CORVID

CYBERDEFENSE

Haven Cloud with MMS

Installation Guide

Contents

Welcome to **Haven**! In this guide, we will outline the components of the service and the steps to get your company set up. You can soon be rest assured that your company's security posture is strong.

As our POC (point-of-contact) we will work with you to make the deployment process as smooth as possible. If you have any issues in the process, please reach out using our support web portal, phone number, or email, and we will quickly jump in to assist you.

Haven Product Overview

First, let's review the key technical security controls that will be provided:

1. Managed Security Protection
    a. Network
    b. Endpoint (workstations and servers)
    c. Email
2. Managed Security Detection and Response
    a. Security Incident and Event Management
    b. 24/7/365 Security Operations
    c. Security Log Management
    d. Threat Analysis, Investigation and Response
3. End-User Security Awareness and Training
4. Vulnerability Management and Patching
5. Full Disk Encryption assistance, if needed

Typical Deployment Schedule

As the point-of-contact you may discuss an alternative deployment schedule. However, standard deployment is as follows:

WEEK 1:	Install MMS Remote Monitoring and Management (RMM, Cylance Endpoint Security, Endpoint Encryption
WEEK 1-3:	Install and Configure Mimecast Email Security
WEEK 2:	Set up Employee Education & Awareness Training
WEEK 2:	Configure Cylance Endpoint Security

Implementation

Haven is a cloud-based solution, which supports remote installation and management in coordination with our main POC.

We will provide you with access to a secure folder on our cloud drive where you will find the downloads for installation.

1. Remote Monitoring and Management (RMM) Deployment | MMS

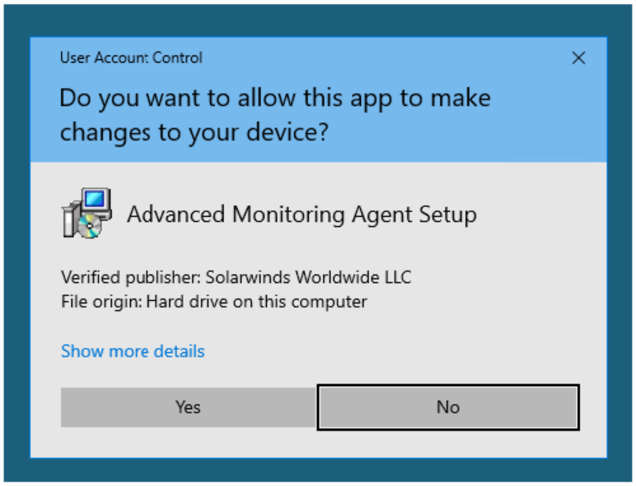
POC Action: We will work with you on the initial install on your endpoint (i.e. computer or laptop). The POC will then install the RMM agent on all the end-points identified in the service agreement. Please note that this does not include BYODs (bring your own devices).

The RMM agent enables the following for each device: persistent vulnerability scans, responsive patch updates, and daily backups (if included in package) which are saved securely offsite.

- Administrative rights are required to install the RMM agent.
- Installation takes up to 5 minutes.
- Once the agent is installed it will complete a vulnerability scan that will be used to build out the scheduling for patching of any applications that need to be updated. Typically, patches are scheduled to be installed on a recurring day and time (specific timing may be requested).
- Devices must be online during the scheduled window to be backed up and patched. After the download, it is recommended to reboot the device at your convenience.

Considerations:

- Initial onboarding will require larger volumes of data to be collected, depending on local internet connectivity speeds and the volume of data, it could take numerous hours for all data to be fully backed up. After the initial system backups and software updates are completed, subsequent backups and updates will be significantly faster.
- In cases where large backups are required, the backups will run during off hours to prevent any impact to business operations.



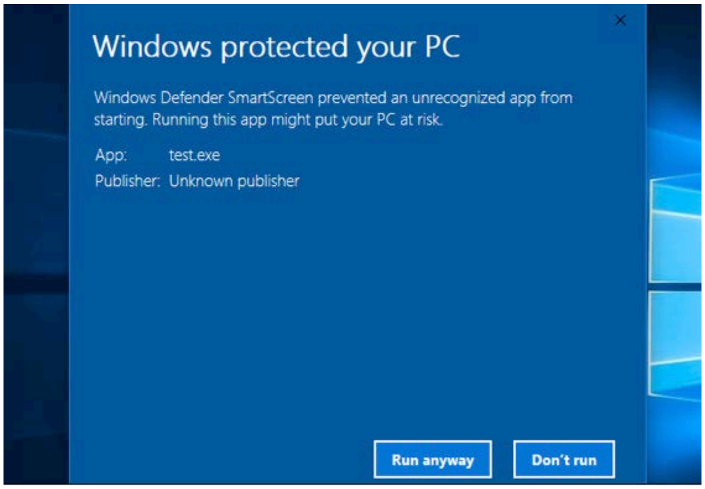
User Account Control

Do you want to allow this app to make changes to your device?

Advanced Monitoring Agent Setup

Verified publisher: Solarwinds Worldwide LLC
File origin: Hard drive on this computer

Figure 1-The agent installer may ask to allow the app to make changes to your device. Select Yes.

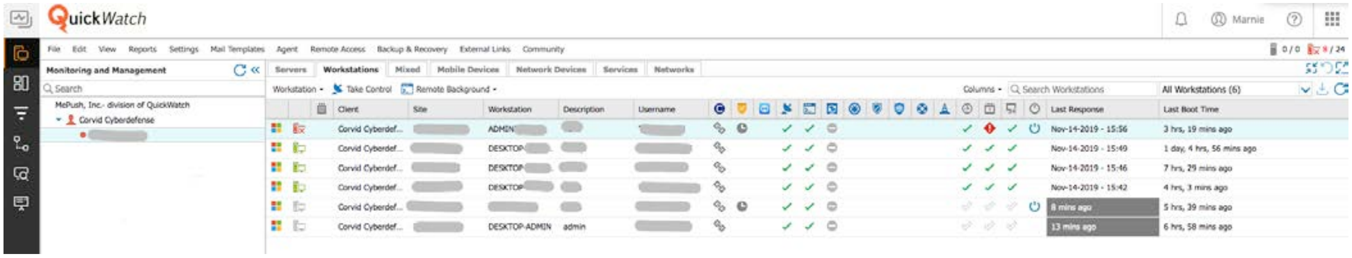


Windows protected your PC

Windows Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

App: test.exe
Publisher: Unknown publisher

Figure 2- You may also see Windows SmartScreen as for permission. Select Run anyway.



Client	Site	Workstation	Description	Username	Last Response	Last Boot Time
Corvid Cyberdef...	[redacted]	ADMIN[redacted]	[redacted]	[redacted]	Nov-14-2019 - 15:56	3 hrs, 19 mins ago
Corvid Cyberdef...	[redacted]	DESKTOP-[redacted]	[redacted]	[redacted]	Nov-14-2019 - 15:49	1 day, 4 hrs, 56 mins ago
Corvid Cyberdef...	[redacted]	DESKTOP-[redacted]	[redacted]	[redacted]	Nov-14-2019 - 15:46	7 hrs, 29 mins ago
Corvid Cyberdef...	[redacted]	DESKTOP-[redacted]	[redacted]	[redacted]	Nov-14-2019 - 15:42	4 hrs, 3 mins ago
Corvid Cyberdef...	[redacted]	[redacted]	[redacted]	[redacted]	8 mins ago	5 hrs, 39 mins ago
Corvid Cyberdef...	[redacted]	DESKTOP-ADMIN	admin	[redacted]	13 mins ago	6 hrs, 58 mins ago

Figure 3- QuickWatch Dashboard

2. Advanced Endpoint Protection | CylancePROTECT & CylanceOPTICS

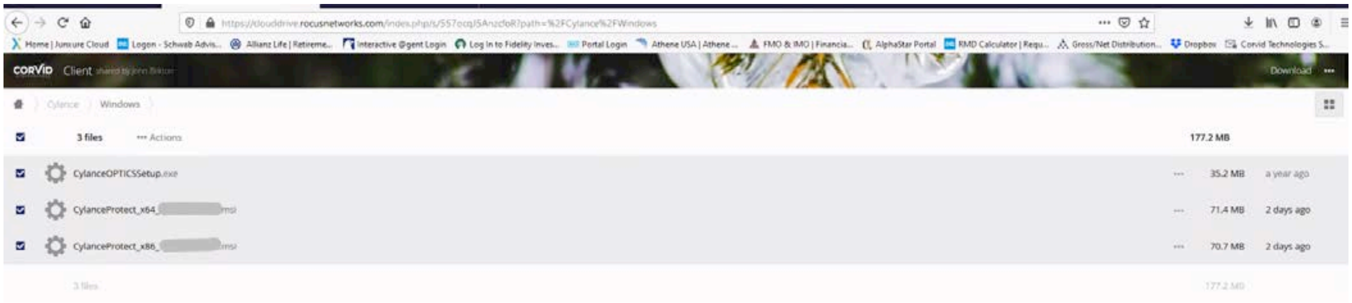
POC Action: You will perform the same process to download CylancePROTECT and CylanceOPTICS on all user devices. THIS WILL HAPPEN AUTOMATICALLY ONCE MMS IS INSTALLED.

