

Configure URL Filtering for Secure Email Gateway and Cloud Gateway

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Enable URL Filtering](#)

[Create URL Filtering Actions](#)

[Untrusted URL\(s\)](#)

[Unknown URL\(s\)](#)

[Questionable URL\(s\)](#)

[Neutral URL\(s\)](#)

[Message Tracking](#)

[Reporting Uncategorized and Misclassified URL\(s\)](#)

[Malicious URLs and Marketing Messages Are Not Caught by Anti-Spam or Outbreak Filters](#)

[Appendix](#)

[Enable URL Filtering Support for Shortened URLs](#)

[Additional Information](#)

[Cisco Secure Email Gateway Documentation](#)

[Secure Email Cloud Gateway Documentation](#)

[Cisco Secure Email and Web Manager Documentation](#)

[Cisco Secure Product Documentation](#)

Introduction

This document describes how to configure URL Filtering on Cisco Secure Email Gateway and Cloud Gateway and best practices for URL Filtering use.

Background Information


URL Filtering was first introduced with AsyncOS 11.1 for Email Security. This release allowed the configuration of Cisco Secure Email to scan for URLs in message attachments and perform configured actions on such messages. Message and content filters use the URL Reputation and URL Category to check for URLs in messages and attachments. For more details, see the "Using Message Filters to Enforce Email Policies," "Content Filters," and "Protecting Against Untrusted or Undesirable URLs" chapters in the [User Guide](#) or online help.

Control and protection against untrusted or undesirable links are incorporated into the work queue for anti-spam, outbreak, content, and message filtering processes. These controls:


- Increase the effectiveness of protection from untrusted URLs in messages and attachments.
- In addition, URL Filtering is incorporated into Outbreak Filters. This strengthened protection is

applicable even if your organization already has a Cisco Web Security Appliance or similar protection from web-based threats because it blocks threats at the point of entry.

- You can also use content or message filters to take action based on the Web-Based Reputation Score (WBRS) of URLs in messages. For example, you can rewrite URLs with a neutral or unknown reputation to redirect them to the Cisco Web Security Proxy for click-time evaluation of their safety.
- Better identify spam
- The appliance uses the reputation and category of links in messages and other spam-identification algorithms to help identify spam. For example, if a link in a message belongs to a marketing website, the message is more likely to be a marketing message.
- Support enforcement of corporate acceptable use policies
- The category of URLs (Adult Content or Illegal Activities, for example) can be used with content and message filters to enforce acceptable corporate use policies.
- Allow you to identify users in your organization who most frequently clicked a URL in a message that has been rewritten for protection and links that have most commonly been clicked.

 **Note:** In the AsyncOS 11.1 for Email Security release, URL Filtering introduced support for shortened URLs. With the CLI command 'websecurityadvancedconfig,' the shortener services could be seen and configured. This configuration option was updated in [AsyncOS 13.5 for Email Security](#). After you upgrade to this release, all shortened URLs are expanded. There is no option to disable the expansion of shortened URLs. For this reason, Cisco recommends AsyncOS 13.5 for Email Security or newer to provide the latest protections for URL defense. Please see the "Protecting Against Malicious or Undesirable URLs" chapter in the user guide or online help and the CLI Reference Guide for AsyncOS for Cisco Email Security Appliance.

 **Note:** For this document, [AsyncOS 14.2 for Email Security](#) is used for the examples and screenshots provided.

 **Note:** Cisco Secure Email also provides an in-depth [URL Defense Guide at docs.ces.cisco.com](https://docs.ces.cisco.com).

Prerequisites

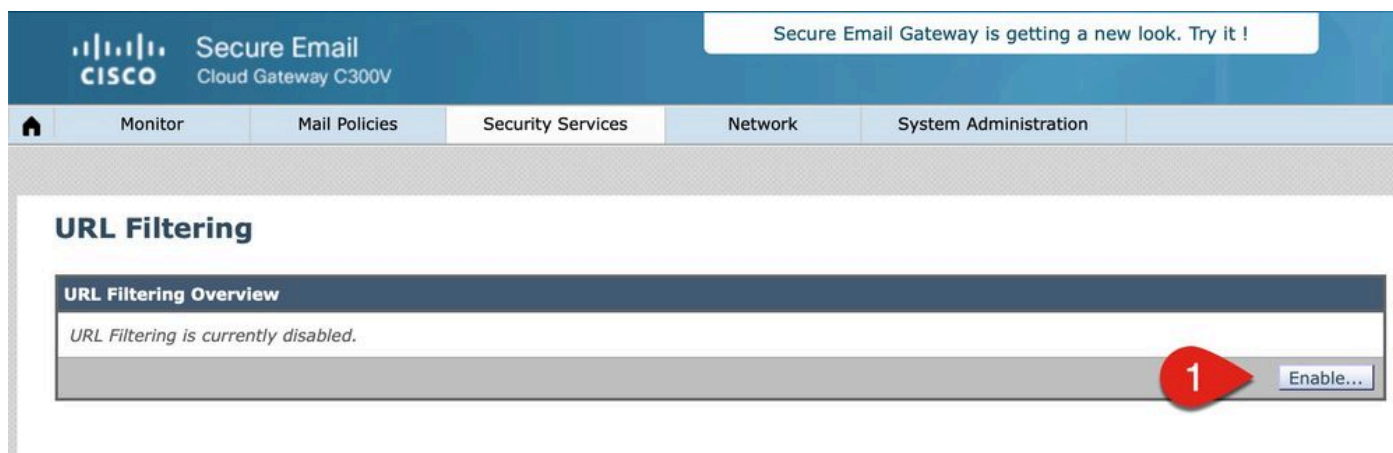
When you configure URL Filtering on the Cisco Secure Email Gateway or Cloud Gateway, you must also configure other features dependent upon your desired functionality. Here are some typical features that are enabled alongside URL Filtering:

