APPENDIX A

CSC SSM Syslog Messages

This appendix lists the syslog messages in numerical order, and includes the following sections:

Messages 181248 - 2392320

Table A-1 shows the variables used by syslog messages in this section.

Table A-1 Messages 181248 - 2392320 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$group	Group name as designated in user/group policy configuration.
$info	Information that explains more about the syslog message
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file-types. • Content filtering uses "Subject," "Body," and "Attachment."
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$proto	Protocol name or value, such as SMTP, POP3, HTTP, FTP
$srcip:$srcport	Source IP address and port number from TCP/IP header
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +–: a plus or minus sign to indicate time zone offset from UTC (+ or –) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable	Description
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$URL	HTTP URL address accessed where spyware was found
$user	Client IP address or username, if username is identified by AD/LDAP integration
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

181248 - Unexpected Connection Loss

Error Message `181248:<$timestamp> A connection was dropped from source $srcip:$srcport to destination $dstip:$dstport via $proto. ($info)`

Example `181248: 2009-03-19T14:23:54-0700 A connection was dropped from source 1.1.1.1:132 to destination 2.2.2.2:25 via SMTP. (network timeout)`

Explanation A connection was not closed normally by the source or the destination. Abnormal closures may be due to timeouts or errors from the source or the destination, or possibly timeouts or errors that occurred in the content security application.

Recommended Action None required unless too many disconnections have been reported or usability issues were discovered.

2113664 - Virus Detected in HTTP but Delivered

Error Message 2113664:<*$timestamp*> Virus - *$vname* (*$vtype*) was detected from source $srcip:$srcport to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file "*$filename*" was passed. The URL accessed was "*$URL*".

Example 2113664: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "eicar.com" was passed. The URL accessed was "http://www.example.com/eicar.com".

Explanation A virus was detected in an HTTP transaction. The infected content was delivered "as-is".

Recommended Action Perform virus scanning on the source and/or the destination, if they are internal. Consider changing the policy settings to block (not deliver) viruses.

2113792 - Virus Blocked in HTTP

Error Message 2113792:<*$timestamp*> Virus - *$vname* (*$vtype*) was detected from source $srcip:$srcport to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file "*$filename*" was blocked. The URL accessed was "*$URL*".

Example 2113792: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "eicar.com" was blocked. The URL accessed was "http://www.example.com/eicar.com".

Explanation A virus was detected in an HTTP transaction. The infected content was blocked.

Recommended Action Perform virus scanning on the violation source, if it is internal.

2113920 - Virus Detected and Cleaned in HTTP

Error Message 2113920:<*$timestamp*> Virus - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file "*$filename*" was cleaned. The URL accessed was "*$URL*".

Example 2113920: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "eicar.com" was cleaned. The URL accessed was "http://www.example.com/eicar.com".

Explanation A virus was detected in an HTTP transaction. The infected content was cleaned then delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

2162816 - Spyware Detected in HTTP but Delivered

Error Message 2162816:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file “*$filename*” was passed. The URL accessed was “*$URL*”.

Example 2162816: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file “clickme.com” was passed. The URL accessed was “http://www.example.com/clickme.com”.

Explanation Spyware was detected in an HTTP transaction. The spyware was delivered “as-is.”

Recommended Action Perform spyware scanning on the receiving machine and the violation source, if they are internal. Consider changing the policy settings to block (not deliver) spyware.

2162944 - Spyware Blocked in HTTP

Error Message 2162944:<*$timestamp*> Spyware - *$vname* (*$vtype*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file “*$filename*” was blocked. The URL accessed was “*$URL*”.

Example 2162944: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file “clickme.com” was blocked. The URL accessed was “http://www.example.com/clickme.com”.

Explanation Spyware was detected in an HTTP transaction. The spyware was blocked.

Recommended Action Perform virus scanning on the violation source, if it is internal.

2212096 - File Blocked in HTTP

Error Message 2212096:<*$timestamp*> File Blocking- *$pname* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via HTTP. The source of violation was *$vip:$vport*. The file “*$filename*” was blocked. The URL accessed was “*$URL*”.

Example 2212096: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The file “iplayer.zip” was blocked. The URL accessed was “http://www.example.com/iplayer/iplayer.zip”.

Explanation A file blocking violation was detected during HTTP access. The access was blocked.

Recommended Action None required.

2228480 - HTTP URL Blocking Blocked

Error Message `2228480:<$timestamp> URL Blocking - user-defined ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The URL was blocked. The URL accessed was "$URL". The user identity was "$user" ($group). The policy matched was "$pname".`

Example `2228480: 2009-03-19T14:23:54-0700 URL Blocking - user-defined (*play*) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The URL was blocked. The URL accessed was "http://www.example.com/iplayer/index.html". The user identity was "finance/joek" (US West BU Finance Dept). The policy matched was "Global Policy".`

Explanation An HTTP access violation was detected based on URL Blocking policy. The access was blocked.

Recommended Action None required.

2244608 - URL Rating Module Error

Error Message `2244608:<$timestamp> URL Rating Module: $info`

Example `2244608: 2009-03-19T14:23:54-0700 URL Rating Module: Error: Failed to rate URL, rc=-231`

Explanation The URL Rating Module reports operational information.

Recommended Action Verify network setup and connections to the Internet.

2244609 - URL Rating Module Information

Error Message `2244609:<$timestamp> URL Rating Module: $info`

Example `2244609: 2009-03-19T14:23:54-0700 URL Rating Module: Started`

Explanation The URL Rating Module reports operational information.

Recommended Action None required.