The endpoint agent provides malware prevention using AI (artificial intelligence) and machine learning and prevents file-less attacks in memory. CylanceOPTICS performs a similar function to a flight recorder, deploying sensors into the device's operating system at various levels and against various subsystems to collect a diverse set of disparate information, then aggregates that information into a localized data store to track, alert upon, and respond to, complex malicious situations as they unfold. After the download, it is recommended to reboot the device at your convenience.

The initial scan will only require up to 6% CPU usage which means employees can continue working as usual during installation.

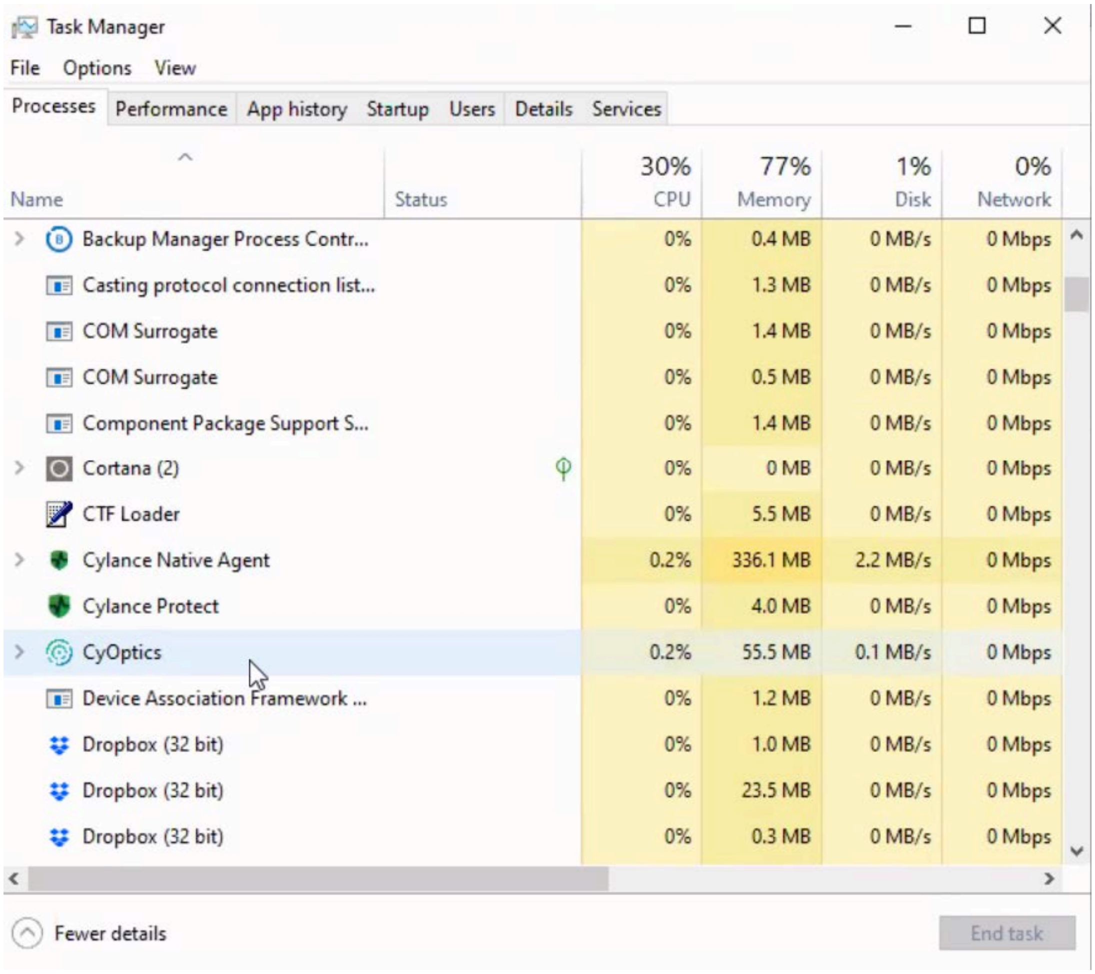
Once the scan is complete, Corvid Cyberdefense will create an auto-quarantine policy. This is after the initial installation once it is clear that the software is running smoothly.

Based on the findings from the Background Threat Detection scan, Corvid Cyberdefense will need some of your input to identify any internal applications used within the environment. With this information, we can prevent operational impact while adding preventative rules (auto-quarantine policy) to protect the organization from threats. This is also the time to remove any other anti-virus software that may have been on the devices.


https://clouddrive.rocusnetworks.com/index.php/s/557ocqJ5AnzcfoR?path=%2FCylance%2FWindows
CORVID Client
Download
Cylance
Windows
Actions

	3 files		177.2 MB	
☑	CylanceOPTICSSetup.exe	···	35.2 MB	a year ago
☑	CylanceProtect_x64_[redacted].msi	···	71.4 MB	2 days ago
☑	CylanceProtect_x86_[redacted].msi	···	70.7 MB	2 days ago
	3 files		177.2 MB	

Figure 4- Corvid Cyberdefense CloudDrive - Cylance downloads



Name	Status	30% CPU	77% Memory	1% Disk	0% Network
Backup Manager Process Contr...		0%	0.4 MB	0 MB/s	0 Mbps
Casting protocol connection list...		0%	1.3 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.4 MB	0 MB/s	0 Mbps
COM Surrogate		0%	0.5 MB	0 MB/s	0 Mbps
Component Package Support S...		0%	1.4 MB	0 MB/s	0 Mbps
Cortana (2)		0%	0 MB	0 MB/s	0 Mbps
CTF Loader		0%	5.5 MB	0 MB/s	0 Mbps
Cylance Native Agent		0.2%	336.1 MB	2.2 MB/s	0 Mbps
Cylance Protect		0%	4.0 MB	0 MB/s	0 Mbps
CyOptics		0.2%	55.5 MB	0.1 MB/s	0 Mbps
Device Association Framework ...		0%	1.2 MB	0 MB/s	0 Mbps
Dropbox (32 bit)		0%	1.0 MB	0 MB/s	0 Mbps
Dropbox (32 bit)		0%	23.5 MB	0 MB/s	0 Mbps
Dropbox (32 bit)		0%	0.3 MB	0 MB/s	0 Mbps

3. Next Generation Firewall & VPN | Palo Alto Networks GlobalProtect

POC Action: You will perform the same process to download GlobalProtect on all user devices.

Corvid Cyberdefense will deploy a VPN (virtual private network) agent that will allow end user traffic to be pushed through a cloud-based firewall we affectionately refer to as the Haven Cloud. This will allow Corvid Cyberdefense to create a hardened security posture that only allows pre-approved applications and URLS to be active within the environment, thus reducing your overall risk of harm.

Corvid Cyberdefense has a standard firewall security policy for all clients. However, you may request custom rules or applications to be allowed on your network. Please inform us if you would like us to work with you on any unique exclusions. We continuously update our rules based on emerging threats we see in the wild.

There are two options for how the VPN agent is configured:

1. Always on VPN
   - Users have no option to turn off/disconnect the vpn agent
   - Recommended deployment method for company managed workstations
2. On-demand VPN
   - Users can choose to turn the VPN off and on
   - Recommended deployment method for Bring Your Own Device (BYOD)

4. Secure Email Protection | Mimecast

POC Action: Please provide administrative rights (user name and password) to the DNS records and your email domain host (e.g. O365) in order for Corvid Cyberdefense to deploy Mimecast. Another option is to have your IT Administrator work with us to coordinate changing the mail routing and DNS records.

Information will need to be distributed to your end users to make them aware of the changes they may see when sending or receiving email. While these changes are minor, they will be critical to ensure users can be self-sufficient accessing their email quarantine folders.

The e-mail security solution is powered by Mimecast. Mimecast provides email security controls designed to protect end users from advanced threats and attacks. Mimecast provides:

- Enhanced security with spam and phishing detection
- Analysis of URLs and attachments for vulnerabilities or threats
- Ability to easily send encrypted emails containing sensitive information

There are multiple steps in securing your company's email.

Deployment steps:

a. Educate the end users on what to expect
   - Templated email provided to main contact to send to all users

b. Add user accounts to the Mimecast cloud tenant

c. Create connectors for mail flow through the Secure Email gateway
   - This requires access to both the DNS and domain host records

d. Monitor outgoing mail recipients to develop a safe recipient and sender list

e. Monitor inbound mail senders to develop a safe recipient and sender list

f. Push Mimecast plugin to customer Outlook email clients (optional)

g. Create policies for your environment
   - Corvid Cyberdefense will set up baseline policies

h. Add more advanced policies after traffic flow analysis
   - Typically after 3-7 days of traffic analysis

5. Disk Encryption | BitLocker or File Vault

POC Action: Please confirm your operating system is Windows 10 Pro or iOS X 10.3 or later and up to date, and you have a dedicated USB to store the encryption key(s).