- For enhanced protection against spam, the Anti-Spam Scanning feature **must be enabled globally** per the applicable mail policy. Anti-Spam is considered either the Cisco IronPort Anti-Spam (IPAS) or the Cisco Intelligent Multi-Scan (IMS) feature.
- For enhanced protection against malware, the Outbreak Filters or Virus Outbreak Filters (VOF) feature **must be enabled globally** per the applicable mail policy.
- For actions based on URL Reputation or to enforce acceptable use policies with the use of message and content filters, VOF **must be enabled globally**.

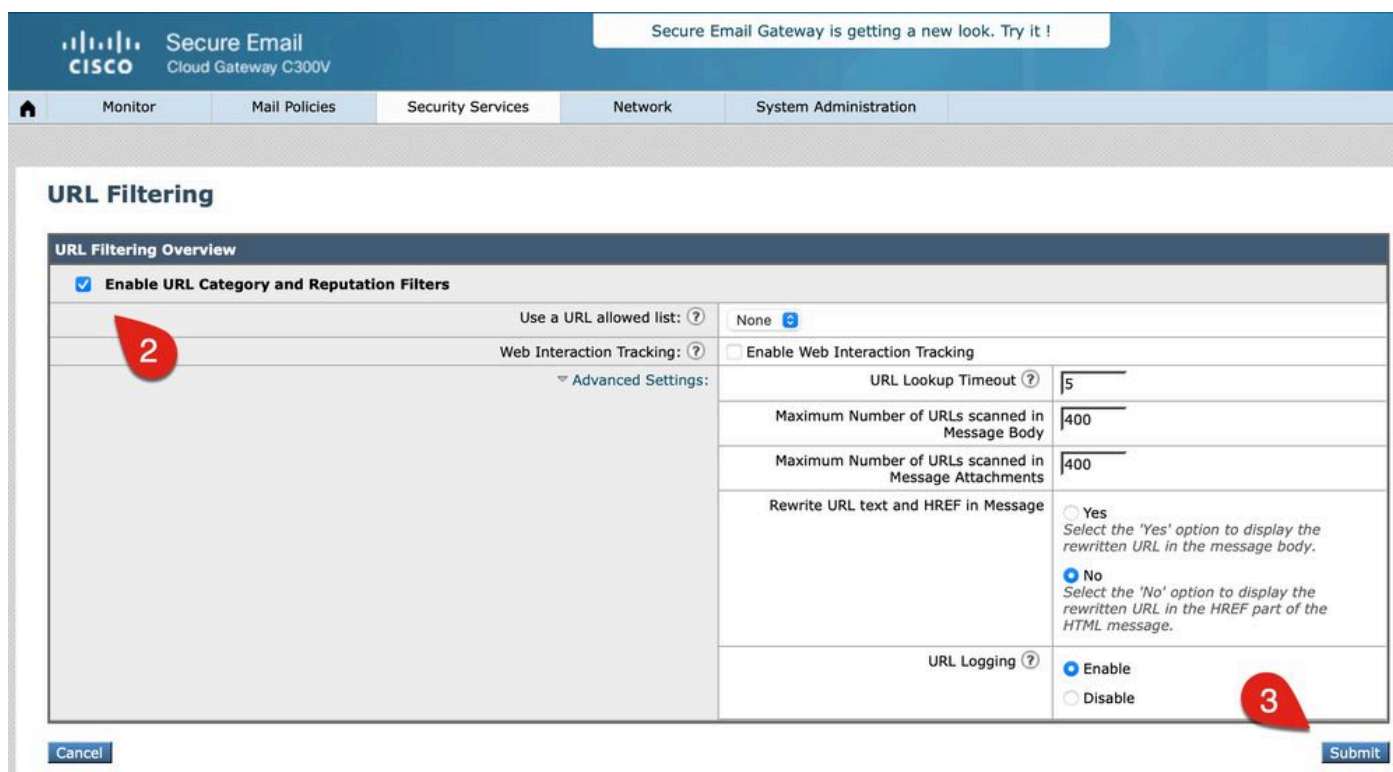
Enable URL Filtering


You must first enable the feature to implement URL Filtering on the Cisco Secure Email Gateway or Cloud Gateway. URL Filtering can be enabled from GUI or CLI by the administrator.

