active Directory domain to CES.

1 Go to **Settings > Users > Active Directory Synchronization**, and slide **ON/OFF** to **ON**.

2 Click **Download**, and save the AD Sync Agent MSI file to you computer.

3 Transfer the AD Sync Agent installation file to a server or workstation within the Active Directory domain. The server or workstation must meet the following requirements:

- Server: Windows Server 2008 RC2 or later.
- Workstation: Windows 7 or later.
- Microsoft.Net 4.5 Framework is installed.

4 Run the AD Sync Agent installation file on the sever or workstation. During installation, you need to specify the following values:

- **LDAP URL**: The URL of the Active Directory server. For example: LDAP://123.456.789.10/OU=myOrgUnit,DC=corp,DC=myCompany,DC=com.
- **Binding User**: The username used to authenticate with and query Active Directory.
- **Password**: The password of the Binding User account.
- **User filter** (optional): Enables you to add a user filter value, so that you only sync a specific set of users. For example, givenName=John.
- **Group filter** (optional) Enables you to add a group filter value, so that you only sync a specific set of groups. For example, memberof=CN=rnd,OU=R&D,OU=group,OU=folder1\+abc/yeloow\+bbb\<a\>abc,OU=sub1\+WIC/MSS\"WIC\\\BBCC,OU=Root,DC=test,DC=group,DC=company,DC=com.
- **Email**: The AD property that matches the email address of the user. This field is required and must be unique.
- **Last Name**: The AD Property that matches the last name of the user
- **Phone Number**: The AD Property that matches the phone number of user
- **Email Aliases**: The AD Property that matches the email aliases of the user

5 After AD Sync Agent is installed, Active Directory synchronization starts after 5 minutes.

6 To configure the frequency of Active Directory synchronization on the server or workstation, open **Windows Task Scheduler,** open **Task Scheduler Library**, and then locate the **CyrenAdSync** task. Edit the task, go to the **Triggers** tab, and then in advanced settings configure **Repeat Task Every**.

6.3.3 Creating a User

Follow the steps below to create a new user in CES.

1 Go to **Settings > Users > Users & Groups**.

2 (Optional) In the group list, select the group that you want to add the user to.

Note: A user can only belong to one group. You cannot change a user's group later.

3 In the user list, locate a blank row.

4 In the blank row, enter a user's email address, alias email address, first name, and last name. The email address must be unique. Then click .
CES adds the new user to the user list and sends a welcome email to the user's email address.

6.3.4 Creating a Group

Follow the steps below to create a new group in CES.

1 Go to **Settings > Users > Users & Groups**.

2 In the group list, perform one of the following actions:

- Right-click on All Users, and then select **Create Group**.