Corvid Cyberdefense can guide you to install whole disk encryption on desktops and laptops. Whole disk encryption ensures data is protected in the event of theft or loss. Encryption will be enforced on all Windows 10 Pro and MacOS X 10.3 or later systems.

Disk encryption is enforced using the native encryption capabilities within Windows 10 Pro (BitLocker) and MacOS (File Vault).

Corvid Cyberdefense can provide you with an encryption installation guide.

Note on encryption key: Because there may be a circumstance where you are prompted for a recovery key, it is very important for you to keep the encryption key on a dedicated USB (also printed) and stored in a safe for emergency use. While we offer our clients the option of also having the key stored in an encrypted file vault that we maintain, it is not our recommendation due to the potential emergency need or use for this information.

6. Education and Awareness | Symbol and Ninjio

POC Action: Corvid Cyberdefense will use the email addresses provided by the POC to implement the training program.

We will implement a security awareness education program for all employees. Training includes 3-5 minute micro-training and awareness videos that will be emailed monthly to all users.

In addition to micro-training and awareness videos, simulated phishing campaigns will be sent monthly to your users. Customized phishing emails will be created and sent to your organization. Results will be reported to the POC for your company to track user progress through repetitive training.

Note on Trusted Access

Corvid Cyberdefense is available to help guide you in the selection of a Multi-Factor Authentication (MFA) application. MFA is a security mechanism that requires an individual to provide two or more credentials in order to authenticate their identity. It prohibits someone from accessing your device or account without being contacted with a short-term code to enter as a secondary verification, most often on a mobile phone.

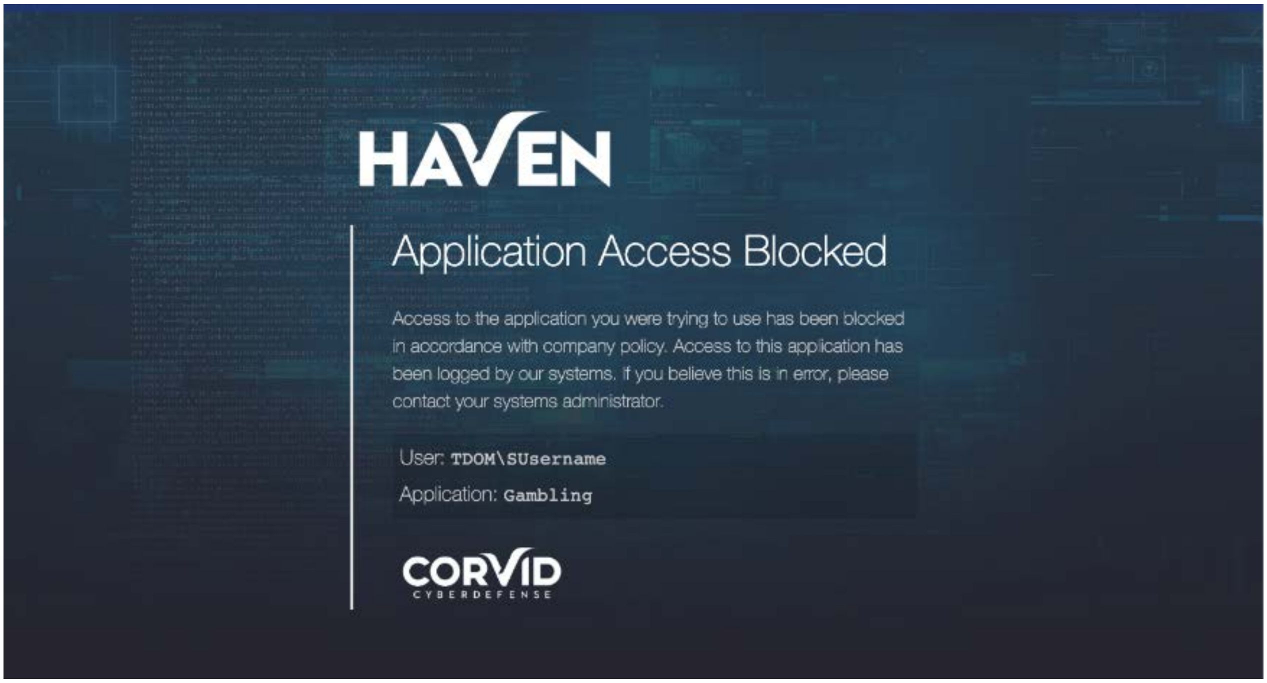
We recommend DUO and Google Authenticator for 2-step verification. These can be found using your mobile phone to download the app and create an account.

Thank you for choosing Corvid Cyberdefense as your security provider. As always, please don’t hesitate to reach out if you need assistance.

–Corvid Cyberdefense

Appendix A - Network Security Solution | Palo Alto GlobalProtect

The Network Security Solution is a next-generation firewall that examines all traffic coming in and out of your organization's network. Corvid Cyberdefense creates sets of policies to allow or deny specific types of traffic (for example, blocking any web traffic categorized as gambling or pornography). In addition to examining and filtering web traffic, this security solution can examine and manage computer applications and devices connected to your network. Daily network security happens almost entirely behind the scenes; the only time you will notice the firewall working is if you encounter a website that has been blocked, in which case you will see an error page like the one below. If you believe a website has been blocked erroneously, you can submit a Support Ticket to investigate and remediate if the site is determined to be safe or flagged as a false positive.



HAVEN

Application Access Blocked

Access to the application you were trying to use has been blocked in accordance with company policy. Access to this application has been logged by our systems. If you believe this is in error, please contact your systems administrator.

User: TDOM\SUsername

Application: Gambling

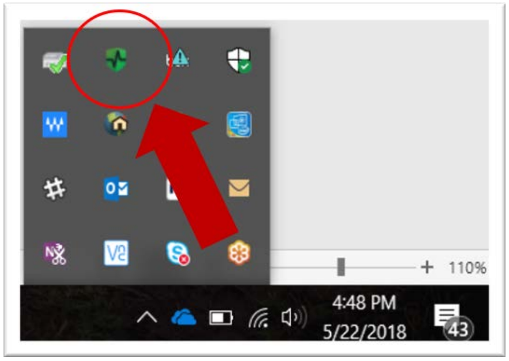
CORVID
CYBERDEFENSE

In the case of a false positive, please notify your POC and have them submit a request to have the site unblocked if needed for business purposes.

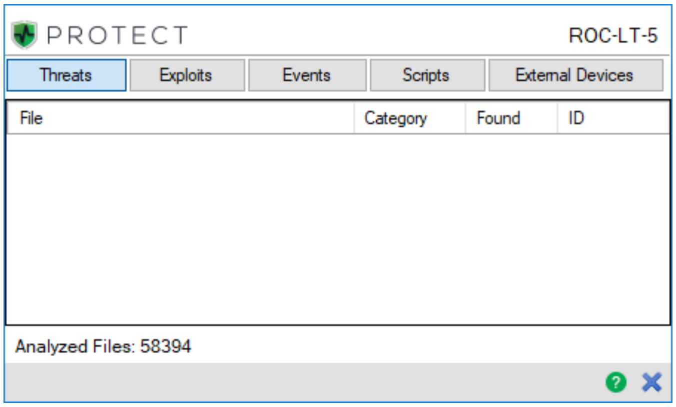
Appendix B – Endpoint Security Solution | Cylance

In the event a threat or malware gets past your organization's Network Security Solution or Email Security Solution, reaching an endpoint (typically either a workstation or a server). CylancePROTECT is the next-generation Endpoint Security Solution. Cylance utilizes machine learning to identify and prevent malware, ransomware, advanced threats, such as zero-day threats, and malicious documents and scripts from executing and infecting your systems.

Once installed, the Cylance agent will run in the background, requiring no further action on your part. You can tell that the client is running and view any alerts by looking at your computer's system tray and selecting the icon shown right.



If you attempt to open a malicious file and Cylance blocks it, you may receive a notification informing you of the block event, assuming your organization has enabled notifications (which we don't recommend). In the event you do receive a block notification and believe it to be in error, you should contact the company POC who can work with Corvid Cyberdefense to investigate the file to see if it is truly malicious or if it is being erroneously blocked.