To enable URL Filtering, from GUI, navigate to **Security Services > URL Filtering** and click **Enable**:



Next, click **Enable URL Category and Reputation Filters**. This example includes best practices values for URL Lookup Timeout, Maximum Number of URLs scanned, and enables the option to log URL(s):



 **Note:** Ensure that you **commit** your changes to the configuration at this time.

Create URL Filtering Actions

When you enable URL Filtering alone, it does not take action against URLs within messages or messages with attachments.

The URL(s) included in messages and attachments for incoming and outgoing mail policies are evaluated.

Any valid string for a URL is evaluated to include strings with these components:

- HTTP, HTTPS, or WWW
- Domain or IP addresses
- Port numbers preceded by a colon (:)
- Uppercase or lowercase letters



Note: URL log entry is visible from mail_logs for most URLs. If the URL is not logged in the mail_logs, please review Message Tracking for the Message ID (MID). Message Tracking does include a tab for "URL Details."

When the system evaluates URLs to determine whether a message is a spam, if necessary for load management, it prioritizes and screens inbound messages over outbound messages.

You can perform actions on messages based on the URL reputation or the URL category in the message body or messages with attachments.

For example, if you want to apply the **Drop (Final Action)** action to all messages that include URLs in the Adult category, add a condition of type URL Category with the Adult category selected.

If you do not specify a category, the action you choose is applied to all messages.

The URL reputation score range for Trusted, Favorable, Neutral, Questionable, and Untrusted are predefined and not editable. You can specify a Custom Range. Use "Unknown" for URLs for which a reputation score has yet to be determined.

To quickly scan URLs and take action, you can create a content filter so that *if* the message has a valid URL, *then* the action is applied. From the GUI, navigate **Mail Policies > Incoming Content Filters > Add Filter**.

Actions associated with URLs are as follows:

- Defang URL
 - The URL is modified to make it unclickable, but the message recipient can still read the intended URL. (Extra characters are inserted into the original URL.)
- Redirect to Cisco Security Proxy
 - The URL is rewritten when clicked to pass through the Cisco Security Proxy for additional verification. Based on the Cisco Security Proxy verdict, the site could be inaccessible to the user.
- Replace URL with a text message
 - With this option, an administrator can rewrite the URL within the message and send it externally for Remote Browser Isolation.

Untrusted URL(s)

Untrusted: URL behavior that is exceptionally bad, malicious, or undesirable. This is the safest recommended blacklist threshold; however, there can be messages that are not blocked because the URLs

therein have a lower threat level. Prioritizes delivery over security.

Recommended action: Block. (An administrator can quarantine or drop the message entirely.)

This example provides context for a content filter for URL Filtering to detect Untrusted URLs:

Content Filter Settings			
Name:	URL_QUARANTINE_UNTRUSTED		
Currently Used by Policies:	Default Policy		
Description:	Quarantine messages with known Untrusted URLs. (Includes messages with attachments.)		

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	quarantine("URL_UNTRUSTED")	

With this content filter in place, Cisco Secure Email scans for a URL with an *Untrusted* reputation (-10.00 to -6.00) and places the message into a quarantine, URL_UNTRUSTED. Here is an example from the mail_logs:

<#root>

```
Tue Jul 5 15:01:25 2022 Info: ICID 5 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country United States
Tue Jul 5 15:01:25 2022 Info: ICID 5 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:01:25 2022 Info: Start MID 3 ICID 5
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 From: <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host: example.com
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: Neutral
Tue Jul 5 15:01:25 2022 Info: MID 3 ICID 5 RID 0 To: <end_user>
Tue Jul 5 15:01:25 2022 Info: MID 3 Message-ID '<20220705145935.1835303@ip-127-0-0-1.internal>'
Tue Jul 5 15:01:25 2022 Info: MID 3 Subject "test is sent you a URL => 15504c0618"
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1.internal
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: Neutral
Tue Jul 5 15:01:25 2022 Info: MID 3 SDR: Tracker Header : 62c45245_jTikQ21V2NYfmrGzMwQMBd68fxqFFueNmE1w
Tue Jul 5 15:01:25 2022 Info: MID 3 ready 3123 bytes from <test@test.com>
Tue Jul 5 15:01:25 2022 Info: MID 3 matched all recipients for per-recipient policy DEFAULT in the inbound
Tue Jul 5 15:01:25 2022 Info: ICID 5 close

Tue Jul 5 15:01:25 2022 Info: MID 3 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matched

Tue Jul 5 15:01:25 2022 Info: MID 3 quarantined to "Policy" (content filter:URL_QUARANTINE_UNTRUSTED)

Tue Jul 5 15:01:25 2022 Info: Message finished MID 3 done
```

The URL [ihaveabadreputation.com](https://www.ihaveabadreputation.com) is considered **UNTRUSTED** and scored at a **-9.5**. URL Filtering detected the Untrusted URL and quarantined it to **URL_UNTRUSTED**.