2244864 - HTTP URL Filtering Blocked

Error Message `2244864:<$timestamp> URL Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The URL was blocked. The URL accessed was "$URL". The user identity was $user ($group). The policy matched was "$pname".`

Example `2244864: 2009-03-19T14:23:54-0700 URL Filtering - Company Prohibited Sites (Gambling) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The URL was blocked. The URL accessed was "http://www.example.com/casino/index.html". The user identity was "finance/joek" (Finance Dept). The policy matched was "Global Policy".`

Explanation An HTTP access violation was detected based on the URL Filtering policy. The access was blocked.

Recommended Action None required.

2359424 - HTTP Unscanned Content Detected but Delivered

Error Message `2359424:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The file "$filename" was passed. The URL accessed was "$URL".`

Example `2359424: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "broken.zip" was passed. The URL accessed was "http://www.example.com/broken.zip".`

Explanation An unscanned attachment was detected during HTTP access. CSC did not scan this content because of a resource or protocol limitation. The original content was delivered anyway.

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

2359552 - Unscanned Content Blocked in HTTP

Error Message `2359552:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The file "$filename" was blocked. The URL accessed was "$URL".`

Example `2359552: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 22.22.22.22:80. The file "broken.zip" was blocked. The URL accessed was "http://www.example.com/broken.zip".`

Explanation Unscanned content was blocked in an HTTP transaction.

Recommended Action Blocking unscanned files may break certain applications that use the "resume transfer" function, such as Windows Update. Customers can either deliver the unscanned content or set the ASA Modular Policy Framework policy to avoid scanning traffic to and from the destination IP address.

2392320 -HTTP Web Reputation Blocked

Error Message `2392320:<$timestamp> Web Reputation - Potentially malicious URL was detected from source $srcip:$srcport to destination $dstip:$dstport via HTTP. The source of violation was $vip:$vport. The URL was blocked. The URL accessed was "$URL". The user identity was $user ($group). The policy matched was "$pname".`

Example `2392320: 2009-03-19T14:23:54-0700 Web Reputation - Potentially malicious URL was detected from source 10.0.0.1:3333 to destination 22.22.22.22:80 via HTTP. The source of violation was 10.0.0.1:3333. The URL was blocked. The URL accessed was "http://www.example.com/casino/index.html". The user identity was "finance/joek" (US West BU Finance Dept). The policy matched was "Global Policy".`

Explanation An HTTP access violation was detected based on the Web Reputation policy. The access was blocked.

Recommended Action None required.

Messages 4423808- 6603008

Table A-2 shows the variables used by syslog messages in this section.

Table A-2 Messages 4423808 - 6603008 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$msgact	Action taken on the message (blocked or delivered)
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file-types. • Content filtering uses “Subject,” “Body,” and “Attachment.”
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$recipient	Recipient’s e-mail address
$sender	Sender’s e-mail address
$srcip:$srcport	Source IP address and port number from TCP/IP header
$subject	Subject line of the e-mail message in question
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character “T” • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable	Description
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

4423808 - SMTP Spam Detected (Match in ERS Standard Database List)

Error Message `4423808:<$timestamp> Spam (identified by Email Reputation Standard Database) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `4423808: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Standard Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was passed.`

Explanation An inbound SMTP connection was flagged as potential spam by the ERS Standard Database list. The SMTP connection was allowed. The actual e-mail delivery was still subject to other content scanning.

Recommended Action None required. Consider blocking ERS if too much spam is received.

4423936 - SMTP Spam Blocked (Match in ERS Standard Database List)

Error Message `4423936:<`*`$timestamp`*`> Spam (identified by Email Reputation Standard Database) was detected from source `*`$srcip:$srcport`*` to destination `*`$dstip:$dstport`*` via SMTP. The source of violation was `*`$vip:$vport`*`. The mail was from sender "`*`$sender`*`" to recipient "`*`$recipient`*`". The mail was blocked.`

Example `4423936: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Standard Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was blocked.`

Explanation An inbound SMTP connection was blocked by the ERS Standard Database list. This blocking may prevent one or more potential spam e-mail messages from being delivered.

Recommended Action None required. If this blocking is incorrect, try the following actions:

- Add *$srcip* to the ERS Exception List.
- Visit the ERS Portal to update the configuration or dispute.

4440192 - SMTP Spam Detected (Match in ERS Dynamic Database List)

Error Message `4440192:<`*`$timestamp`*`> Spam (identified by Email Reputation Dynamic Database) was detected from source `*`$srcip:$srcport`*` to destination `*`$dstip:$dstport`*` via SMTP. The source of violation was `*`$vip:$vport`*`. The mail was from sender "`*`$sender`*`" to recipient "`*`$recipient`*`". The mail was passed.`

Example `4440192: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Dynamic Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was passed.`

Explanation An inbound SMTP connection was flagged as potential spam by the ERS Dynamic Database list. The SMTP connection was allowed. The actual e-mail delivery was still subject to other content scanning.

Recommended Action None required. Consider blocking ERS if too much spam is received.

4440320 - SMTP Spam Blocked (Match in ERS Dynamic Database List)

Error Message `4440320:<$timestamp> Spam (identified by Email Reputation Dynamic Database) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `4440320: 2009-03-19T14:23:54-0700 Spam (identified by Email Reputation Dynamic Database) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was from sender "foo@foo.com" to recipient "bar@bar.com". The mail was blocked.`

Explanation An inbound SMTP connection was blocked by the ERS Dynamic Database list. This blocking may stop one or more potential spam e-mail messages from being delivered.

Recommended Action None required. If this blocking is incorrect, try the following actions:

- Add *$srcip* to the ERS Exception List.
- Visit the ERS Portal to update the configuration or dispute.

6307968 - POP3 Virus Detected but Delivered

Error Message `6307968:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6307968: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was passed then the mail was passed.`

Explanation A virus was detected in a POP3 message. The mail was delivered anyway.

Recommended Action Perform virus scanning on the receiving machine to ensure virus removal. Perform virus scanning on the POP3 server, if it is internal. Consider changing the policy settings to block (not deliver) viruses.