File	Category	Found	ID

Analyzed Files: 58394

Appendix C - E-mail Security Solution Set-Up | Mimecast

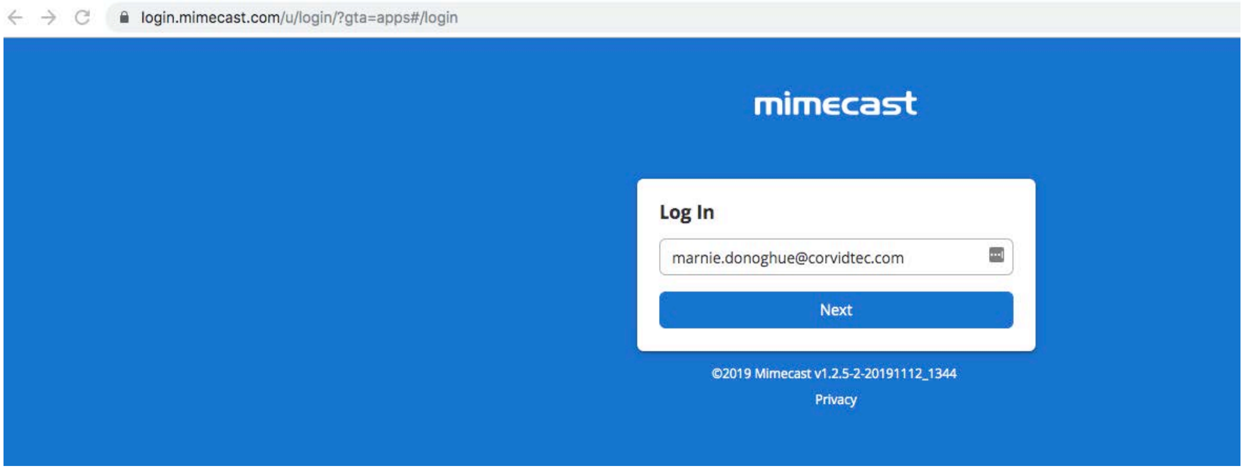
The Haven E-mail Security Solution is powered by Mimecast. Mimecast provides email security controls designed to protect end users from advanced threats and attacks. Mimecast provides:

- Enhanced security with spam and phishing detection
- Analysis of URLs and attachments for vulnerabilities or threats
- Ability to easily send encrypted emails containing sensitive information
- Employee training and awareness

Mimecast Activation

Corvid Cyberdefense will work with your organizations Point-of-Contact to create user Mimecast accounts. Alternatively, the following process can be used to activate individual Mimecast accounts after receiving an email notification:

1. Go to https://login.mimecast.com. This is the Mimecast Personal Portal. ***We recommend bookmarking this webpage in your browser.***

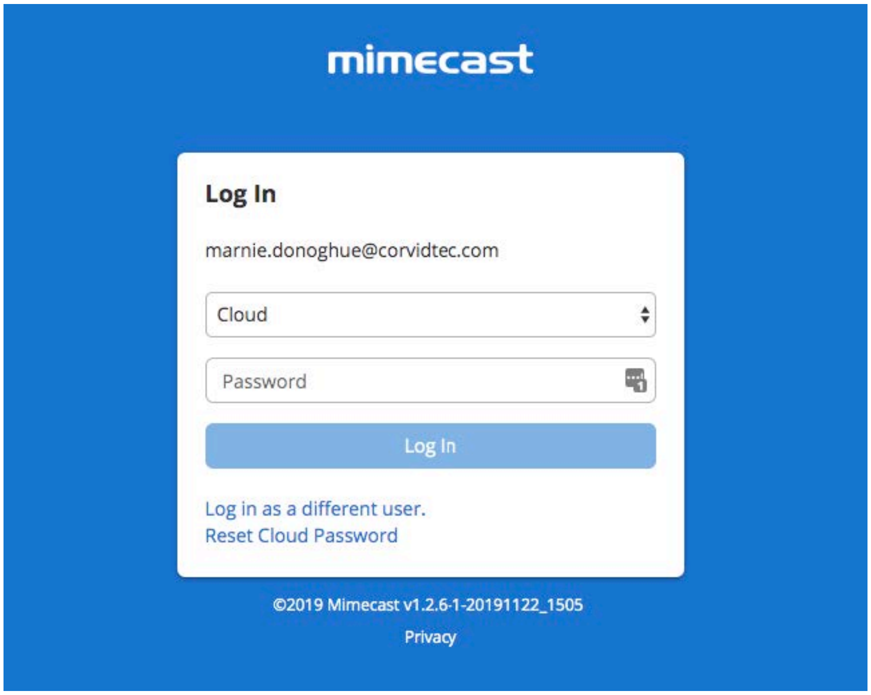


login.mimecast.com/u/login/?gta=apps#/login

mimecast
Log In
marnie.donoghue@corvidtec.com
Next
©2019 Mimecast v1.2.5-2-20191112_1344
Privacy

2. Enter your email address and select "Next."

3. Below the "Log In" button, select the option "Reset Cloud Password."



mimecast

Log In

marnie.donoghue@corvidtec.com

Cloud

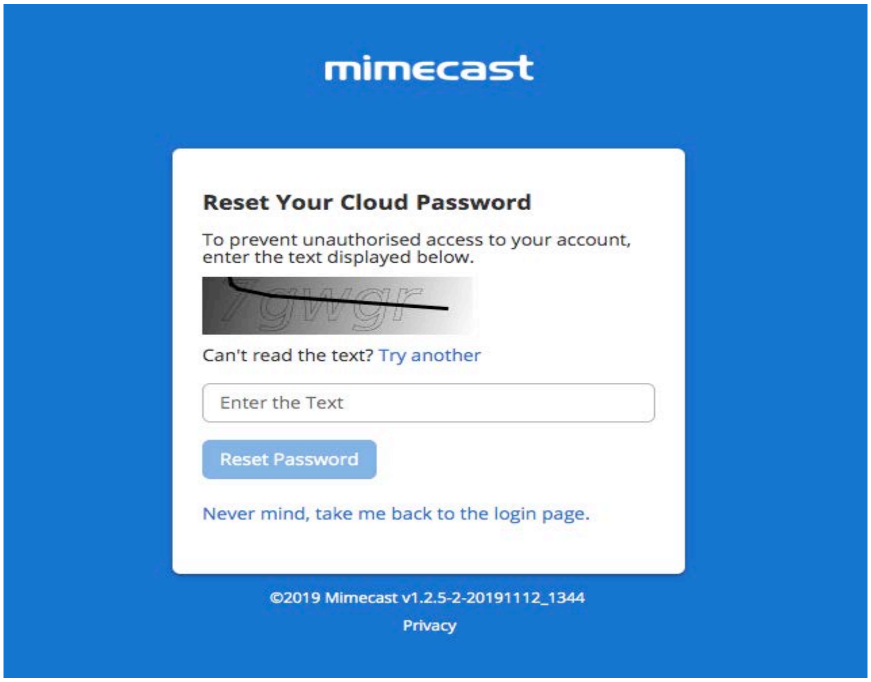
Password

Log In

Log in as a different user.
Reset Cloud Password

©2019 Mimecast v1.2.6-1-20191122_1505
Privacy

4. Enter the Captcha text for security purposes and select “Reset Password.”



mimecast

Reset Your Cloud Password

To prevent unauthorised access to your account, enter the text displayed below.

Can't read the text? Try another

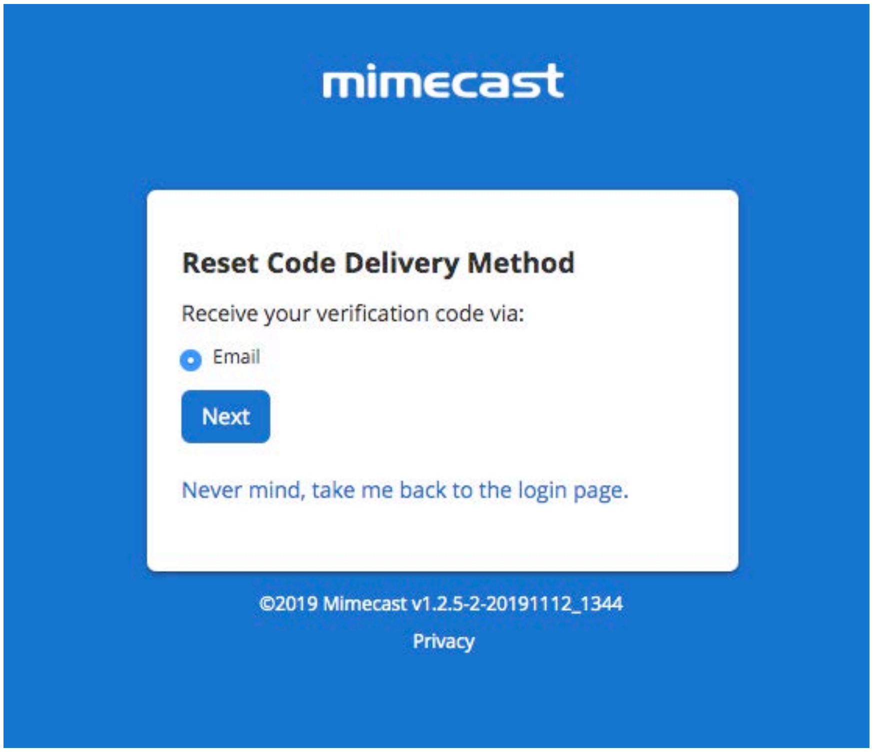
Enter the Text

Reset Password

Never mind, take me back to the login page.