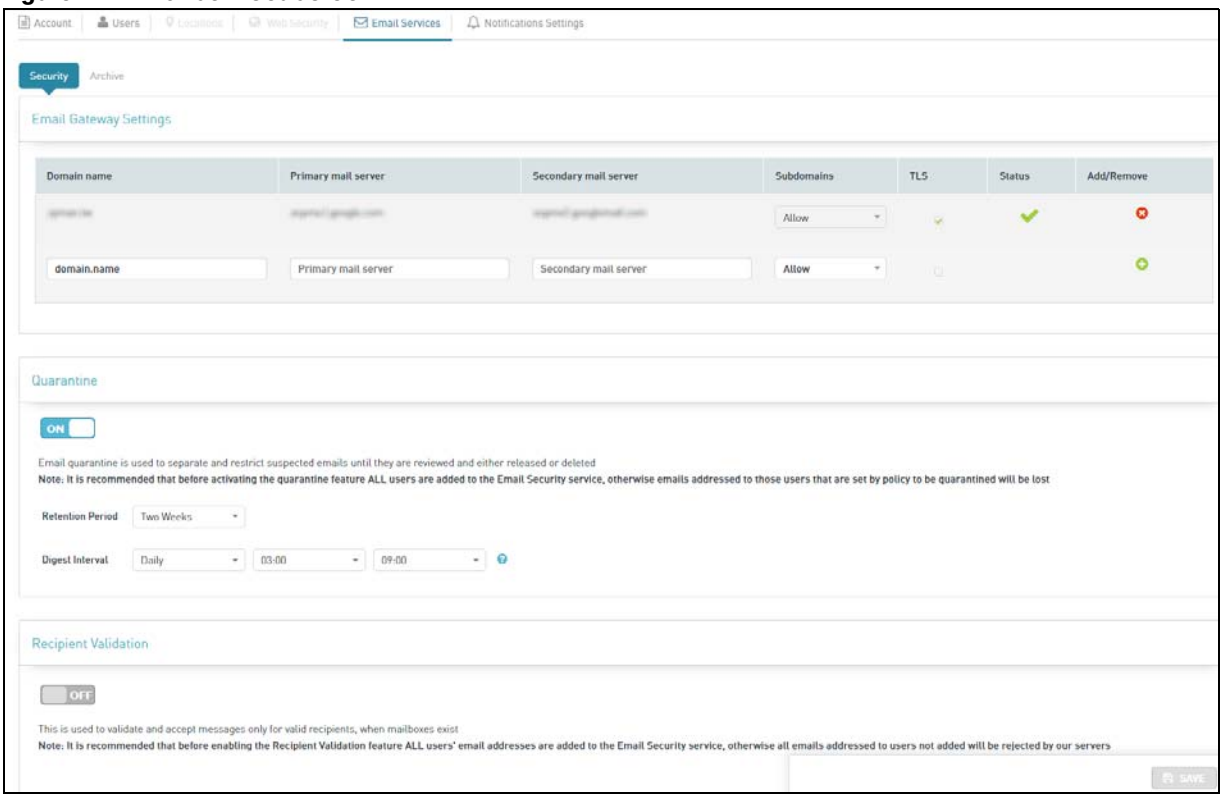
- Right-click on a group, and then select **Create Subgroup**.
  The **Create New Group** window opens.

3 Enter a unique name for the group, and then click **Create**.

6.4 Email Services Screen

Use the **Email Services** screen to configure email settings such as mail servers, quarantine, and recipient validation.

Figure 21 Email Services Screen



The following table describes the labels on this screen

Table 23 Email Services Screen

LABEL	DESCRIPTION
Email Gateway Settings	The email gateway settings allow you to specify the address of your domain's mail servers. CES forwards emails to these servers after scanning them.
Domain name	This shows the name of your email domain, for example mycompany.com. You can manage multiple email domains in the same CES organization. For details, see Section 6.4.1 on page 50.
Primary mail server	This shows the hostname, IPv4 address, or IPv6 address of the primary email server for the domain.
	Click this to edit the field.

Table 23 Email Services Screen (continued)

LABEL	DESCRIPTION
Secondary mail server	This shows the hostname, IPv4 address, or IPv6 address of the secondary mail email server for the domain.
Subdomains	This shows whether CES allows emails to subdomains of the domain, such as user@subdomain.mycompany.com. If set to **Reject** then emails to subdomains are automatically rejected.
TLS	This shows whether Transport Layer Security (TLS) encryption is enabled on the SMTP connection between CES and the domain's mail server. For security reasons, you should enable this setting if the domain's mail server supports TLS.
Status	This field shows a check mark if the domain configuration is confirmed, or **Pending** if it is not yet confirmed. After adding a new email domain, CES verifies if the primary or secondary mail server is ready to receive mail or not. For details, see Section 1.4 on page 5.
Add/Remove	Click these icons to add or remove email domains.
	Click this to remove the email domain.
	Click this to add a new email domain.
Quarantine	
ON/OFF	Click this to enable or disable the quarantine feature in CES. For details of this feature, see Section 3.4 on page 19.
Retention Period	Select how long emails are stored in the quarantine folder before being deleted. The maximum is 4 weeks.
Digest Interval	Set how often users and administrators receive a quarantine digest email. The timezone for this date and time is Central European Time (CET). The digest email contains a list of all of the recipient's quarantined emails, with the following information: • The date and time that the email was received. • The recipient's name and email address. • The sender's name, email address, domain, and X-headers. X-headers are email headers that are added into the email in addition to the standard headers, such as the To, From, and Subject • The subject line of the email.
Recipient Validation	
ON/OFF	Click this to enable or disable Recipient Validation. Recipient Validation determines how CES handles an email sent to an email address that is not associated with any CES user account. • **ON**: CES rejects the email without sending a notification to the recipient. • **OFF**: CES automatically passes the email and forwards it to the recipient. This is the default setting.