6308096 - POP3 Virus Blocked

Error Message `6308096:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6308096: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was blocked then the mail was passed.`

Explanation A virus was detected in a POP3 message. The infected attachment was removed, and the mail was delivered.

Recommended Action Perform virus scanning on the POP3 server, if it is internal.

6308224 - POP3 Virus Cleaned and Delivered

Error Message `6308224:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was cleaned then the mail was $msgact.`

Example `6308224: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was cleaned then the mail was passed.`

Explanation A virus was detected in a POP3 message. The infected attachment was cleaned, and the mail was delivered.

Recommended Action Customers should perform virus scanning on the POP3 server, if it is internal.

6357120 - Spyware Detected in POP3 but Delivered

Error Message `6357120:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6357120: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.`

Explanation Spyware was detected in a POP3 message. The mail was delivered "as-is."

Recommended Action Perform spyware scanning on the receiving machine to ensure spyware removal. Consider changing the customer's policy setting to block (not deliver) spyware.

6357248 - Spyware Blocked in POP3

Error Message `6357248:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6357248: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation Spyware was detected in a POP3 message. The mail was delivered without the detected spyware.

Recommended Action None required.

6373504 - POP3 IntelliTrap Detected by Delivered

Error Message `6373504:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6373504: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.`

Explanation IntelliTrap was detected in a POP3 message. The original mail was delivered "as is."

Recommended Action Perform malware scanning on the receiving machine to ensure malware removal. Consider changing the policy settings to block (not deliver) IntelliTrap.

6373632 - POP3 IntelliTrap Blocked

Error Message `6373632:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6373632: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation IntelliTrap was detected in a POP3 message. The malware was removed and the mail was delivered.

Recommended Action None required.

6406272 - File Detected in POP3 Message but Delivered

Error Message `6406272:<$timestamp> File Blocking - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6406272: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was passed then the mail was passed.`

Explanation A file blocking violation was detected in an inbound SMTP message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

6406400 - File Blocked in POP3 Message

Error Message `6406400:<$timestamp> File Blocking - $pname ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6406400: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 22.22.22.22:110. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was blocked then the mail was passed.`

Explanation A file blocking violation was detected in a POP3 message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

6455424 - E-mail Content-filtering Violation Detected in POP3 Message

Error Message `6455424:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `6455424: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.`

Explanation A content-filtering violation was detected in POP3 message. The mail was delivered.

Recommended Action None required.

6455552 - E-mail Content-filtering Violation Detected in POP3 Message

Error Message `6455552:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `6455552: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.`

Explanation A content-filtering violation was detected in POP3 message. The mail was blocked.

Recommended Action None required.

6553728 - Unscanned Content Detected in POP3 but Delivered

Error Message `6553728:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `6553728: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was passed then the mail was passed.`

Explanation An unscanned attachment was detected in a POP3 message, and CSC did not scan this content because of a resource or protocol limitation. The original mail was delivered "as-is."

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

6553856 - Unscanned Content Blocked in POP3

Error Message `6553856:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via POP3. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `6553856: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:110 via POP3. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was blocked then the mail was passed.`

Explanation An unscanned attachment was detected in a POP3 message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

6602880 - Spam Detected in POP3

Error Message 6602880:<*$timestamp*> Spam (identified by pattern-recognition technology) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via POP3. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "$sender" to recipient "*$recipient*". The mail was passed.

Example 6602880: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spammer" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.

Explanation A spam mail was detected in a POP3 message. The mail was delivered "as-is."

Recommended Action None required.

6603008 - Spam Blocked in POP3

Error Message 6603008:<*$timestamp*> Spam (identified by pattern-recognition technology) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via POP3. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The mail was blocked.

Example 6603008: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via POP3. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spammer" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.

Explanation A spam mail was detected in a POP3 message. The mail was blocked.

Recommended Action None required.

Messages 8405120 - 8651008

Table A-3 shows the variables used by syslog messages in this section.

Table A-3 Messages 8405120 - 8651008 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$srcip:$srcport	Source IP address and port number from TCP/IP header
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +–: a plus or minus sign to indicate time zone offset from UTC (+ or –) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

8405120 - Virus Detected in FTP but Delivered

Error Message `8405120:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was passed.`

Example `8405120: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "eicar.com" was passed.`

Explanation A virus was detected in an FTP transaction. The infected content was delivered.

Recommended Action Customers should perform virus scanning on the source and/or the destination, if they are internal. Consider changing the policy setting to block (not deliver) viruses.

8405248 - Virus Blocked in FTP

Error Message `8405248:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was blocked.`

Example `8405248: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "eicar.com" was blocked.`

Explanation A virus was detected in an FTP transaction. The infected content was blocked.

Recommended Action Perform virus scanning on the violation source, if it is internal.

8405376 - FTP Virus Cleaned and Delivered

Error Message `8405376:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was cleaned.`

Example `8405376: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "eicar.com" was cleaned.`

Explanation A virus was detected in a FTP transaction. The infected content was cleaned then delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

8454272 - Spyware Blocked in FTP but Delivered

Error Message `8454272:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was passed.`

Example `8454272: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "clickme.com" was passed.`

Explanation Spyware was detected in an FTP transaction. The spyware was passed "as-is."

Recommended Action Perform spyware scanning on the receiving machine and the source of violation, if they are internal. Consider changing the policy setting to block (not deliver) spyware.

8454400 - Spyware Blocked in FTP

Error Message `8454400:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was blocked.`

Example `8454400: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "clickme.com" was blocked.`

Explanation Spyware was detected in an FTP transaction. The spyware was blocked.

Recommended Action Perform spyware scanning on the violation source, if it is internal.

8503552 - File Blocked in FTP

Error Message `8503552:<$timestamp> File Blocking - $pname ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was blocked.`

Example `8503552: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "iplayer.zip" was blocked.`

Explanation A file blocking violation was detected during FTP access. The access was blocked.