©2019 Mimecast v1.2.5-2-20191112_1344
Privacy

5. Select the password reset link delivery method. Generally, “Email” should be the only option available and the default selection. Select “Next” to continue.



mimecast

Reset Code Delivery Method

Receive your verification code via:

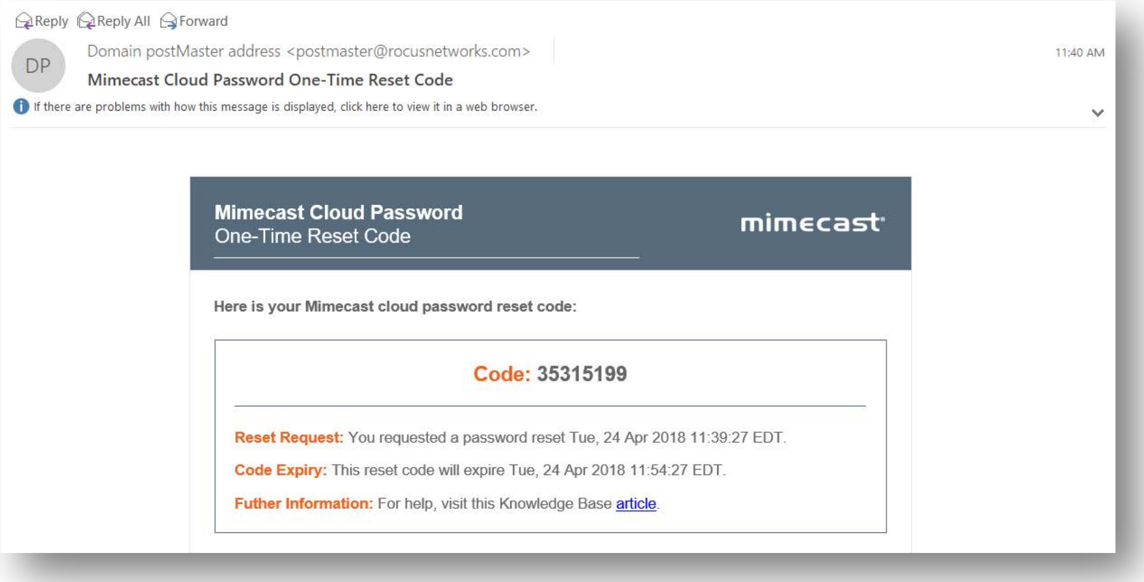
● Email

Never mind, take me back to the login page.

©2019 Mimecast v1.2.5-2-20191112_1344

Privacy

6. An email from sender "Mimecast Domain Postmaster" will be delivered to the user mailbox with a one-time password reset code.



Domain postMaster address <postmaster@rocusnetworks.com>

11:40 AM

Mimecast Cloud Password One-Time Reset Code

If there are problems with how this message is displayed, click here to view it in a web browser.

Mimecast Cloud Password
One-Time Reset Code

mimecast

Here is your Mimecast cloud password reset code:

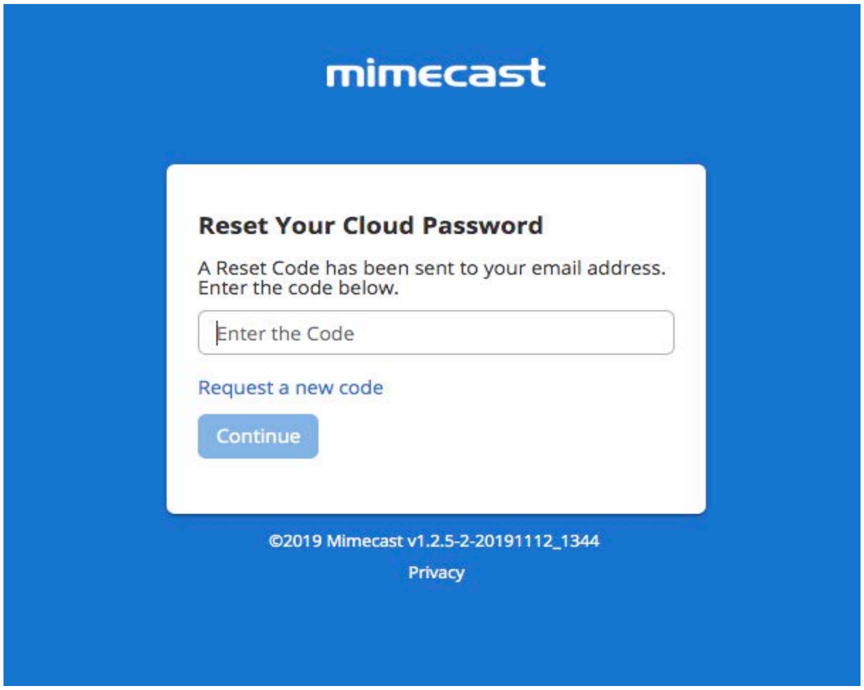
Code: 35315199

Reset Request: You requested a password reset Tue, 24 Apr 2018 11:39:27 EDT.

Code Expiry: This reset code will expire Tue, 24 Apr 2018 11:54:27 EDT.

Futher Information: For help, visit this Knowledge Base article.

7. Enter the one-time passcode from the email into the empty field in your browser.

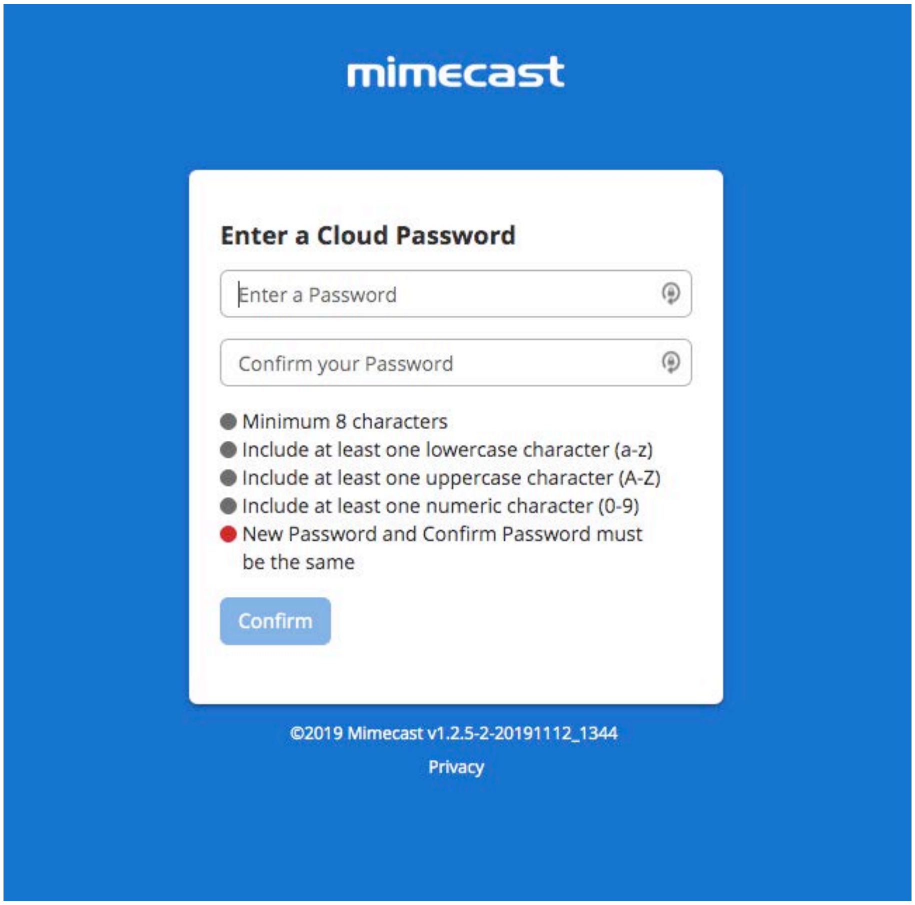


Reset Your Cloud Password

A Reset Code has been sent to your email address. Enter the code below.

©2019 Mimecast v1.2.5-2-20191112_1344

8. Create your new unique password by following the instructions. Select “Confirm” once all password criteria are check-marked green.

