

The background features a dark blue field with a series of thin, yellow, wavy lines that create a sense of depth and movement. In the lower right corner, there are several overlapping geometric shapes: a large yellow circle, a smaller yellow circle, and a white circle, all set against a semi-transparent yellow polygonal shape.

QUICK START GUIDE

Email Security Activation


censornet.



Copyright © Censornet Limited, 2007-2022

This guide is designed to help customers prepare for migration to Censornets Email Security Solution. It outlines the logical steps involved in the process and also establishes configuration required at the customers end.

This document is designed to provide information about the first-time configuration and administrator use of the Censornet MailSafe service (cloud based e-mail filtering). Every effort has been made to make this document as complete and accurate as possible, but no warranty or fitness is implied. Censornet Ltd does not accept any liability for poorly designed or malfunctioning networks.

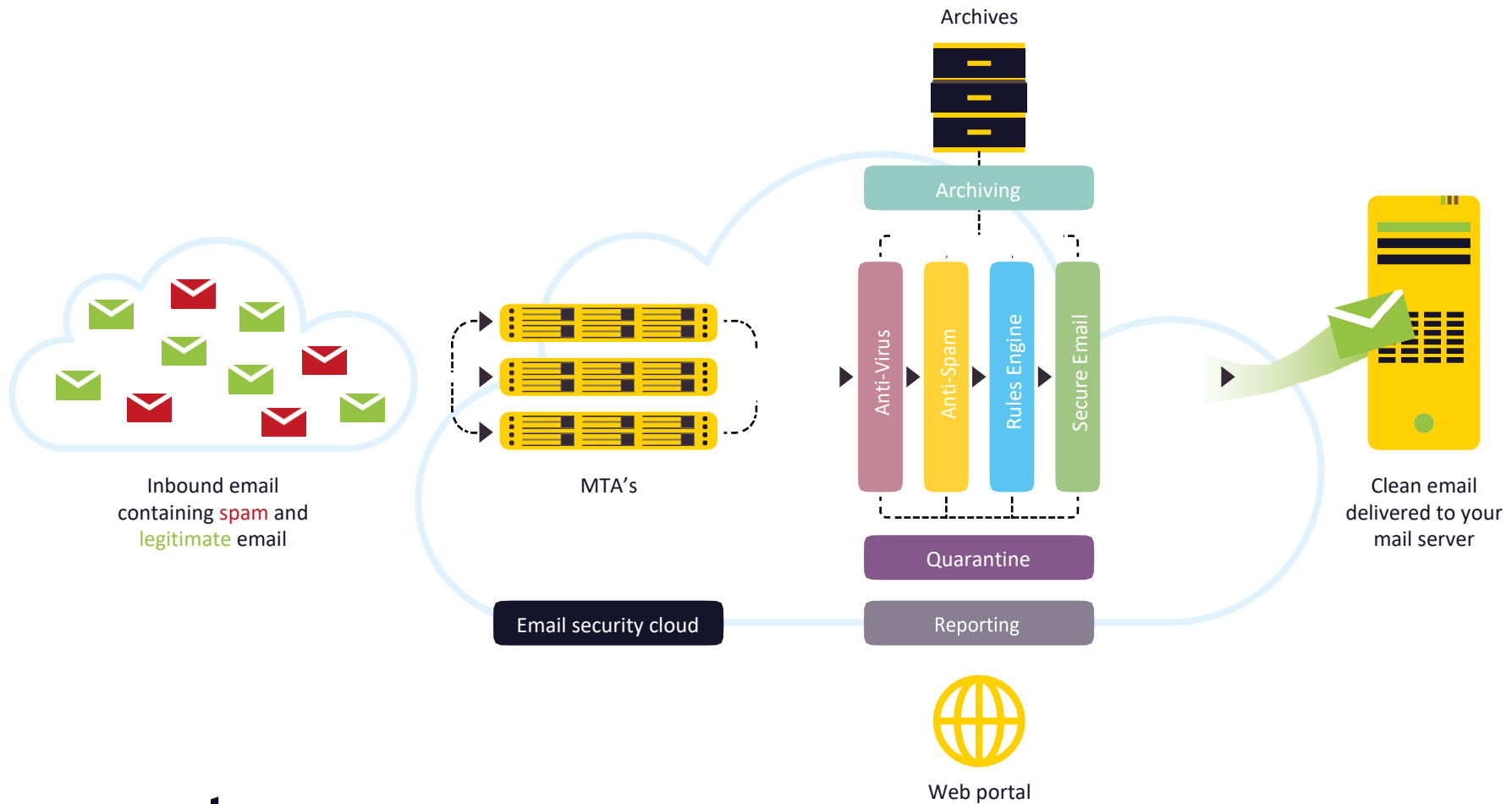


Contents

Page 3	Basics
Page 4	High Level Implementation Steps & order of events
Page 10	Logging in to the portal
Page 11	Synchronisation Troubleshooting
Page 11	Amending Firewall Rules - Ensure you can accept e-mail from Email Security servers
Page 12	Outbound e-mail
Page 13	Updating MXrecords
Page 14	Technical support

Basics

Through a simple redirection of MX records and outbound “Smart Host” configuration Censornet provides comprehensive Real-Time Email Threat protection. Through Multi-layered protection and utilising a unique combination of technologies, Censornet offers complete control over mail flow and protection against both traditional and emerging threats.



High Level Implementation Steps

Each of these steps should be performed in the order stated below to ensure successful implementation.

PREPARING THE ENVIRONMENT

1. Complete the Censornet Email Provisioning Document which outlines domains Censornet will relay mail for on behalf of the customer as well as routing information for inbound/outbound delivery.



Completed

2. Customer will receive a provisioning email (following Censornets receipt of provisioning document) outlining account activation for the email security portal (see p.10). At this point customer can define password and log into their Email Security Portal. Ensure Domains and Routes are configured (Email Security>Product Configuration) if they haven't already been done by provisioning team. See <https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-office-365>. At this stage do not make any changes in your O365 tenant referenced by the KB. They will be covered in later steps.



Received

3. Ensure organisational mailboxes are synchronised with the Email Security Portal. The method used will depend on whether mailboxes are maintained in Azure AD or in an On-premise Active Directory (or neither). This can be completed via the Azure API (<https://help.clouduss.com/settings/active-directory>), installation of the local AD Connector (see <https://help.clouduss.com/settings/ad-connector>) and configuration of an AD Sync (<https://help.clouduss.com/settings/active-directory>) **OR** via a bulk manual import in the portal. Use of the AD/Azure connector will ensure that new mailboxes will be synchronised automatically. **Note:** Please see <https://help.clouduss.com/settings/active-directory-object-synchronisation> for details on objects not auto synced.