Recommended Action None required.

8650880 - Unscanned Content Detected in FTP but Delivered

Error Message `8650880:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was passed.`

Example `8650880: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "broken.zip" was passed.`

Explanation An unscanned file was detected during FTP access. CSC did not scan this content because of a resource or protocol limitation. The file was passed “as-is.”

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

8651008 - Unscanned Content Blocked in FTP

Error Message `8651008:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via FTP. The source of violation was $vip:$vport. The file "$filename" was blocked.`

Example `8651008: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:21 via FTP. The source of violation was 22.22.22.22:21. The file "broken.zip" was blocked.`

Explanation Unscanned content was blocked in an FTP transaction.

Recommended Action Blocking unscanned files may break certain applications that use the “resume transfer” function, such as Windows Update. Customers can either deliver the unscanned content or set the ASA MPF policy to avoid scanning traffic to and from the destination IP address.

Messages 16777216 - 18874370

Table A-4 shows the variables used by syslog messages in this section.

Table A-4 Messages 16777216 - 18874370 Section Variables

Variable	Description
$component	Application components, such as Protocol Proxy, Scan Server, Service Module, System Monitor, Event Manager, Config Manager, URL Rating Module, E-mail Notification Module, Virus Scan Engine, Virus Pattern, and Spyware Pattern
$info	Information that explains more about the syslog message
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)
$version	The product or component version number

16777216 - Update Not Successful

Error Message `16777216:<$timestamp> Component update failed: $component/$version ($info)`

Example `16777216: 2009-03-19T14:23:54-0700 Component update failed: VirusScanEngine/9.0.1000 (network timeout)`

Explanation A content security component has failed to be updated.

Recommended Action Verify your network configuration, network connectivity, or ActiveUpdate configuration.

16777217 - Update Status Report

Error Message `16777217:<$timestamp> Component successfully updated: $component/$version`

Example `16777217: 2009-03-19T14:23:54-0700 Component successfully updated: VirusScanEngine/8.5.1001`

Explanation A content security component has been successfully updated.

Recommended Action None required.

18874368 - License Status Update

Error Message `18874368:<$timestamp> The Content Security license has been updated. License Details: $info`

Example `18874368: 2009-03-19T14:23:54-0700 The Content Security license has been updated. License Details: Hardware S/N: JAA0828037K, No of Users: 50, License Type: Standard, License Key: PZ-8XJ4-MQ7JL-DZGCD-5WLJC-T26ZZ-WJ63B, License Expiration Date: 2008-01-31`

Explanation The Content Security license has been updated because of license activation or license renewal.

Recommended Action None required.

18874369 - License has Expired

Error Message `18874369:<$timestamp> The Content Security license has expired. License Details: $info`

Example `18874369: 2009-03-19T14:23:54-0700 The Content Security license has expired. License Details: Hardware S/N: JAA0828037K, No of Users: 50, License Type: Standard, License Key: PZ-8XJ4-MQ7JL-DZGCD-5WLJC-T26ZZ-WJ63B, License Expiration Date: 2008-01-31`

Explanation The Content Security license has expired and may stop inspecting traffic.

Recommended Action To renew or purchase the license, contact your reseller or visit http://www.cisco.com/go/asa.

18874370 - License Expiration Reminder

Error Message `18874370:<$timestamp> The Content Security license is due to expire. License Details: $info`

Example `18874370: 2009-03-19T14:23:54-0700 The Content Security license is due to expire. License Details: Hardware S/N: JAA0828037K, No of Users: 50, License Type: Standard, License Key: PZ-8XJ4-MQ7JL-DZGCD-5WLJC-T26ZZ-WJ63B, License Expiration Date: 2008-01-31`

Explanation The Content Security license is going to expire on the specified expiration date.

Recommended Action Renew the Content Security license before the product expires. Contact your reseller or visit http://www.cisco.com/go/asa.

Messages 21151744 - 21184513

Table A-5 shows the variables used by syslog messages in this section.

Table A-5 Messages 21151744 - 21184513 Section Variables

Variable	Description
$info	Information that explains more about the syslog message
$proto	Protocol name or value, such as SMTP, POP3, HTTP, FTP
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character “T” • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

21151744 - System Monitoring Critical Condition Message

Error Message `21151744:<$timestamp> System Monitor: $info`

Example `21151744: 2009-03-19T14:23:54-0700 System Monitor: HTTP service is DOWN.`

Explanation The System Monitor reports critical operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

21151745 - System Monitoring Error Condition Message

Error Message `21151745:<$timestamp> System Monitor: $info.`

Example `21151745: 2009-03-19T14:23:54-0700 System Monitor: Invalid ASA state is received.`

Explanation The System Monitor reports error operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

21151746 - System Monitoring Informational Message

Error Message `21151746:<$timestamp> System Monitor: $info.`

Example `21151746: 2009-03-19T14:23:54-0700 System Monitor: CSC SSM is not activated.`

Explanation The System Monitor reports normal operational information.

Recommended Action None required.

21151747 - System-level Notice

Error Message `21151747:<$timestamp> System Monitor: $info.`

Example `21151747: 2009-03-19T14:23:54-0700 System Monitor: Set CSC SSM Application Status to UP.`

Explanation The System Monitor reports normal operational information.

Recommended Action None required.

21152512 - System is Ready

Error Message `21152512:<$timestamp> Content Security system is ready.`

Example `21152512: 2009-03-19T14:23:54-0700 Content Security system is ready.`

Explanation The content security system is ready to inspect traffic.

Recommended Action None required.

21152513 - System is Reloading

Error Message `21152513:<$timestamp> Content Security system is reloading. ($info)`

Example `21152513: 2009-03-19T14:23:54-0700 Content Security system is reloading. (configuration update)`

Explanation The content security system is reloading for administrative reasons, such as a configuration update or a pattern/engine update.