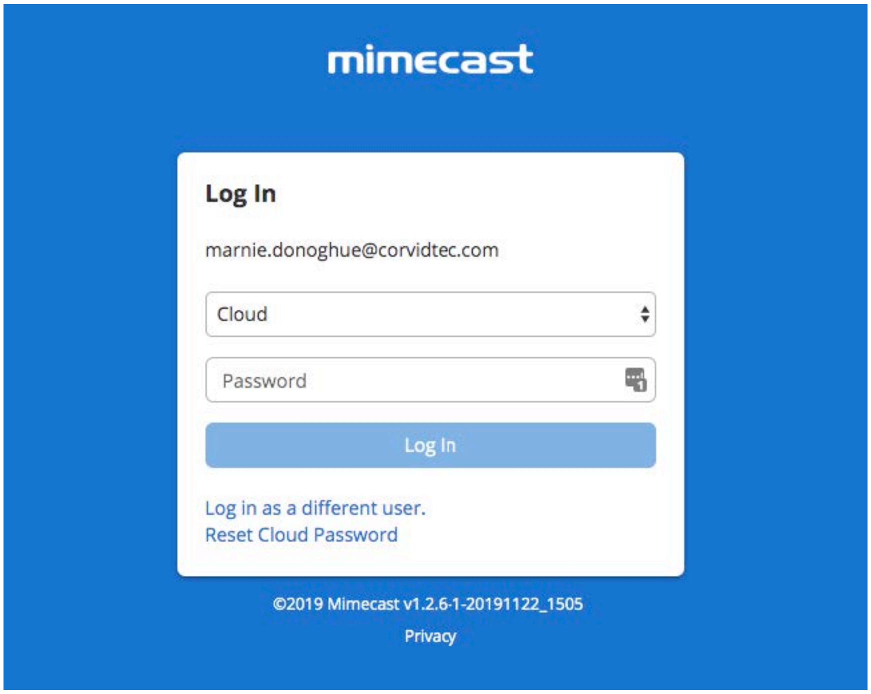


Enter a Cloud Password

- ● Minimum 8 characters
- ● Include at least one lowercase character (a-z)
- ● Include at least one uppercase character (A-Z)
- ● Include at least one numeric character (0-9)
- ● New Password and Confirm Password must be the same

©2019 Mimecast v1.2.5-2-20191112_1344

9. You will be redirected back to the login page. Ensure the dropdown box reads "Cloud" and **not** "Domain" and login with your new password. After a successful login, you will be taken to your Mimecast Online Mailbox. Further down, this guide will explain how to use this mailbox.



mimecast

Log In

marnie.donoghue@corvidtec.com

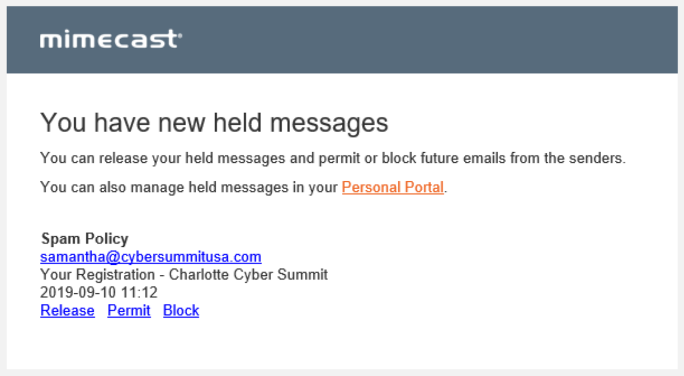
Cloud

©2019 Mimecast v1.2.6-1-20191122_1505

Privacy

How will my email change?

Throughout the day, you will receive digest emails from "Domain Postmaster Address" with the subject line "[Postmaster] Messages on Hold" listing emails that were quarantined from your inbox. For each quarantined email, you have the option to Release, Block, or Permit.



mimecast

You have new held messages

You can release your held messages and permit or block future emails from the senders.

You can also manage held messages in your Personal Portal.

Spam Policy
samantha@cybersummitusa.com
Your Registration - Charlotte Cyber Summit
2019-09-10 11:12
Release Permit Block

Release: Releases the email from the quarantine queue and send it to your Inbox; future emails from this sender may still be placed On Hold.

Block: Rejects the email and adds the sender's address to your personal block list to prevent receiving future emails from the sender.

Permit: Permits or delivers the email to your inbox and adds the sender's address to your personal permit list to allow future emails from this sender. See the “Note” below regarding permitted senders that continue to be quarantined.

Note: Spam Filter policies implemented for your organization may cause emails to be quarantined. In some cases, permitting a sender will still result in their emails being quarantined. If this occurs, there are likely other Policy Rules blocking the email based on matching characteristics. Please contact Corvid Cyberdefense Support for assistance.

If you do not select one of the above options, the email will remain in your “on hold” inbox. You can access emails in your “on hold” inbox by either logging into the Mimecast web portal through your browser (at https://login.mimecast.com), the Mimecast smartphone application (available for iOS and Android), or the Mimecast Outlook Plugin.

Mimecast Plug-in

Note: The Mimecast Plugin is currently only available for Outlook users. If your organization does not use Outlook, skip to the section “What is Mimecast.com for?”

The Mimecast Plugin for Outlook allows you to access your online inbox and hold queue, manage your blocked senders list, report spam and phishing emails, and more, all from the Outlook application.

Installing the Mimecast Plugin

Your organization may have the ability to remotely push this plugin to users. Alternately, your organization may have security controls in place requiring credentials to download plugins such as Mimecast for Outlook. If your IT administrator gives you the ability to download the plugin, follow these steps.

1. Close Microsoft Outlook.
2. Go to: https://community.mimecast.com/community/knowledge-base/application-downloads/pages/mimecast-for-outlook and then select whether to download the 32-bit or 64-bit client (most users on Windows 7 or above will need the 64-bit client).
3. Run the Mimecast for Outlook installer.
4. When the welcome window is displayed, click the Next button to start the installation.
5. Read and accept the End User License Agreement.
6. Click the Next button. Next the installer will check your system to ensure all technical prerequisites are met and that Outlook is closed.
7. Once all prerequisite checks have been performed, click the Next button to continue with the installation.
8. Specify the Installation Directory (typically this is the default folder location suggested unless specified otherwise by your administrator).
9. Click the Install button to begin the installation.
10. Once complete, click the Finish button. Microsoft Outlook should start automatically when exiting the installation wizard.
11. As with any Windows application installation, we recommend restarting your computer to ensure installation was successful.

Authenticating the Mimecast Plugin

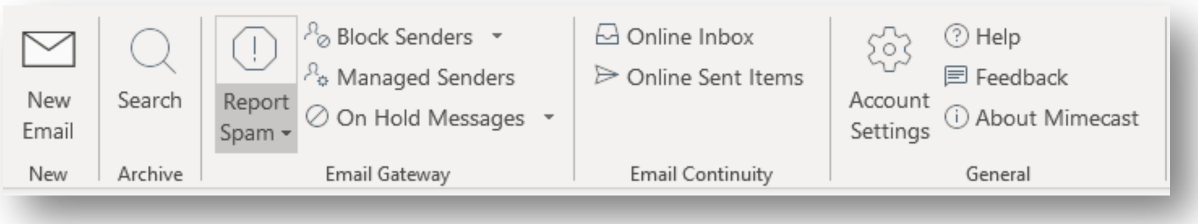
After installing the Outlook plugin, Outlook should start automatically. To authenticate your Mimecast account and enable the Mimecast ribbon function, follow these steps.

1. Navigate to the Mimecast ribbon in Outlook.
2. Under the “General Selection” select “Account Settings”.
3. You will be taken to the Authentication dialogue box. Select “Fix” and enter your credentials.

Note: If you do not have your Mimecast credentials, please contact your IT administrator or follow the password reset process outlined in the “Mimecast Activation” section.

Navigating the Mimecast Ribbon

Below is a sample of what the ribbon in your Outlook application may look like:



In the “Archive” section of the ribbon, you can:

- Search for archived files and documents.
- Export search results back into Outlook.

In the “Email Gateway” section of the ribbon, you can:

- Report suspected spam emails, sending them to a blocked spam folder.
- Report suspected phishing emails to your Mimecast administrator for further investigation.
- Manage your blocked senders list (add or remove blocked senders).
- View your email hold/quarantine queue – if you do not take action on an email through the daily digest emails, you can access that email through this ribbon menu option (detailed below).