6.4.1 Adding an Email Domain

Follow the steps below to add a new email domain to CES.

1 Go to **Settings > Email Services**.

2 Under **Email Gateway Settings**, locate an empty row.

3 In the empty row under **Domain Name**, enter the name of the email domain for CES to manage.

4 Under **Primary mail server**, enter the hostname, IPv4 address, or IPv6 address of the primary email server for the domain.

5 (Optional): Under **Secondary mail server**, enter the address of the secondary email server for the domain.
This value can be a hostname, IPv4 address, or IPv6 address.

6 Select whether subdomains of the domain are supported and scanned by Cloud Email Security.
If set to **Reject**, then emails to a sub domain of the domain, for example user@subdomain.mycompany.com, are automatically rejected.

7 (Optional) Enable Transport Layer Security (TLS) encryption on the connection between Cloud Email Security and the domain's mail server.
Typically, you should enable this setting if possible.

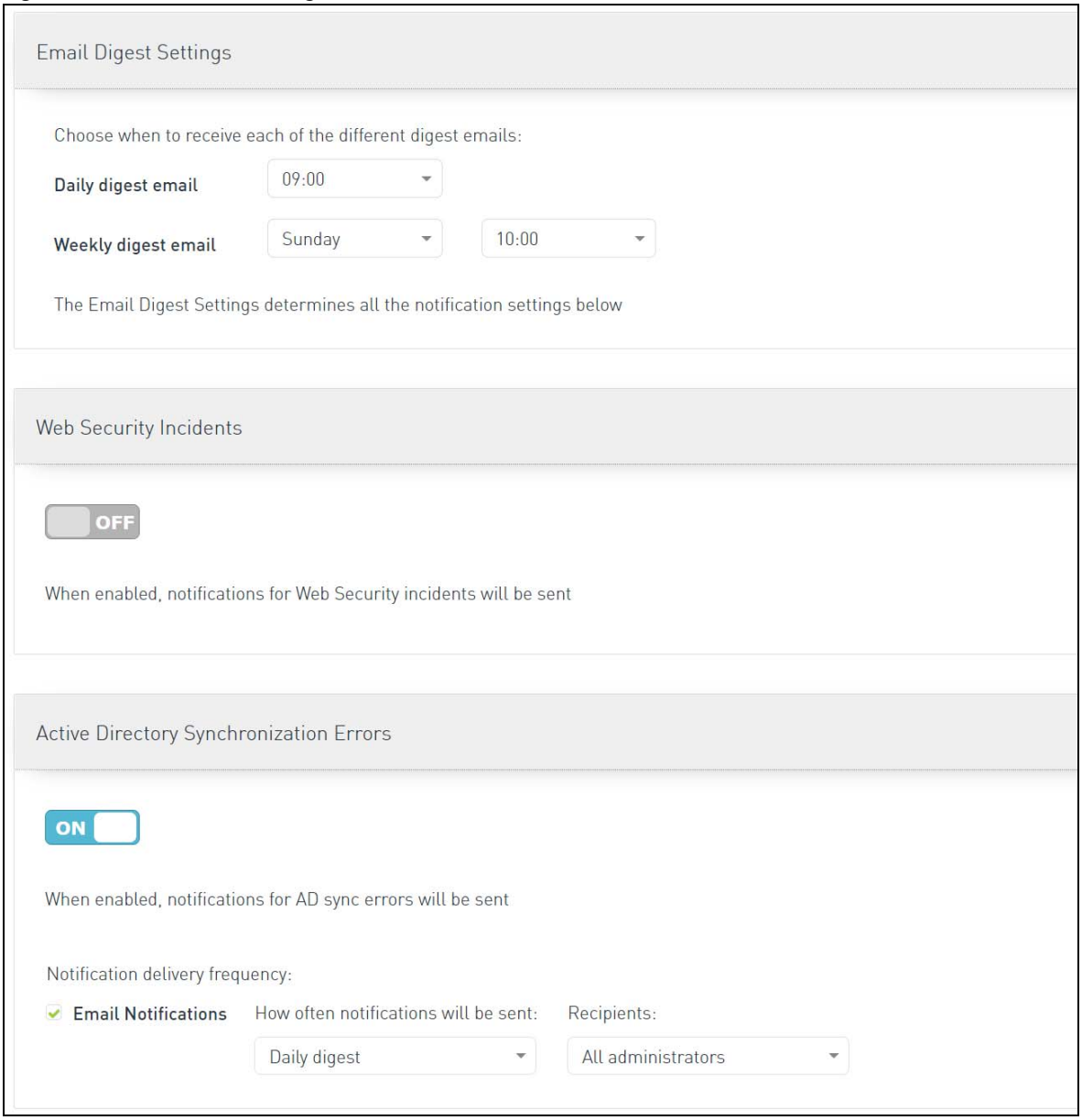
8 Click Add.