Further notes are provided on page 11.



Completed



4. Ensure inbound and outbound firewall rules AND/OR mail server connector/transport rules (e.g. Office 365) are configured to also allow authorised Censornet SMTP servers inbound and outbound (if previously restricted). For EU customers see p.12 and <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-eu-customers> . For Non-EU customers see p.12 and <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-non-eu-customers> . Prior to the MX record change ensure that authorised Censornet servers are configured alongside any existing authorised servers.



Completed

5. Ensure Censornet addresses are whitelisted in existing mail delivery platform (e.g. Office 365, Gmail) to prevent incorrect spam identification or potential delays. Note: When using Censornet in a G Suite environment careful consideration has to be taken with regards to internal G Suite messages. See p.12 and links below. Prior to MX record change ensure Censornet servers are configured alongside any existing servers (Connection and content levels) to avoid pre cutover issues. <https://help.clouduss.com/ems-knowledge-base/safelisting-email-security-ip-addresses-in-office-365> & <https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-office-365> (section titled “configuration changes for Office 365”) or <https://help.clouduss.com/ems-knowledge-base/configure-gmail-using-g-suite-for-ems>

Completed

6. The default Spoofing rule within Censornet ensures that any inbound emails received from internal domains will be quarantined (aaa@domainA.com > bbb@domainA.com) as spam. Legitimate scenarios exist where third party external servers send inbound mail from addresses that purport to be from your internal domain. Identify whether such scenarios exist within your organisation and if so it is recommended that the sending server IP addresses are added to the Censornet spam safe list.



Completed

7. Prior to MX record change update any External DNS SPF records for mail relayed domains to include “scanscope.net” (EU customers <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-eu-customers> . For non-EU customers <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-non-eu-customers>



Completed

8. Prior to MX record change, to help combat impersonation/spoofing attacks ensure that External DNS DKIM and DMARC records are defined to take advantage of default out of the box rules (<https://help.clouduss.com/ems-knowledge-base/configure-outbound-dkim> & <https://help.clouduss.com/ems-knowledge-base/configure-outbound-dmarc>)

Important Note: To finalise DKIM signing verify the DKIM record from the Dashboard

Completed

9. Prior to MX record change to ensure easy roll back of MX records if required it is recommended to reduce DNS TTL of MX records to a minimum value.