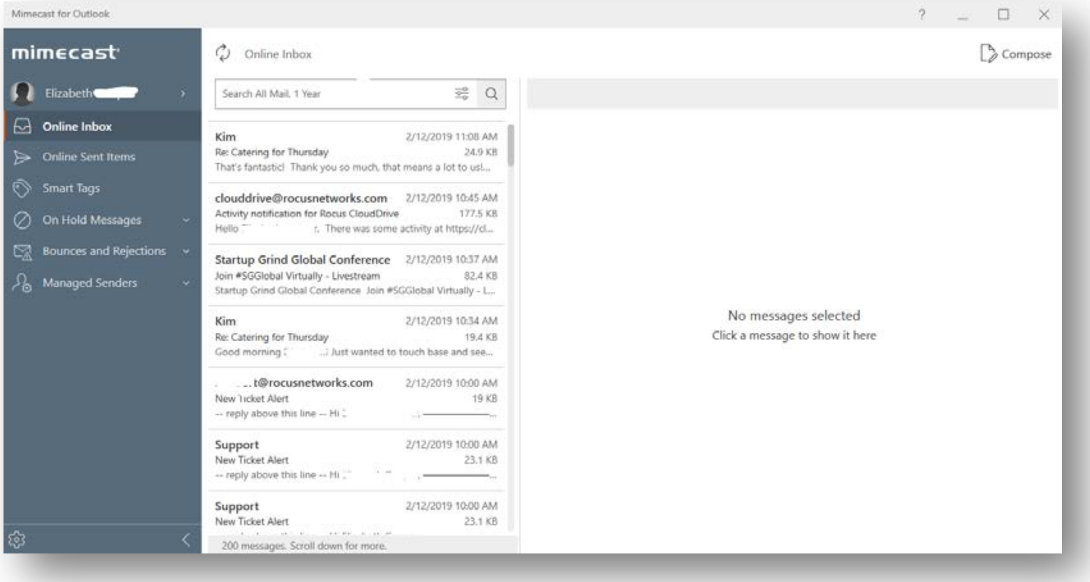
In the “Email Continuity” section of the ribbon, you can:

- Check your online inbox (useful if your Outlook is having trouble connecting to your Exchange server).

In the “Account Settings” section of the ribbon, you can:

- Select “help” to take you to the Mimecast Knowledge Base.
- Select “About Mimecast” to verify you are running the most up-to-date version of the plugin.
- Send Feedback. **Note that this feedback only goes to Mimecast, not to your IT team or Corvid Cyberdefense.**Your Online Inbox

Selecting “Online Inbox” in the Mimecast ribbon, your online inbox will pop open in another window. This allows you to access your inbox and send and receive mail as usual in the event Outlook is unable to connect to your mail server. You can also use your Online Inbox to access your hold queue and view messages that have been blocked or bounced due to the Mimecast policies implemented by your organization.



Kim 2/12/2019 11:08 AM
Re: Catering for Thursday 24.9 KB
That's fantastic! Thank you so much, that means a lot to us!...

clouddrive@rocusnetworks.com 2/12/2019 10:45 AM
Activity notification for Rocus CloudDrive 177.5 KB
Hello [redacted]r. There was some activity at https://cl...

Startup Grind Global Conference 2/12/2019 10:37 AM
Join #SGGlobal Virtually - Livestream 82.4 KB
Startup Grind Global Conference Join #SGGlobal Virtually - L...

Kim 2/12/2019 10:34 AM
Re: Catering for Thursday 19.4 KB
Good morning [redacted] Just wanted to touch base and see...

[redacted]t@rocusnetworks.com 2/12/2019 10:00 AM
New Ticket Alert 19 KB
-- reply above this line -- Hi [redacted]

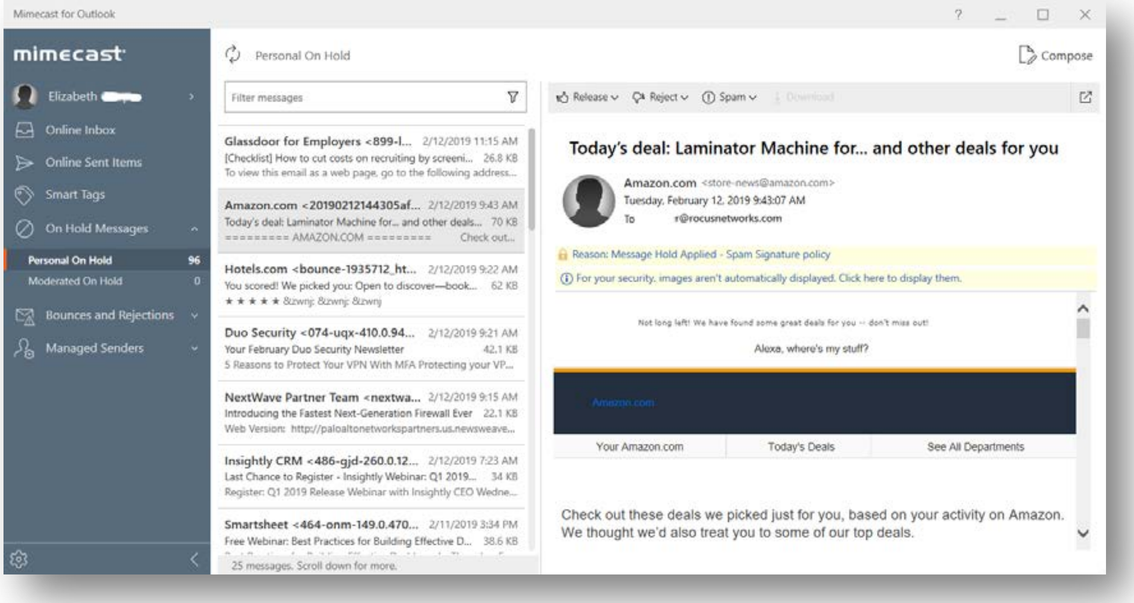
Support 2/12/2019 10:00 AM
New Ticket Alert 23.1 KB
-- reply above this line -- Hi [redacted]

Support 2/12/2019 10:00 AM
New Ticket Alert 23.1 KB

200 messages. Scroll down for more.

No messages selected
Click a message to show it here

To see emails in quarantine before your next digest email, select "On Hold Messages" in the left column. This will display all of your messages currently on hold. You can view why the message was quarantined and choose to release the email, permit the sender, permit the domain, reject the sender, reject the domain, or mark the email as suspected spam or phishing for further investigation.



Glassdoor for Employers <899-I... 2/12/2019 11:15 AM
[Checklist] How to cut costs on recruiting by screeni... 26.8 KB
To view this email as a web page, go to the following address...

Amazon.com <20190212144305af... 2/12/2019 9:43 AM
Today's deal: Laminator Machine for... and other deals... 70 KB
========= AMAZON.COM ========= Check out...

Hotels.com <bounce-1935712_ht... 2/12/2019 9:22 AM
You scored! We picked you: Open to discover—book... 62 KB
★ ★ ★ ★ ★ &zwnj; &zwnj; &zwnj

Duo Security <074-uqx-410.0.94... 2/12/2019 9:21 AM
Your February Duo Security Newsletter 42.1 KB
5 Reasons to Protect Your VPN With MFA Protecting your VP...

NextWave Partner Team <nextwa... 2/12/2019 9:15 AM
Introducing the Fastest Next-Generation Firewall Ever 22.1 KB
Web Version: http://paloaltonetworkspartners.us.newsweave...

Insightly CRM <486-gjd-260.0.12... 2/12/2019 7:23 AM
Last Chance to Register - Insightly Webinar: Q1 2019... 34 KB
Register: Q1 2019 Release Webinar with Insightly CEO Wedne...

Smartsheet <464-onm-149.0.470... 2/11/2019 3:34 PM
Free Webinar: Best Practices for Building Effective D... 38.6 KB

25 messages. Scroll down for more.

Today's deal: Laminator Machine for... and other deals for you

Amazon.com <store-news@amazon.com>
Tuesday, February 12, 2019 9:43:07 AM
To [redacted]r@rocusnetworks.com

Reason: Message Hold Applied - Spam Signature policy

For your security, images aren't automatically displayed. Click here to display them.

Not long left! We have found some great deals for you -- don't miss out!

Alexa, where's my stuff?

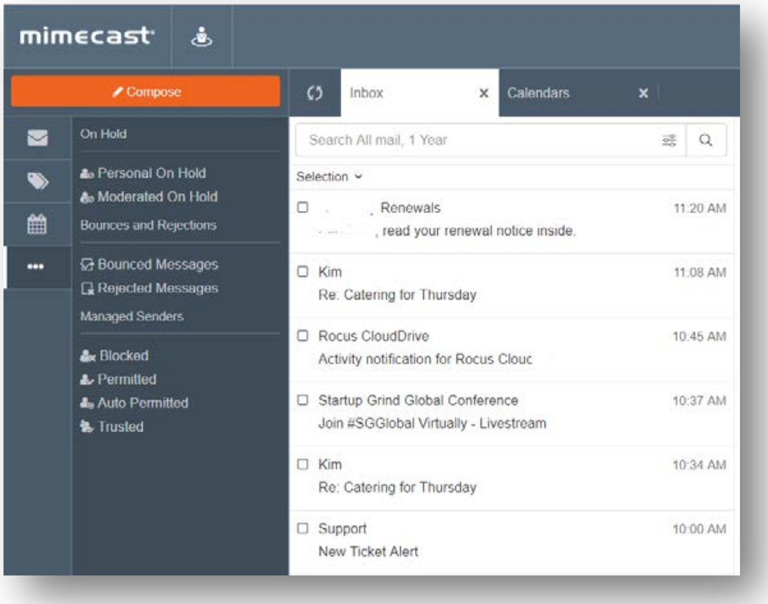
Amazon.com

Check out these deals we picked just for you, based on your activity on Amazon. We thought we'd also treat you to some of our top deals.