The previous example from `mail_logs` provides an example if **ONLY** the content filter for URL Filtering is enabled for the incoming mail policy. If the same mail policy has additional services enabled, such as Anti-Spam, the other services indicate if the URL has been detected from **THOSE** services and their rules. In the same URL example, Cisco Anti-Spam Engine (CASE) is enabled for the incoming mail policy, and the message body is scanned and determined to be spam positive. This is indicated first in the `mail_logs` since Anti-Spam is the first service in the mail processing pipeline. Content Filters come later in the mail processing pipeline:

```
<#root>
```

```
Tue Jul 5 15:19:48 2022 Info: ICID 6 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country United States
Tue Jul 5 15:19:48 2022 Info: ICID 6 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 15:19:48 2022 Info: Start MID 4 ICID 6
Tue Jul 5 15:19:48 2022 Info: MID 4 ICID 6 From: <test@test.com>
Tue Jul 5 15:19:48 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
Tue Jul 5 15:19:49 2022 Info: MID 4 ICID 6 RID 0 To: <end_user>
Tue Jul 5 15:19:49 2022 Info: MID 4 Message-ID '<20220705151759.1841272@ip-127-0-0-1.internal>'
Tue Jul 5 15:19:49 2022 Info: MID 4 Subject "test is sent you a URL => 646aca13b8"
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0-0-1
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A
Tue Jul 5 15:19:49 2022 Info: MID 4 SDR: Tracker Header : 62c45695_mqwplhpxGDqtgUp/XTLGFKD60hwNKKsghUKA
Tue Jul 5 15:19:49 2022 Info: MID 4 ready 3157 bytes from <test@test.com>
Tue Jul 5 15:19:49 2022 Info: MID 4 matched all recipients for per-recipient policy DEFAULT in the inbound
Tue Jul 5 15:19:49 2022 Info: ICID 6 close

Tue Jul 5 15:19:49 2022 Info: MID 4 interim verdict using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: MID 4 using engine: CASE spam positive

Tue Jul 5 15:19:49 2022 Info: ISQ: Tagging MID 4 for quarantine
Tue Jul 5 15:19:49 2022 Info: MID 4 URL https://www.ihaveabadreputation.com/ has reputation -9.5 matched
Tue Jul 5 15:19:49 2022 Info: MID 4 quarantined to "URL_UNTRUSTED" (content filter:URL_QUARANTINE_UNTRUSTED)
Tue Jul 5 15:19:49 2022 Info: Message finished MID 4 done
```

There are times when CASE and IPAS rules contain rules, reputation, or scores that match against a specific sender, domain, or message contents to detect URL threats alone. In this example, [ihaveabadreputation.com](https://www.ihaveabadreputation.com) was seen, tagged for the Spam Quarantine (ISQ), and the **URL_UNTRUSTED** quarantine by the **URL_QUARANTINE_UNTRUSTED** content filter. The message goes into the **URL_UNTRUSTED** quarantine first. When the message is released from that quarantine by an administrator or the time limit/configuration criteria of the **URL_UNTRUSTED** quarantine have been met, the message is next moved into the ISQ.

Based on administrator preferences, additional conditions and actions can be configured for the content filter.


Unknown URL(s)


Unknown: Not previously evaluated or does not display features to assert a threat-level verdict. The URL Reputation Service does not have enough data to establish a reputation. This verdict is not suitable for actions in a URL Reputation policy directly.


Recommended action: Scan with subsequent engines to check for other potentially malicious content.

Unknown URL(s) or "no reputation" can be URLs that contain new domains or URL(s) that have seen little to no traffic and cannot have an evaluated reputation and threat level verdict. These can turn in Untrusted as more information is obtained for their domain and origination. For such URL(s), Cisco recommends a content filter to log or one that includes the detection of the Unknown URL. As of with AsyncOS 14.2, Unknown URL(s) are sent to the Talos Intelligence Cloud Service for deep URL analysis triggered on various threat indicators. In addition, a mail log entry of the Unknown URL(s) provides the administrator an indication of the URL(s) included in a MID and possible remediation with URL Protection. (See [How to configure Cisco Secure Email Account Settings for Microsoft Azure \(Microsoft 365\) API - Cisco](#) for more information.)