Completed

10. Ensure Executive tracking is enabled on Mailboxes or Group Objects synchronised to protect against impersonation type attacks. See "Exec Tracking" in <https://help.clouduss.com/email-security/mailboxes> &

Completed

CHECKING THE DEFAULT RULEBASE

11. Ensure you have reviewed default rules provided and configured any specific rules required for the organisational policy to be enforced. Determine whether user-based spam digests will be utilised (and whether SSO is preferred).

Completed

12. Import users and assign “End User Portal” role to any users using Spam Digests. Settings>Administrators

13. OPTIONAL - If you have purchased Archiving please contact your Censornet representative to ensure correct setup.

Completed

14. OPTIONAL - If you have purchased SecureMail ensure the appropriate rule is configured and in place (if a license has been activated the rule should be configured by default).

- <https://help.clouduss.com/securemail/internal-and-external-securemail-users-explained>
- <https://help.clouduss.com/securemail/configuring-securemail>
- <https://help.clouduss.com/securemail/using-the-secure-mail-dashboard>

Completed

TESTING SMTP CONNECTIVITY

- 14a. Perform inbound connectivity tests to ensure setup correct. Please send mail request to support@censornet.com with “EMAIL CONNECTIVITY TEST REQUEST” in the subject field.

Support will then run inbound connectivity tests to ensure SMTP flow will work and reply accordingly.

Completed

GOING LIVE – OUTBOUND MAIL

15. Configure Outbound SMTP (Smart Host) flow to go via Censornet Email Security SMTP Servers (see below P.12).

Office365

- <https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-office-365>

On-Premise Exchange

- <https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-exchange-2007-2010>

Google Workspace

- <https://help.clouduss.com/ems-knowledge-base/configure-gmail-using-g-suite-for-ems>



Completed

GOING LIVE – INBOUND MAIL

16. Modify MX records to re-route inbound mail through Censornet

EU CUSTOMERS SEE P.13 AND

- <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-eu-customers>

Non-EU CUSTOMERS SEE P.13 AND

- <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-non-eu-customers>

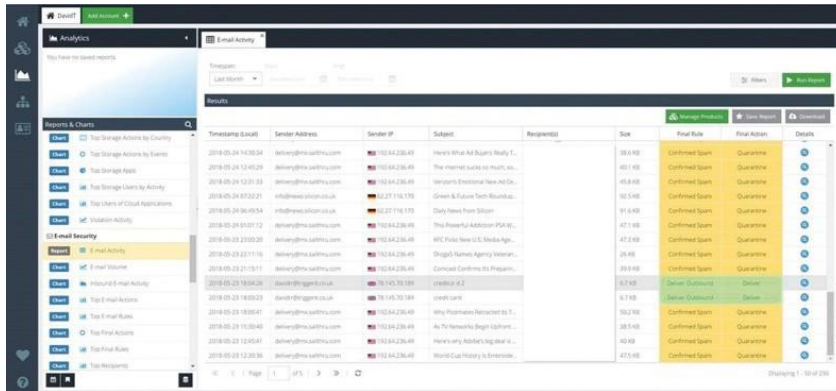


Completed

VERIFYING MAIL THROUGH CENSORNET

17. To verify inbound and outbound mail through Censornet navigate to Analytics -> Email Activity within the dashboard.

N.B. In the example below the recipient field has been redacted.