What is Mimecast.com for?

The online Mimecast user interface (accessed at https://login.mimecast.com) is a secure web-based portal offering the following features:

- Manage user account information
- Update user preferences.
- Create and manage trusted and blocked sender lists.
- Search email logs.
- Access to inbox and send/receive emails similar to a typical email client.



□ [redacted] Renewals 11:20 AM
[redacted] read your renewal notice inside.

□ Kim 11:08 AM
Re: Catering for Thursday

□ Rocus CloudDrive 10:45 AM
Activity notification for Rocus Clouc

□ Startup Grind Global Conference 10:37 AM
Join #SGGlobal Virtually - Livestream

□ Kim 10:34 AM
Re: Catering for Thursday

□ Support 10:00 AM
New Ticket Alert

If your organization uses Microsoft Outlook, almost all Mimecast features will be available to you through the Mimecast ribbon in Outlook, so you will rarely need to log into the Mimecast.com website. For users not using Microsoft Outlook, we recommend bookmarking the https://login.mimecast.com website. This will be your primary destination for managing your hold/quarantine queues, sender lists, and more.

Other Mimecast Features

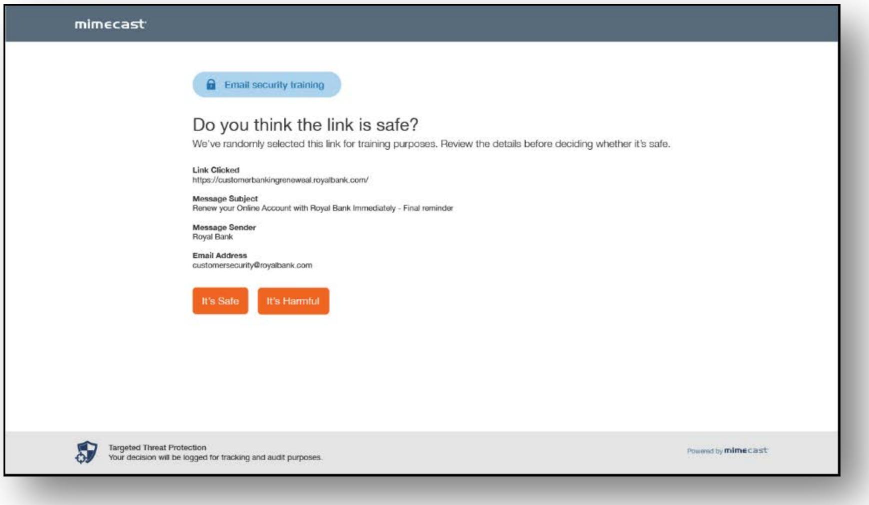
The following features may not be enabled for all users at all organizations. Please speak with your organization's primary IT contact for additional information.

Device Registration

A feature of Mimecast's Targeted Threat Protection is user device registration. The first time you click an email link on a new device, use a new browser, or clear your browser cache, you will be redirected to a registration page to register the new device or browser to your Mimecast account. Through this cookie-based system, Mimecast tracks who opens links, the device the link was opened on, and what links have been opened; this is useful in the event someone clicks a malicious link, intentionally or otherwise, as it allows administrators to identify "Patient Zero" and create a remediation strategy. Depending on your organization's security settings, you may have to periodically re-enroll your device (typically every 90 days).

URL Testing and Training

To enhance employee education and awareness, at least 5% of all URLs opened (your organization can opt to make this percentage higher), Mimecast will redirect the user to a training page where they will be shown information about the link opened and asked to re-affirm that the link is safe.



Do you think the link is safe?

We've randomly selected this link for training purposes. Review the details before deciding whether it's safe.

Link Clicked
https://customerbankingreneweal.royalbank.com/

Message Subject
Renew your Online Account with Royal Bank Immediately - Final reminder

Message Sender
Royal Bank

Email Address
customersecurity@royalbank.com

Targeted Threat Protection
Your decision will be logged for tracking and audit purposes.

What happens next depends on:

- The settings configured in the organization's URL protection policies.
- Whether the URL is considered safe or harmful.
- What action the user chooses when presented with the user awareness prompts.

If the website is identified to be safe and the user chooses to continue to the website, they will be redirected as normal. If the website is determined to be harmful they will be notified, and an alert will be generated for the SOC to review. The URL Testing and Training feature serves to increase user awareness and train users to be diligent in examining emails and links for authenticity to prevent successful phishing attacks against your organization.

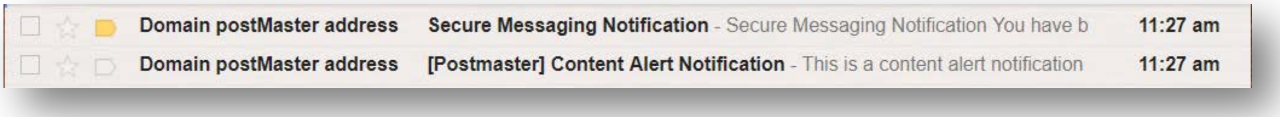
How to Send an Encrypted/Secure Email

Encrypting an email is a way to securely send an email to ensure that only the intended recipient is able to open the email and read its contents. While it is a good habit to secure all emails, it is particularly important to encrypt any emails that are sent over a unsecure networks, such as public Wi-fi or emails that contain sensitive information such as personally identifiable information (PII), banking info, proprietary or trade secrets, or sensitive client data, etc.

Mimecast makes it simple and easy to send encrypted emails. By adding "**<e>**" at the beginning or end of the email subject line, Mimecast will send the message securely. Once sent, the sender will receive a confirmation email from Mimecast confirming email encryption was successful.

While it may be easy to send an encrypted email using Mimecast, it is important that the sender communicates with the recipient(s), informing them that they will receive an encrypted email and that they will need to access it through the Mimecast Secure Mail inbox rather than opening it as a normal email. The following section provides an overview of what the recipient will see.

The recipient will receive an email from “Domain postmaster address” instead of the senders name and email address.

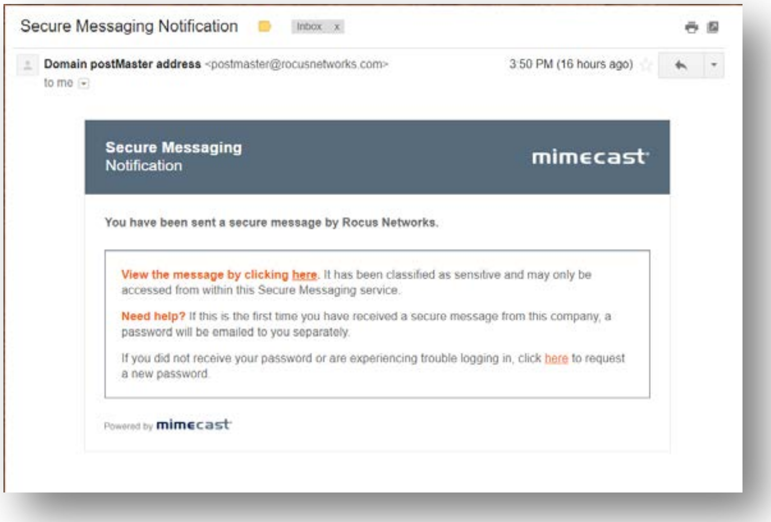


Domain postMaster address Secure Messaging Notification - Secure Messaging Notification You have b 11:27 am

Domain postMaster address [Postmaster] Content Alert Notification - This is a content alert notification 11:27 am

If this is the recipient’s first time receiving a secure email from someone at your organization, they will receive both the Secure Message Notification as well as a temporary password for accessing the Mimecast Secure Portal.

Selecting “View the message by clicking here” opens up a browser window to the Mimecast Secure portal. Here the recipient will be asked to login using either the temporarily created credentials or their normal login information, if they previously registered. Once logged in, the user will be taken to their Secure Mail inbox to view the message, download attachments, and reply with another encrypted email.



Domain postMaster address <postmaster@rocusnetworks.com> 3:50 PM (16 hours ago)
to me

Secure Messaging Notification

You have been sent a secure message by Rocus Networks.

View the message by clicking here. It has been classified as sensitive and may only be accessed from within this Secure Messaging service.

Need help? If this is the first time you have received a secure message from this company, a password will be emailed to you separately.

If you did not receive your password or are experiencing trouble logging in, click here to request a new password.

What if I have questions?

Please reach out to your network or IT administrator if you have any questions. If they are unable to help you, he or she can work with the Corvid Cyberdefense Email Administration team to resolve your issue. You can also check Mimecast resources and troubleshooting guides at https://community.mimecast.com/docs/DOC-1526.

V20201216