Recommended Action If the system becomes ready shortly, none required.

21152514 - System is Down

Error Message `21152514:<$timestamp> Content Security system has failed. ($info)`

Example `21152514: 2009-03-19T14:23:54-0700 Content Security system has failed. (Scan Server has failed)`

Explanation The content security system has failed and is unable to inspect traffic.

Recommended Action Check for a valid license or system failure. Reload the system if necessary.

21184512 - Maximum Connections Reached

Error Message `21184512:<$timestamp> The maximum number of connections for $proto has been reached. New connections will be kept in a backlog and may time out.`

Example `21184512: 2009-03-19T14:23:54-0700 The maximum number of connections for SMTP has been reached. New connections will be kept in a backlog and may time out.`

Explanation The device has reached its maximum concurrent scanning for the specific protocol. New connections with the same protocol will be queued and may time out. Network performance may be affected.

Recommended Action If this issue occurs frequently, the device may be underpowered for the amount of traffic being passed. Consider scanning less traffic with ASA MPF skip rules or segmenting the network with more adaptive security appliances.

21184513 - Maximum Connections Returned to Normal

Error Message `21184513:<$timestamp> The maximum number of connections for $proto has returned to normal threshold.`

Example `21184513: 2009-03-19T14:23:54-0700 The maximum number of connections for SMTP has returned to normal threshold.`

Explanation The concurrent connections of the specific protocol have fallen below 80 percent of the maximum capacity. New connections of the specific protocol can be processed normally.

Recommended Action None required.

Messages 33570944 - 33865984

Table A-6 shows the variables used by syslog messages in this section.

Table A-6 Messages 33570944 - 33865984 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$msgact	Action taken on the message (blocked or delivered)
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file-types. • Content filtering uses “Subject,” “Body,” and “Attachment.”
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses “user-defined.” • File Blocking uses user-configured file types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$recipient	Recipient’s e-mail address
$sender	Sender’s e-mail address
$srcip:$srcport	Source IP address and port number from TCP/IP header
$subject	Subject line of the e-mail message in question
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character “T” • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable	Description
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

33570944 - Incoming Virus Detected in SMTP but Delivered

Error Message `33570944:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `33570944: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was passed then the mail was passed.`

Explanation A virus was detected in an inbound SMTP message. The mail was delivered “as-is.”

Recommended Action Perform virus scanning on the receiving machine to ensure virus removal. Consider changing the policy settings to block (not deliver) viruses.

33571072 - Virus Blocked in SMTP (Incoming)

Error Message `33571072:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled “$subject” from sender “$sender” to recipient “$recipient”. The file “$filename” was blocked then the mail was $msgact.`

Example `33571072: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello from eicar” from sender “user1@example.com” to recipient “user2@example.com”. The file “eicar.com” was blocked then the mail was passed.`

Explanation A virus was detected in an inbound SMTP message. The infected attachment was removed, and the mail was delivered.

Recommended Action None required.

33571200 - Incoming SMTP Virus Cleaned and Delivered

Error Message `33571200:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled “$subject” from sender “$sender” to recipient “$recipient”. The file “$filename” was cleaned then the mail was $msgact.`

Example `33571200: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello from eicar” from sender “user1@example.com” to recipient “user2@example.com”. The file “eicar.com” was cleaned then the mail was passed.`

Explanation A virus was detected in an inbound SMTP message. The infected attachment was cleaned, and the mail was delivered.

Recommended Action None required.

33620096 - Incoming SMTP Spyware Detected but Delivered

Error Message

```
33620096:<$timestamp> Spyware - $vname ($vtype) was detected from
source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of
violation was $vip:$vport. The mail was titled "$subject" from sender "$sender"
to recipient "$recipient". The file "$filename" was passed then the mail was
$msgact.
```

Example

```
33620096: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was
detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The
source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy"
from sender "user1@example.com" to recipient "user2@example.com". The file
"clickme.exe" was passed then the mail was passed.
```

Explanation Spyware was detected in an inbound SMTP message. The original mail was delivered "as-is."

Recommended Action Perform spyware scanning on the receiving machine to ensure spyware removal. Consider changing the policy settings to block (not deliver) spyware.

33620224 - Incoming SMTP Spyware Blocked

Error Message

```
33620224:<$timestamp> Spyware - $vname ($vtype) was detected from
source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of
violation was $vip:$vport. The mail was titled "$subject" from sender "$sender"
to recipient "$recipient". The file "$filename" was blocked then the mail was
$msgact.
```

Example

```
33620224: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was
detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The
source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy"
from sender "user1@example.com" to recipient "user2@example.com". The file
"clickme.exe" was blocked then the mail was passed.
```

Explanation Spyware was detected in an inbound SMTP message. The spyware was removed, and the mail was delivered.

Recommended Action None required.

33636480 - Incoming SMTP IntelliTrap Detected but Delivered

Error Message `33636480:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `33636480: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was passed then the mail was passed.`

Explanation IntelliTrap was detected in an inbound SMTP message. The original mail was delivered "as-is."

Recommended Action Perform malware scanning on the receiving machine to ensure malware removal. Consider changing the policy settings to block (not deliver) IntelliTrap.

33636608- Incoming SMTP IntelliTrap Blocked

Error Message `33636608:<$timestamp> IntelliTrap - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `33636608: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP (GenericUnpack) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello from spy" from sender "user1@example.com" to recipient "user2@example.com". The file "clickme.exe" was blocked then the mail was passed.`

Explanation IntelliTrap was detected in an inbound SMTP message. The malware was removed and the mail was delivered.

Recommended Action None required.