The new domain is added to the table with the status **Pending**, indicating that CES is verifying the mail server settings. Once verified then the status changes to a check mark. Then you can set the domain's MX records to point to the CES mail servers. For details on MX records, see Section 1.4 on page 5.

6.5 Notifications Settings Screen

Use the **Notification Settings** screen to configure notification settings.

Figure 22 Notification Settings Screen1

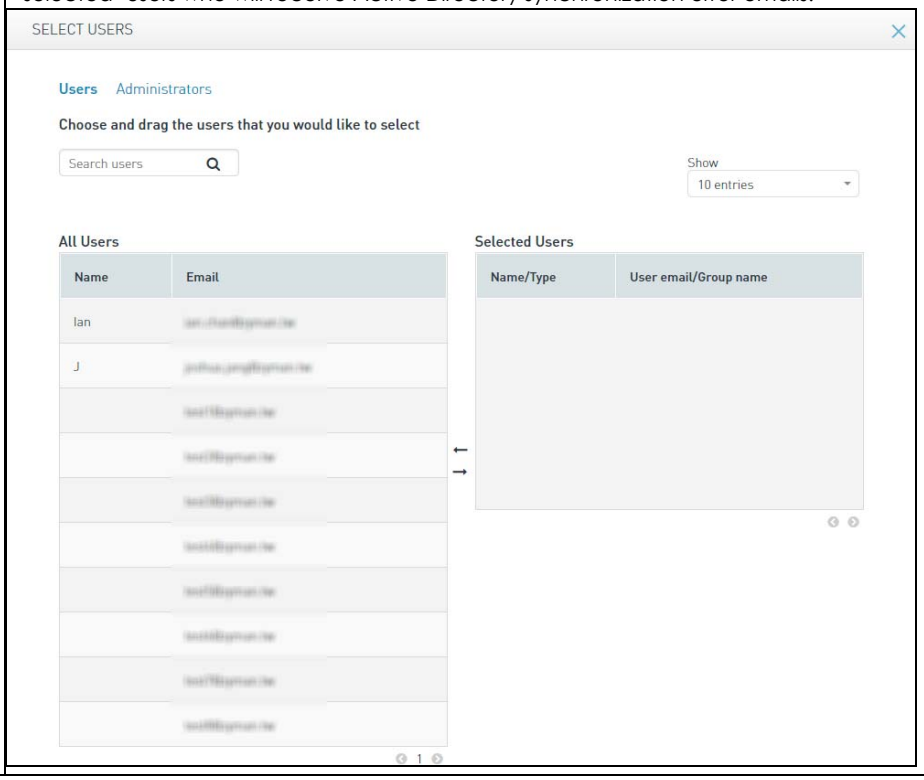


The following table describes the labels on this screen

Table 24 Notification Settings Screen

LABEL	DESCRIPTION
Email Digest Settings	
Daily digest email	Specify what time CES sends daily digest emails. Note: At the time of writing, this setting only affects Active Directory Synchronization Error mails.
Weekly digest email	Specify what day and time CES sends weekly digest emails. Note: At the time of writing, this setting only affects Active Directory Synchronization Error mails.