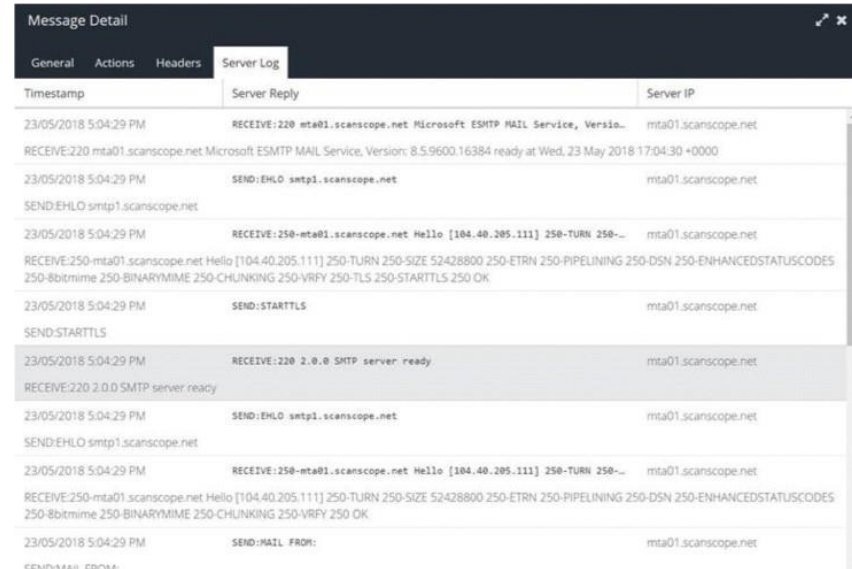


The screenshot shows the Censornet Analytics dashboard with the 'Email Activity' tab selected. A table displays a list of email messages with columns for Timestamp, Sender Address, Sender IP, Subject, Recipients, Size, Final Rule, and Final Action. The 'Final Action' column shows 'Confirmed Spam' for most entries, with some marked as 'Quarantine'.

Timestamp (Local)	Sender Address	Sender IP	Subject	Recipients	Size	Final Rule	Final Action
2018-05-24 14:05:34	delany@ms.scanscope.net	103.84.236.49	Here's What AI Experts Really T...		38,830	Confirmed Spam	Quarantine
2018-05-24 12:45:29	delany@ms.scanscope.net	103.84.236.49	The internet battle to build, co...		40,180	Confirmed Spam	Quarantine
2018-05-24 12:31:33	delany@ms.scanscope.net	103.84.236.49	Verizon's Emotional Spam ADS...		40,888	Confirmed Spam	Quarantine
2018-05-24 07:52:21	inf@newsaction.co.uk	82.27.116.170	Green & Future Term Roundup...		30,548	Confirmed Spam	Quarantine
2018-05-24 06:05:54	inf@newsaction.co.uk	82.27.116.170	Daily News from Bloomberg		91,640	Confirmed Spam	Quarantine
2018-05-24 03:07:12	delany@ms.scanscope.net	103.84.236.49	This PowerUp Addiction PAK B...		47,185	Confirmed Spam	Quarantine
2018-05-24 23:05:20	delany@ms.scanscope.net	103.84.236.49	NYC Police New U.S. Media Age...		47,248	Confirmed Spam	Quarantine
2018-05-23 23:11:16	delany@ms.scanscope.net	103.84.236.49	Shing's Number Agency Vetera...		26,498	Confirmed Spam	Quarantine
2018-05-23 21:15:11	delany@ms.scanscope.net	103.84.236.49	General Confirms 60 Progres...		20,940	Confirmed Spam	Quarantine
2018-05-23 16:08:36	asash@agencys.com	76.145.70.788	Weekend 82		30,740	Spam Confirmed	Quarantine
2018-05-23 18:05:23	asash@agencys.com	76.145.70.788	Weekend 82		4,178	Spam Confirmed	Quarantine
2018-05-23 18:05:41	delany@ms.scanscope.net	103.84.236.49	Why Popstars Reminded to T...		262,500	Confirmed Spam	Quarantine
2018-05-23 16:05:40	delany@ms.scanscope.net	103.84.236.49	As TV Networks Begin Spinn...		38,540	Confirmed Spam	Quarantine
2018-05-23 12:40:41	delany@ms.scanscope.net	103.84.236.49	Here's why Airbnb's App And L...		40,108	Confirmed Spam	Quarantine
2018-05-23 12:30:36	delany@ms.scanscope.net	103.84.236.49	World Cup History Is Underwa...		475,408	Confirmed Spam	Quarantine

To verify Censornets action upon messages, check the final action applied to the messages. To investigate the actual SMTP conversation between the USS Email servers and your own e-mail.

Server double click the subject line of a message and then click the "Headers" or "Server Log" tabs within the Message Detail window.



The screenshot shows the 'Message Detail' window with the 'Server Log' tab selected. It displays a list of SMTP transactions between the server and the client, including 'RECEIVE', 'SEND', and 'STARTTLS' messages. The 'Server Reply' column shows the raw SMTP protocol text, and the 'Server IP' column shows the IP address of the server.