33669248 - Incoming SMTP File Blocking Detected but Delivered

Error Message `33669248:<$timestamp> File Blocking - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled “$subject” from sender “$sender” to recipient “$recipient”. The file “$filename” was passed then the mail was $msgact.`

Example `33669248: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello” from sender “user1@example.com” to recipient “user2@example.com”. The file “hello.zip” was passed then the mail was passed.`

Explanation Spyware was detected in an outbound SMTP message. The mail was delivered “as-is.”

Recommended Action Perform spyware scanning on the sending machine to ensure spyware removal. Consider changing policy settings to block (not deliver) spyware.

33669376 - File Blocked in Incoming SMTP Message

Error Message `33669376:<$timestamp> File Blocking - $pname ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled “$subject” from sender “$sender” to recipient “$recipient”. The file “$filename” was blocked then the mail was $msgact.`

Example `33669376: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello” from sender “user1@example.com” to recipient “user2@example.com”. The file “hello.zip” was blocked then the mail was passed.`

Explanation A file blocking violation was detected in an inbound SMTP message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

33718400 - E-mail Content-filtering Violation Blocked in SMTP - Incoming

Error Message `33718400:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was passed.`

Example `33718400: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.`

Explanation A content-filtering violation was detected in SMTP-Incoming message. The mail was delivered.

Recommended Action None required.

33718528 - E-mail Content-filtering Violation Blocked in SMTP - Incoming

Error Message `33718528:<$timestamp> Content-Filtering - $pcat ($prule) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The mail was blocked.`

Example `33718528: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.`

Explanation A content-filtering violation was detected in SMTP-Incoming message. The mail was blocked.

Recommended Action None required.

33816704 - Incoming SMTP Unscanned Content Detected and Delivered

Error Message `33816704:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `33816704: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was passed then the mail was passed.`

Explanation An unscanned attachment was detected in an inbound SMTP message, and CSC did not scan this content because of a resource or protocol limitation. The mail was delivered "as-is."

Recommended Action Unscanned files may or may not be safe. Scan the receiving machine for malware.

33816832 - Incoming SMTP Unscanned Content Blocked

Error Message `33816832:<$timestamp> Unscanned - $unscanexp (N/A) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `33816832: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "broken.zip" was blocked then the mail was passed.`

Explanation An unscanned attachment was detected in an inbound SMTP message. The attachment was removed, and the mail was delivered.

Recommended Action None required.

33865856 - SMTP Spam is Detected but Delivered

Error Message 33865856:<*$timestamp*> Spam (identified by pattern-recognition technology) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The mail was passed.

Example 33865856: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello from spammer” from sender “user1@example.com” to recipient “user2@example.com”. The mail was passed.

Explanation A spam mail was detected in a SMTP message. The mail was delivered “as is.”

Recommended Action None required.

33865984 -SMTP Spam Blocked

Error Message 33865984:<*$timestamp*> Spam (identified by pattern-recognition technology) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The mail was blocked.

Example 33865984: 2009-03-19T14:23:54-0700 Spam (identified by pattern-recognition technology) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello from spammer” from sender “user1@example.com” to recipient “user2@example.com”. The mail was blocked.

Explanation A spam mail was detected in a SMTP message. The mail was blocked.

Recommended Action None required.

Messages 35668096 - 48234497

Table A-7 shows the variables used by the syslog messages in this section.

Table A-7 Messages 35668096 - 48234497 Section Variables

Variable	Description
$dstip:$dstport	Destination IP address and port number from TCP/IP header
$filename	Name of file with suspected problem
$info	Information that explains more about the syslog message.
$msgact	Action taken on the message (blocked or delivered)
$pcat	Policy categories are used in the following features: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file-types. • Content filtering uses "Subject," "Body," and "Attachment."
$pname	Policy name, for example: • URL Filtering uses URL category grouping. • URL Blocking uses "user-defined." • File Blocking uses user-configured file-types.
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$recipient	Recipient's e-mail address
$sender	Sender's e-mail address
$srcip:$srcport	Source IP address and port number from TCP/IP header
$subject	Subject line of the e-mail message in question
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delays or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)

Variable (continued)	Description (continued)
$unscanexp	Names an unscanned exception, such as: • Decompressed_File_Size_Exceeded • Compression_Layer_Count_Exceeded • Compression_Ratio_Limit_Exceeded • Decompressed_File_Count_Exceeded • Password-Protected_File • Corrupt_Compressed_File • Unsupported_Compression_Type • Scanning_Limit_Exceeded
$vip:$vport	IP address of the machine and port number of the connection that violates the policy
$vname	Name of the virus or spyware detected
$vtype	Type of virus or spyware found (worm, dialer, or bot)

35668096 - Outgoing SMTP Virus Detected but Delivered

Error Message `35668096:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was passed then the mail was $msgact.`

Example `35668096: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was passed then the mail was passed.`

Explanation A virus was detected in an outbound SMTP message. The mail was delivered "as-is."

Recommended Action Perform virus scanning on the violation source, if it is internal. Consider changing the policy settings to block (not deliver) viruses.

35668224 - Virus Blocked in SMTP-Outgoing

Error Message `35668224:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was blocked then the mail was $msgact.`

Example `35668224: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was blocked then the mail was passed.`

Explanation A virus was detected in an outbound SMTP message. The infected attachment was removed, and the mail was delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

35668352 - Outgoing SMTP Virus Cleaned and Delivered

Error Message `35668352:<$timestamp> Virus - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled "$subject" from sender "$sender" to recipient "$recipient". The file "$filename" was cleaned then the mail was $msgact.`

Example `35668352: 2009-03-19T14:23:54-0700 Virus - EICAR_TEST_VIRUS (Virus) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello from eicar" from sender "user1@example.com" to recipient "user2@example.com". The file "eicar.com" was cleaned then the mail was passed.`

Explanation A virus was detected in an outbound SMTP message. The infected attachment was cleaned, and the mail was delivered.