This example provides context for a content filter for URL Filtering to detect Unknown URLs:

Content Filter Settings			
Name:	URL_UNKNOWNN		
Currently Used by Policies:	Default Policy		
Description:	Log messages with Unknown URLs. (Includes messages with attachments.)		
Order:	2  (of 2)		

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-no-reputation("", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>")	

With this content filter in place, Cisco Secure Email scans for a URL with an *Unknown* reputation and writes a log line into the mail_logs. Here is an example from the mail_logs:

<#root>

```
Tue Jul 5 16:51:53 2022 Info: ICID 20 ACCEPT SG MY_TRUSTED_HOSTS match 127.0.0.1 SBRS None country Unit
Tue Jul 5 16:51:53 2022 Info: ICID 20 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Jul 5 16:51:53 2022 Info: Start MID 16 ICID 20
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 From: <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
Tue Jul 5 16:51:53 2022 Info: MID 16 ICID 20 RID 0 To: <end_user>
Tue Jul 5 16:51:53 2022 Info: MID 16 Message-ID '<20220705165003.1870404@ip-127-0-0-1.internal>'
Tue Jul 5 16:51:53 2022 Info: MID 16 Subject "test is sent you a URL => e835eadd28"
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Domains for which SDR is requested: reverse DNS host:ip-127-0
Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N
```



```

Tue Jul 5 16:51:53 2022 Info: MID 16 SDR: Tracker Header : 62c46c29_vrAqZZys2Hqk+BFINvrzdNLLn81kuIf/K6o
Tue Jul 5 16:51:53 2022 Info: MID 16 ready 3208 bytes from <test@test.com>
Tue Jul 5 16:51:53 2022 Info: MID 16 matched all recipients for per-recipient policy DEFAULT in the inbound
Tue Jul 5 16:51:53 2022 Info: ICID 20 close
Tue Jul 5 16:51:54 2022 Info: MID 16 interim verdict using engine: CASE spam negative
Tue Jul 5 16:51:54 2022 Info: MID 16 using engine: CASE spam negative

Tue Jul 5 16:51:54 2022 Info: MID 16 URL http://mytest.example.com/test_url_2022070503 has reputation no

Tue Jul 5 16:51:54 2022 Info: MID 16 Custom Log Entry: <<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>>

Tue Jul 5 16:51:54 2022 Info: MID 16 queued for delivery
Tue Jul 5 16:51:54 2022 Info: Delivery start DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: Message done DCID 13 MID 16 to RID [0]
Tue Jul 5 16:51:56 2022 Info: MID 16 RID [0] Response '2.6.0 <20220705165003.1870404@ip-127-0-0-1.internal>'
Tue Jul 5 16:51:56 2022 Info: Message finished MID 16 done
Tue Jul 5 16:52:01 2022 Info: DCID 13 close

```

The URL `mytest.example.com/test_url_2022070503` has no reputation and is seen with "noscore." The `URL_UNKNOWN` content filter wrote the logline as configured to the `mail_logs`.

After a polling cycle from the Cisco Secure Email Gateway to the Talos Intelligence Cloud Service, the URL is scanned and determined to be Untrusted. This can be seen in the ECS logs at the "Trace" level:

```

Tue Jul 5 16:54:42 2022 Debug: ECS: Finish polling
Tue Jul 5 16:55:42 2022 Debug: ECS: Remediation service notified.
Tue Jul 5 16:55:42 2022 Debug: ECS: Initiating remediation
Tue Jul 5 16:55:42 2022 Info: ECS: Initiating message remediation:
{'from': ['test@test.com'], 'URL': 'http://mytest.example.com/test_url_2022070503', 'message ID':
'<20220705165003.1870404@ip-172-31-43-120.us-east-2.compute.internal>', 'MID': 16, 'verdict':
'MALICIOUS', 'message UUID': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422'}
Tue Jul 5 16:55:42 2022 Debug: ECS: Unprocessed Remediation Data : [{'url_hash':
'8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxyy', 'message_details': '{"mid": 16,
"birth_time": "1657039913", "from_addr": ["test@test.com"], "recipients": ["", "", "", "", "", ""],
"delivery_status": 1, "remediation_req_status": 3}', 'created_at': '2022-07-05 16:52:42.04515',
'verdict': '{"url": "http://mytest.example.com/test_url_2022070503", "verdict": "MALICIOUS"}',
'message_uuid': 'e90dec74-f50b-4a63-9ab2-6adda4fcf422', 'message_id':
'<20220705165003.1870404@ip-127-0-0-1.internal>'}]
Tue Jul 5 16:55:42 2022 Debug: ECS: Remediation records: [
[
16,
"<20220705165003.1870404@ip-127-0-0-1.internal>",
1657039913,
"delete",
3,
"[{\\"url\\": \\"http://mytest.example.com/test_url_2022070503\\", \\"conviction_timestamp\\":
\\"2022-07-05 16:52:42.04515\\", \\"url_hash\\":
\\"8c6915e2ebbc9225ff8958db06db33beb4e932ae9e0d8c5b35805a2fxxyyxyy\\"}]",
[
" ", " ", " ", " ", " ", " ", " ", " "
],
[
"test@test.com"
]
]
]
Tue Jul 5 16:55:42 2022 Debug: ECS: Remediation initiated.
Tue Jul 5 16:55:42 2022 Debug: ECS: Successfully recorded remediation initiation status into datastore.