Timestamp	Server Reply	Server IP
23/05/2018 5:04:29 PM	RECEIVE:220 mta01.scanscope.net Microsoft ESMT... Microsoft ESMT... ready at Wed, 23 May 2018 17:04:30 +0000	mta01.scanscope.net
23/05/2018 5:04:29 PM	SEND:EHL0 smtp1.scanscope.net	mta01.scanscope.net
23/05/2018 5:04:29 PM	RECEIVE:250-mta01.scanscope.net Hello [104.40.205.111] 250-TURN 250-... Hello [104.40.205.111] 250-TURN 250-SIZE 52428800 250-ETRN 250-PIPELINING 250-DSN 250-ENHANCEDSTATUSCODES 250-8bitmime 250-BINARYMIME 250-CHUNKING 250-VRFY 250-TLS 250-STARTTLS 250 OK	mta01.scanscope.net
23/05/2018 5:04:29 PM	SEND:STARTTLS	mta01.scanscope.net
23/05/2018 5:04:29 PM	RECEIVE:220 2.0.0 SMTP server ready	mta01.scanscope.net
23/05/2018 5:04:29 PM	SEND:EHL0 smtp1.scanscope.net	mta01.scanscope.net
23/05/2018 5:04:29 PM	RECEIVE:250-mta01.scanscope.net Hello [104.40.205.111] 250-TURN 250-... Hello [104.40.205.111] 250-TURN 250-SIZE 52428800 250-ETRN 250-PIPELINING 250-DSN 250-ENHANCEDSTATUSCODES 250-8bitmime 250-BINARYMIME 250-CHUNKING 250-VRFY 250 OK	mta01.scanscope.net
23/05/2018 5:04:29 PM	SEND:MAIL FROM:	mta01.scanscope.net

ROLL BACK (if required)

18. If at any point inbound or outbound routing has to be rolled back revert MX records and or Smart host connectors respectively.

FINAL STEPS (Recommended after period of stability confirmed)

19. Remove any unwanted SPF records from DNS that are no longer required.



Completed

20. Ensure inbound and outbound firewall rules AND/OR mail server connector rules (e.g. Office 365) where appropriate are locked down to only allow authorised Censornet SMTP servers inbound and outbound.

<https://help.clouduss.com/email-security/configure-inbound-mail-on-office-365-to-reject-non-ems-emails>

21. For On-premise Exchange environments take note of any internal servers that are configured to send outbound directly rather than via Exchange. Ensure Firewall rules continue to allow SMTP traffic outbound from these sources OR ensure they are relayed via Exchange.