Recommended Action Perform virus scanning on the violation source, if it is internal.

35717248 - Outgoing SMTP Spyware Detected but Delivered

Error Message `35717248:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled “$subject” from sender “$sender” to recipient “$recipient”. The file “$filename” was passed then the mail was $msgact.`

Example `35717248: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled “Hello from spy” from sender “user1@example.com” to recipient “user2@example.com”. The file “clickme.exe” was blocked then the mail was passed.`

Explanation Spyware was detected in an inbound SMTP message. The spyware was removed, and the mail was delivered.

Recommended Action None required.

35717376 - Outgoing SMTP Spyware Blocked

Error Message `35717376:<$timestamp> Spyware - $vname ($vtype) was detected from source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of violation was $vip:$vport. The mail was titled “$subject” from sender “$sender” to recipient “$recipient”. The file “$filename” was blocked then the mail was $msgact.`

Example `35717376: 2009-03-19T14:23:54-0700 Spyware - TEST_ADWARE (Adware) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled “Hello from spy” from sender “user1@example.com” to recipient “user2@example.com”. The file “clickme.exe” was blocked then the mail was passed.`

Explanation Spyware was detected in an outbound SMTP message. The spyware was removed, and the mail was delivered.

Recommended Action Perform spyware scanning on the sending machine to ensure spyware removal.

35733632 - Outgoing SMTP IntelliTrap Detected but Delivered

Error Message

```
35733632:<$timestamp> IntelliTrap - $vname ($vtype) was detected from
source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of
violation was $vip:$vport. The mail was titled "$subject" from sender "$sender"
to recipient "$recipient". The file "$filename" was passed then the mail was
$msgact.
```

Example

```
35733632: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP
(GenericUnpack) was detected from source 22.22.22.22:3333 to destination
10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was
titled "Hello from spy" from sender "user1@example.com" to recipient
"user2@example.com". The file "clickme.exe" was passed then the mail was passed.
```

Explanation IntelliTrap was detected in an outbound SMTP message. The original mail was delivered "as-is."

Recommended Action Perform malware scanning on the receiving machine to ensure malware removal.

35733760- Outgoing SMTP IntelliTrap Blocked

Error Message

```
35733760:<$timestamp> IntelliTrap - $vname ($vtype) was detected from
source $srcip:$srcport to destination $dstip:$dstport via SMTP. The source of
violation was $vip:$vport. The mail was titled "$subject" from sender "$sender"
to recipient "$recipient". The file "$filename" was blocked then the mail was
$msgact.
```

Example

```
35733760: 2009-03-19T14:23:54-0700 IntelliTrap - TEST_ITRAP
(GenericUnpack) was detected from source 22.22.22.22:3333 to destination
10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was
titled "Hello from spy" from sender "user1@example.com" to recipient
"user2@example.com". The file "clickme.exe" was blocked then the mail was passed.
```

Explanation IntelliTrap was detected in an outbound SMTP message. The malware was removed and the mail was delivered.

Recommended Action Perform malware scanning on the sending machine to ensure malware removal.

35766400 - Outgoing SMTP File Blocking Detected but Delivered

Error Message 35766400:<*$timestamp*> File Blocking - *$pname* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was passed then the mail was *$msgact*.

Example 35766400: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was passed then the mail was passed.

Explanation A file blocking violation was detected in an outbound SMTP message. The mail was delivered with the original attachments.

Recommended Action None required.

35766528 - File Blocked on Outgoing SMTP Message

Error Message 35766528:<*$timestamp*> File Blocking - *$pcat* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The file "*$filename*" was blocked then the mail was *$msgact*.

Example 35766528: 2009-03-19T14:23:54-0700 File Blocking - Compressed File (zip) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The file "hello.zip" was blocked then the mail was passed.

Explanation A file blocking violation was detected in a POP3 message. The mail was delivered with original attachments.

Recommended Action None required.

35815552 - E-mail Content-filtering Violation Detected in SMTP Outgoing

Error Message 35815552:<*$timestamp*> Content-Filtering - *$pcat* (*$prule*) was detected from source $srcip:$srcport to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "$sender" to recipient "*$recipient*". The mail was passed.

Example 35815552: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was passed.

Explanation A content-filtering violation was detected in SMTP-Outgoing message. The mail was delivered.

Recommended Action None required.

35815680 - E-mail Content-filtering Violation Blocked in SMTP Outgoing

Error Message 35815680:<*$timestamp*> Content-Filtering - *$pcat* (*$prule*) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled "*$subject*" from sender "*$sender*" to recipient "*$recipient*". The mail was blocked.

Example 35815680: 2009-03-19T14:23:54-0700 Content-Filtering - Body (bad words) was detected from source 22.22.22.22:3333 to destination 10.0.0.1:25 via SMTP. The source of violation was 22.22.22.22:3333. The mail was titled "Hello" from sender "user1@example.com" to recipient "user2@example.com". The mail was blocked.

Explanation A content-filtering violation was detected in SMTP-Incoming message. The mail was blocked.

Recommended Action None required.

35913856 - Outgoing SMTP Unscanned Content Detected but Delivered

Error Message 35923856:<*$timestamp*> Unscanned - *$unscanexp* (N/A) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The file “*$filename*” was passed then the mail was *$msgact*.

Example 35923856: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled “Hello” from sender “user1@example.com” to recipient “user2@example.com”. The file “broken.zip” was passed then the mail was passed.

Explanation An unscanned attachment was detected in an outbound SMTP message. CSC did not scan this content because of a resource or protocol limitation. The mail was delivered “as-is.”

Recommended Action None required.

35913984 - Unscanned Content Blocked in SMTP (Outgoing)

Error Message 35913984:<*$timestamp*> Unscanned - *$unscanexp* (N/A) was detected from source *$srcip:$srcport* to destination *$dstip:$dstport* via SMTP. The source of violation was *$vip:$vport*. The mail was titled “*$subject*” from sender “*$sender*” to recipient “*$recipient*”. The file “*$filename*” was blocked then the mail was *$msgact*.