```


And then subsequently, in the mail_logs, when the remediation itself is called and completed:

```
Tue Jul 5 16:55:42 2022 Info: Message 16 containing URL 'http://mytest.example.com/test_url_2022070503'  
Tue Jul 5 16:55:55 2022 Info: Message 16 was processed due to URL retrospection by Mailbox Remediation v
```

Administrators must consider action for Unknown URL(s) at their discretion. If there is a seen increase in Phish-related emails and attachments, please review the mail_logs and Content Filters report. Additionally, administrators can configure to have Unknown URL(s) redirected to the Cisco Security proxy service for click-time evaluation. In this example, navigate to **Add Action > URL Reputation** within our URL_UNKNOWN content filter:

URL Reputation

[Help](#)

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBR) or using information from the External Threat Feed engine.

Matching Condition

- URL Reputation
 - Untrusted (-10.0 to -6.0)
 - Questionable (-5.9 to -3.1)
 - Neutral (-3.0 to 0.0)
 - Favorable (0.1 to 5.9)
 - Trusted (6.0 to 10.0)
 - Custom Range (min to max)
| |

Unknown



External Threat Feeds

This option is currently unavailable because no threat feed sources have been configured. To create one, go to Mail Policies > External Threat Feeds Manager.

Use a URL allowed list:  


Check URLs within


- Message Body and Subject
- Attachments
- All (Message Body, Subject and Attachments)




Action on URL within the message body and subject:

 . The option to strip attachments for some administrators is not preferable. Please review the action and consider only the option to configure **Message Body and Subject**.

The updated content filter now looks like this example, with the addition of the **Redirect to Cisco Secure Proxy** action:

Content Filter Settings			
Name:	URL_UNKNOWN		
Currently Used by Policies:	Default Policy		
Description:	Log messages with Unknown URLs. (Includes messages with attachments.)		
Order:	2  (of 3)		

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-no-reputation("", 1, 1)	


Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<<=== LOGGING UNKNOWN URL FOR MAIL_LOGS ===>>")	
2	 URL Reputation	url-no-reputation-proxy-redirect-strip("",0)	


Questionable URL(s)


Questionable: URL behavior that can indicate risk or could be undesirable. While not safe for all organizations, this verdict has a low and relatively safe false-positive (FP) rate. A verdict not blocked prioritizes delivery over security, which can result in messages that contain risky URLs.

Recommended action: Scan with subsequent engines and block after review.

As we have configured in Unknown URL(s), administrators can find it beneficial to send Questionable URL(s) to the Cisco Security Proxy or utilize the action to defang the URL(s) entirely.

Content Filter Settings	
Name:	URL_REWRITE_QUESTIONABLE
Currently Used by Policies:	Default Policy
Description:	Re-write URLs on the cusp of Untrusted reputation to be scanned again at click time, very small subset of URLs
Order:	3  (of 3)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-5.90, -3.10, "bypass_urls", 1, 1)	


Actions			
Add Action...			
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-5.90, -3.10,"",0)	


Neutral URL(s)


Neutral: URL with neither positive nor negative behavior. However, it has been evaluated. Namely, the URL has no currently known risk. Therefore, this is the bulk of the reputation verdicts.

Recommended action: Scan with subsequent engines to check for other potentially malicious content.

Administrators can see a Neutral URL with a negative score as a threat. Evaluate the number of messages and occurrences of Neutral URL(s) at your discretion. Similar to how we updated Unknown URL(s) and Questionable URL(s) to utilize the action to send the URL(s) to the Cisco Security Proxy, Neutral URL(s) or a Custom Range that includes a subset of the negative side of Neutral can be considered. This example shows a scan for neutral URLs with the implementation of this inbound content filter:

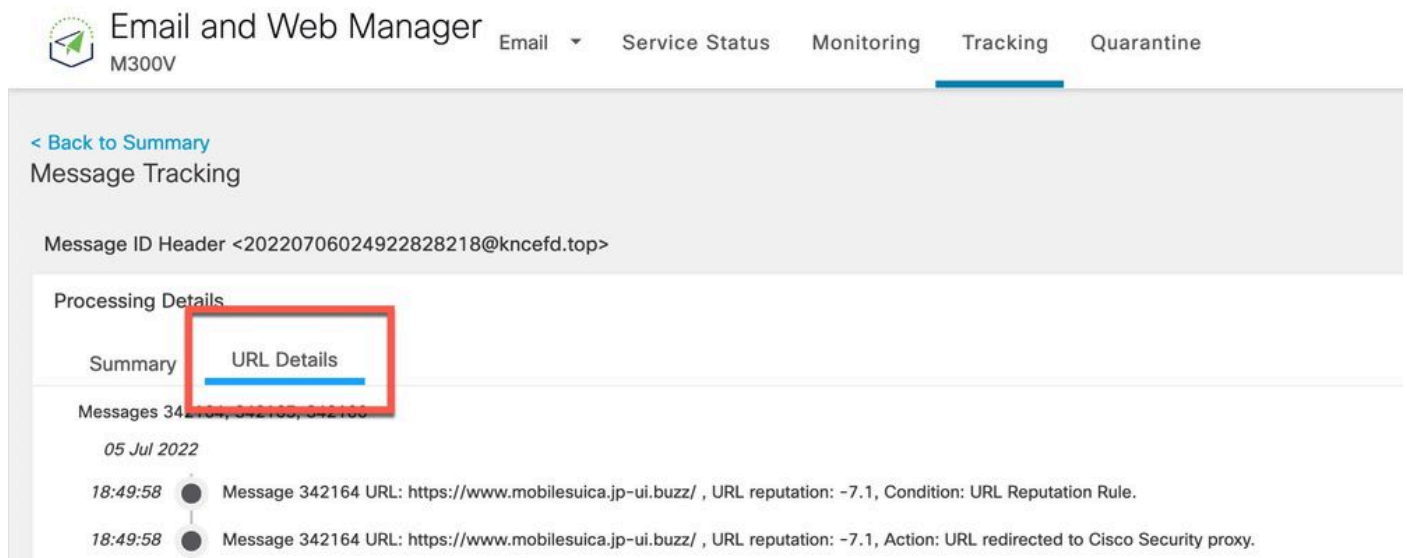
Content Filter Settings	
Name:	URL_NEUTRAL
Currently Used by Policies:	No policies currently use this rule.
Description:	Send questionable Neutral URLs to be scanned again at click time. (Includes messages with attachments.)
Order:	4  (of 4)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-3.00, -0.50, "", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	URL Reputation	url-reputation-proxy-redirect-strip(-3.00, -0.50,"",0)	

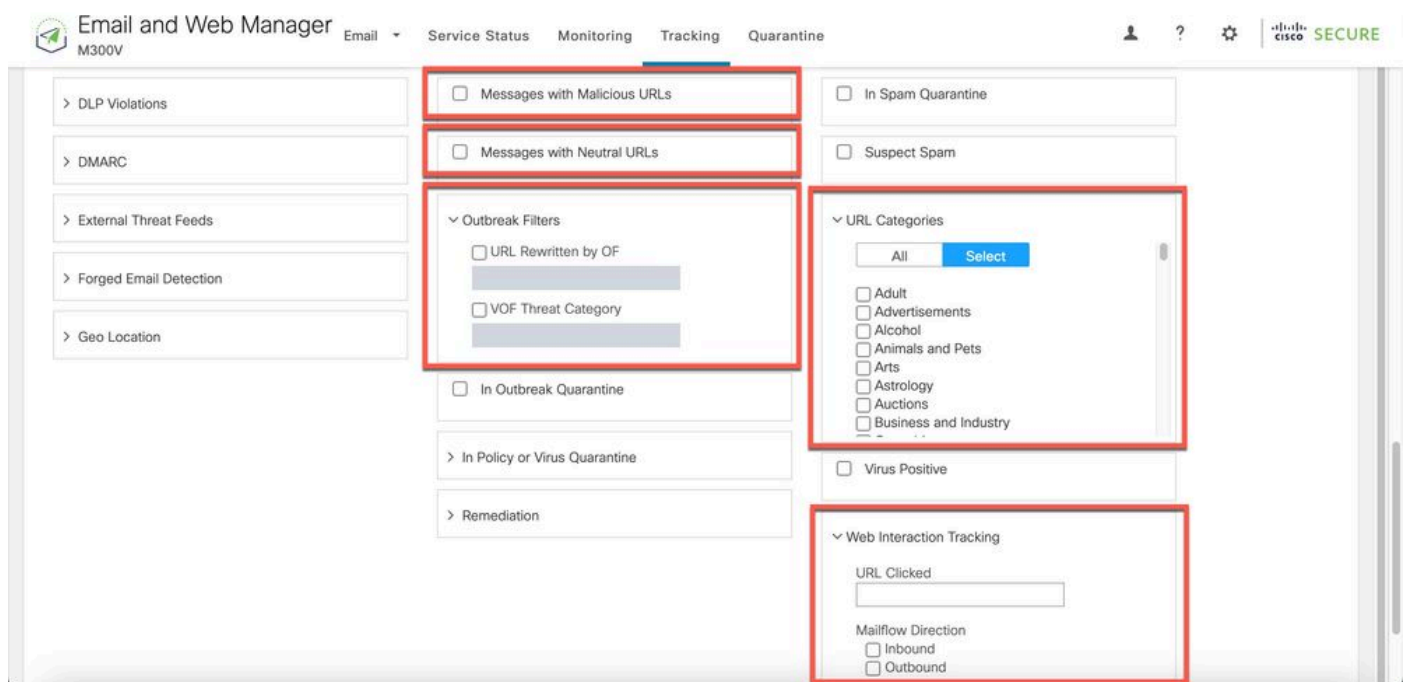
Message Tracking

Review the Message Tracking options for associated URL(s) with MIDs. Sometimes, URLs do not log to the mail_logs, and you can locate them in the Message Tracking details. For example:



The screenshot shows the 'Email and Web Manager' interface with the 'Tracking' tab selected. The main heading is 'Message Tracking' with a '< Back to Summary' link. Below this, the 'Message ID Header' is '<20220706024922828218@kncefd.top>'. A 'Processing Details' section contains two tabs: 'Summary' and 'URL Details', with 'URL Details' highlighted by a red box. The message list shows two entries for 'Message 342164' with the URL 'https://www.mobilesuica.jp-ui.buzz/'. The first entry has a URL reputation of -7.1 and a condition of 'URL Reputation Rule'. The second entry has the same URL reputation and an action of 'URL redirected to Cisco Security proxy'.

Message Tracking also provides Advanced Search options for messages with URL defense and interaction:



The screenshot displays the 'Advanced Search' options in the 'Email and Web Manager' interface. The 'Tracking' tab is active. On the left, there are expandable sections for 'DLP Violations', 'DMARC', 'External Threat Feeds', 'Forged Email Detection', and 'Geo Location'. The main search area contains several filter categories, each with a red box highlighting its search options: 'Messages with Malicious URLs', 'Messages with Neutral URLs', 'Outbreak Filters' (including 'URL Rewritten by OF' and 'VOF Threat Category'), 'In Outbreak Quarantine', 'In Policy or Virus Quarantine', 'Remediation', 'In Spam Quarantine', 'Suspect Spam', 'URL Categories' (with a 'Select' button and a list of categories like 'Adult', 'Advertisements', 'Alcohol', etc.), 'Virus Positive', and 'Web Interaction Tracking' (including 'URL Clicked' and 'Mailflow Direction' options for 'Inbound' and 'Outbound').

Reporting Uncategorized and Misclassified URL(s)

A URL can sometimes report as without a reputation or classification. There are also URL(s) that are miscategorized. To report these URL(s) sightings, visit the Cisco Talos' Web Categorization Requests at [Talos' Reputation Center Support](#) page.

After you report a URL, you can view the status on your [My Tickets](#) page.

Malicious URLs and Marketing Messages Are Not Caught by Anti-Spam or Outbreak Filters

This can occur because the site reputation and category are only two criteria among many that anti-spam and outbreak filters use to determine their verdicts. To increase the sensitivity of these filters, lower the required thresholds to take action, such as rewrite or replace URLs with text, quarantine, or drop messages.

Alternatively, you can create content or message filters based on the URL reputation score.

Appendix

Enable URL Filtering Support for Shortened URLs



Note: This section only applies to AsyncOS 11.1 through 13.0 for Email Security.

URL Filtering support for shortened URLs can be done by CLI only, with the **websecurityadvancedconfig** command:

```
<#root>
```

```
myesa.local>
```

```
websecurityadvancedconfig
```

```
...
```

```
Do you want to enable URL filtering for shortened URLs? [N]>
```

```
y
```

For shortened URL support to work, please ensure that ESA is able to connect to following domains: bit.ly, tinyurl.com, ow.ly, tumblr.com, ff.im,youtu.be, tl.gd, plurk.com, url4.eu, j.mp, goo.gl, yfrog

Cisco recommends this to be enabled for URL Filtering configuration best practices. Once enabled, the mail logs reflect anytime a shortened URL is used within the message:

```
Mon Aug 27 14:56:49 2018 Info: MID 1810 having URL: http://bit.ly/2tztQUi has been expanded to https://
```

Once URL Filtering is enabled as described in this article, from the mail_logs example, we can see the bit.ly

link is recorded, AND the original link it expands out to is also recorded.

• **Additional Information**

Cisco Secure Email Gateway Documentation

- [Release Notes](#)
- [User Guide](#)
- [CLI Reference Guide](#)
- [API Programming Guides for Cisco Secure Email Gateway](#)
- [Open Source Used in Cisco Secure Email Gateway](#)
- [Cisco Content Security Virtual Appliance Installation Guide](#)(includes vESA)

Secure Email Cloud Gateway Documentation

- [Release Notes](#)
- [User Guide](#)

Cisco Secure Email and Web Manager Documentation

- [Release Notes and Compatibility Matrix](#)
- [User Guide](#)
- [API Programming Guides for Cisco Secure Email and Web Manager](#)
- [Cisco Content Security Virtual Appliance Installation Guide](#)(includes vSMA)

Cisco Secure Product Documentation

- [Cisco Secure portfolio naming architecture](#)