Table 24 Notification Settings Screen (continued)

LABEL	DESCRIPTION
Web Security Incidents	At time of writing, web security features are not supported in CES.
ON/OFF	Enable or disable notifications for web security events
Active Directory Synchronization Errors	
ON/OFF	Enable or disable notifications for errors when CES is synchronizing users and groups with Active Directory.
Email Notifications	Enable or disable email notifications for Active Directory synchronization errors.
How often notifications will be sent	Specify how often Active Directory synchronization error emails are sent to administrators. You can select daily, weekly, or whenever an error occurs (**Per Event**).
Recipients	Select who receives Active Directory synchronization error emails. You can select all administrators, or a specific set of users and administrators. For a specific set, select **List of recipients**, then click **Add Recipients**. In the dialog box use the arrows to add or remove 'selected' users who will receive Active Directory synchronization error emails. 

CHAPTER 7
Troubleshooting

This chapter offers some suggestions to solve problems you might encounter when using CES.

7.1 Active Directory Sync

The AD synchronization process fails.

If your domain is a child domain, then AD Sync Agent might not be able to automatically retrieve the domain of the server or workstation that it is installed on. To resolve this issue:

1. On the server or workstation that AD Sync Agent is installed on, go to folder **Program Files (X86) > Cyren > AdSyncAgent**.
2. Create the file *AdsyncCustomConfig.txt.*
3. Open *AdsyncCustomConfig.txt* in a text editor, and add the line *NETBIOSNAME=domain_netbios_name*, where *domain_netbios_name* is the NetBIOS name of your domain. Typically, the NetBIOS domain name is the highest sub domain of the DNS domain name. For example, for domain *company.com*, the NetBIOS name is *company*. For domain *us.company.com*, the NetBIOS name is *us*.

You can diagnose synchronization errors by checking the AD Sync Agent log:

1. On the server or workstation that AD Sync Agent is installed on, go to folder **Program Files (X86) > Cyren > AdSyncAgent**.
2. Locate and then check the file *AdSyncStatus.xml*.

7.2 General

Cloud Email Security is not scanning emails.

Each email address to be scanned must be associated with a CES user account. Emails to addresses not associated with a user account are automatically cleared and delivered to the recipient.
You can change this behavior by enabling Recipient Validation. For details, see Section 6.4 on page 49.

Cloud Email Security is not delivering emails.

- Ensure your email servers are configured correctly on the **Email Services** screen. For details, see Section 6.4 on page 49.
- There might be an issue with rule priority. For details, see Section 3.3.1 on page 17.

My mail server went down or changed IP addresses

Ensure your new email servers are configured correctly on the **Email Services** screen. For details, see Section 6.4 on page 49.

I want to know who has logged into CES and what they did. What can I do?

Check the **Audit Log** screen for changes made to settings and objects. For details, see Section 4.8 on page 37.

7.3 Licensing

My CES license has expired. What should I do?

Buy a new license and register it at myZyxel.com

I want to buy a standard license, but my trial license has not yet expired. Should I wait until the trial license expires?

No, you don't have to. The standard license can be activated during the trial, and unused time in the trial license will be added to the standard license.

I want to renew a standard license, but my existing standard license has not yet expired. Should I wait until the existing standard expires?

- If you want to renew a license with the same number of users, you don't have to wait until the existing license expires. You can activate the new license before the existing one expires and the license will be extended.

- However, if you want to renew a license with a different number of users, you must wait until the existing license expires first, before activating the new license.

How can I add more licensed users.

If you decide to add users to your existing license, you must contact support. Alternatively, buy a new license with more users.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communication products, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network products, see *https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan

- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- https://www.zyxel.com/th/th/

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Europe

Belarus

- Zyxel BY
- https://www.zyxel.by

Bulgaria

- Zyxel България

- https://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

France

- Zyxel France
- https://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

Romania

- Zyxel Romania
- https://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

- Zyxel Communications Corporation

- https://www.zyxel.com/co/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- https://www.zyxel.com/us/en/

APPENDIX B
Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.