Example 35913984: 2009-03-19T14:23:54-0700 Unscanned - Corrupt_Compressed_File (N/A) was detected from source 10.0.0.1:3333 to destination 22.22.22.22:25 via SMTP. The source of violation was 10.0.0.1:3333. The mail was titled “Hello” from sender “user1@example.com” to recipient “user2@example.com”. The file “broken.zip” was blocked then the mail was passed.

Explanation An unscanned attachment was detected in an outbound SMTP message. The detected attachment was removed, and the mail was delivered.

Recommended Action None required.

39845888 - Scan Server Error

Error Message 39845888:<*$timestamp*> Scan Server: *$info*

Example 39845888: 2009-03-19T14:23:54-0700 Scan Server: Unable to allocate memory block for scan

Explanation The Scan Server reports abnormal operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

39845889 - Scan Server Information

Error Message `39845889:<$timestamp> Scan Server: $info`

Example `39845889: 2009-03-19T14:23:54-0700 Scan Server: Started`

Explanation The Scan Server reports abnormal operational information.

Recommended Action None required.

44220416 - Service Module Information

Error Message `44220416:<$timestamp> Service Module: $info`

Example `44220416: 2009-03-19T14:23:54-0700 Service Module: Application state: Up`

Explanation The Service Module reports operational information.

Recommended Action None required.

44220419 - Service Module Error

Error Message `44220419:<$timestamp> Service Module: $info`

Example `44220419: 2009-03-19T14:23:54-0700 Service Module: Init CP failed`

Explanation The service module reports abnormal operational information.

Recommended Action If the service module does not recover automatically, reboot theCSC SSM.

46317569 - Failover Module Information

Error Message `46317569:<$timestamp> Failover Module: $info`

Example `46317569: 2009-03-19T14:23:54-0700 Failover Module: Started`

Explanation The Failover Module reports operational information.

Recommended Action None required.

46317570 - Failover Module Error

Error Message `46317570:<$timestamp> Failover Module: $info`

Example `46317570: 2009-03-19T14:23:54-0700 Failover Module: HELLO handler error - The peers do not have the same software and/or hardware version.`

Explanation The Failover Module reports abnormal operational information.

Recommended Action Verify the failover configuration and network setup between the two peers.

48234496- Log Server Information

Error Message `48234496:<$timestamp> Log Server: $info`

Example `48234496: 2009-03-19T14:23:54-0700 Log Server: Unable to allocate memory`

Explanation The Log Server reports abnormal operational information.

Recommended Action If the issue persists, reboot the CSC SSM.

48234497- Log Server Information

Error Message `48234497:<$timestamp> Log Server: $info`

Example `48234497: 2009-03-19T14:23:54-0700 Log Server: Started`

Explanation The Log Server reports operational information.

Recommended Action None required.

Messages 52429184 - 52430720

Table A-8 shows the variables used in the syslog messages in this section.

Table A-8 Messages 52429184 - 52430720 Section Variables

Variable	Description
$component	Application component names, such as: Protocol Proxy, Scan Server, Service Module, System Monitor, Event Manager, Config Manager, URL Rating Module, E-mail Notification Module, Virus Scan Engine, Virus Pattern, and Spyware Pattern
$info	Information that explains more about the syslog message
$prule	Policy, rule, or setting, such as URL Filtering, URL Blocking, or File Blocking
$srcip	Source IP address from TCP/IP header

Variable (continued)	Description (continued)
$timestamp	Time that the event occurred. This allows the identification of the exact time an event was triggered. The timestamp may not reflect the event time, due to processing delay or queuing on the device. Time expressed as: [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS][+-][hhmm] Where: • YYYY: 4 digits for the year • MM: 2 digits for the month (01 to 12) • DD: 2 digits for the day (01 to 31) • T: a single character "T" • HH: 2 digits for the hour (00 to 23) • MM: 2 digits for the minute (00 to 59) • SS: 2 digits for the second (00 to 59) • +-: a plus or minus sign to indicate time zone offset from UTC (+ or -) • hh: 2 digits for the number of hours of time offset from UTC (00 to 12) • mm: 2 digits for the number of minutes of time offset from UTC (00 to 59)
$vname	Name of the virus or spyware detected

52429184 - DCS Successful Cleanup

Error Message `52429184:<`*`$timestamp`*`> Damage Cleanup - `*`$vname`*` (`*`$prule`*`) was cleaned successfully at `*`$srcip.`*

Example `52429184: 2009-03-19T14:23:54-0700 Damage Cleanup - WORM_SKA.A (Trojan) was cleaned successfully at 1.1.1.1.`

Explanation An internal machine was cleaned up successfully by the Damage Cleanup Service.

Recommended Action None required.

52430592 - DCS Cleanup Failed

Error Message `52430592:<`*`$timestamp`*`> Damage Cleanup - `*`$vname`*` (`*`$prule`*`) failed to be cleaned at `*`$srcip`*`.`

Example `52430592: 2009-03-19T14:23:54-0700 Damage Cleanup - WORM_SKA.A (Trojan) failed to be cleaned at 1.1.1.1.`

Explanation The Damage Cleanup Service failed to clean up an internal machine.

Recommended Action Perform manual malware cleanup on the machine specified.

52430720 - DCS Service Failed

Error Message `52430720:<$timestamp> Damage Cleanup - DCS server unreachable for cleanup at $srcip.`

Example `52430720: 2009-03-19T14:23:54-0700 Damage Cleanup - DCS server unreachable for cleanup at 1.1.1.1.`

Explanation The DCS server cannot be reached by CSC.

Recommended Action Verify the DCS server installation and configuration.