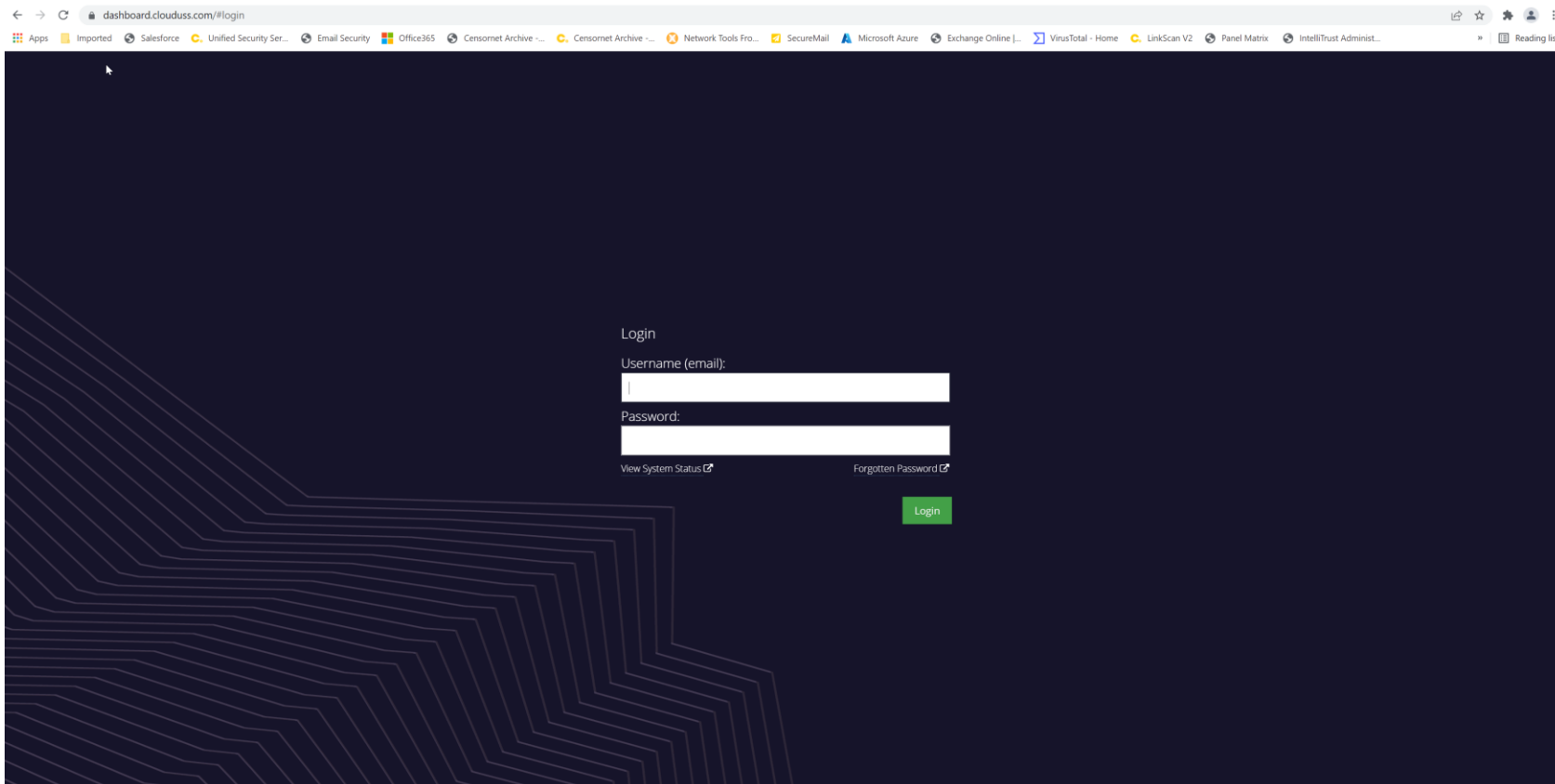
Completed

Logging On

Requirements: Web browser / Internet access

For more details about this product, please visit <https://www.censornet.com/products/email-security/>

To configure and manage the Email Security system you need access to the Internet so that you can log into the web based portal and activate the account from the link provided in the provisioning email. Here you will be requested to configure a password for the initial administrator account.



Verifying Synchronisation of mailboxes

Navigate to Products > Email Security > Mailboxes to confirm list of users added.

Now, go to the Products > Email Security, Select Mailboxes and you should see a list of e-mail addresses exported from Active Directory. Censornet support can also verify if mailbox synchronisation has been successful.

Ensure you can accept email from email security servers

The next step is to ensure that your firewall is configured to allow e-mail to be delivered from the Email Security servers after it has been filtered. You should add firewall rule entries to allow the following IP addresses to connect from the public Internet to your mail server on port 25.

Our ip addresses are always available here:

EU customers: <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-eu-customers>

Non-EU customers: <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-non-eu-customers>

Outbound Email

If you wish to use the Email Security service for outbound E-mail please follow the instructions in the links below or follow the relevant documentation provided by your Mail Server Vendor:

<https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-exchange-2007-2010>

<https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-exchange-2016>

<https://help.clouduss.com/ems-knowledge-base/configure-outbound-email-for-office-365>

<https://help.clouduss.com/ems-knowledge-base/configure-gmail-for-ems>

EU Customers:

<https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-eu-customers>

If you are a Non-EU customer please ensure you are using these outbound services:

<https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-non-eu-customers>

Updating MX Records

Once you are happy that the Users are synchronised (Step 1) and the firewall is updated (Step 2) you can go ahead and update the MX records for your domain.

The final step in the setup process is for the you to update the MX records for the domain to be filtered. The MX records to use are available in the following link:

EU customers: <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-eu-customers>

Non-EU Customers: <https://help.clouduss.com/ems-knowledge-base/mx-records-and-ip-addresses-for-non-eu-customers>

You should remove any other MX records that may have been in place before. Failure to do so allows attackers to bypass mail protections.

Technical Support

Telephone: +44 (0)845 230 9592

Email: support@censornet.com

Live desk support: www.censornet.com/support

Knowledge base: help.scanscope.net