Cisco IronPort ESA CLI Reference Card

release 20160226, by Jens Roesen

Default user & password, batch command mode and contacts

The default username is **admin** and it's password is **ironport**. The default IP is 192.168.42.42 on Data1 on C1X0 appliances and Management Interface on all others.
For access through serial console use 9600/8-N-1 with hardware flow control.

Send undetected spam to *spam@access.ironport.com*, false positives to *ham@access.ironport.com*, missed ads to *ads@access.ironport.com* and false positive ads to *not_ads@access.ironport.com*. Send each as RFC822 MIME encoded attachment. See Knowledge Base article 472.

Basic commands

`help` *command* or `h` *command*	View online help for *command*.
`who`	Show a list of currently logged in users.
`whoami`	Show name and groups for current user.
`date`	View current date and time.
`passwd`	Change password for the current user.
`last`	Show list of recently logged in users and session dates.
`clear` or `clearchanges`	Abandon all pending configuration changes.
`commit`	Commit pending configuration changes.
`clustermode`	Switch between machine, cluster and group mode.
`shutdown`	Shut down and power-off the appliance.
`reboot`	Reboot the appliance.
`exit` or `quit` or `q`	Exit CLI. Will warn you about uncommitted changes.

Infos and status

`credits`	Show the credits for this AsyncOS version.
`version`	Show brief hardware and software information.
`ipcheck`	Show extended hardware and software information.
`status detail`	View detailed system status.
`healthcheck`	Analyse collected data to determine the health of the appliance.
`commitdetail`	View details about the last commit in the active session.
`showchanges`	View pending config changes as nested tree structure.
`antispamstatus`	Show status and latest update for enabled anti-spam engines.
`antivirusstatus`	Show status and latest update for active antivirus engines.
`websecuritydiagnostics`	View Web Security Service/URL Filtering statistics and errors.
`contentscannerstatus`	View content scanner engine version and latest update.
`repengstatus`	Show version and latest updates for SBRS engines.
`outbreakstatus`	Show status and last update of Virus Outbreak Filters.
`sbstatus`	Show SenderBase status.
`encryptionstatus`	Show PXE engine status and last engine update.
`dlpstatus`	Show status of RSA DLP engine.
`ecstatus`	Show enrollment client version info.
`showlicense`	Display virtual appliance license information.
`graymailstatus`	Display Graymail version information.
`workqueue status`	Display current work queue status.
`workqueue rate` *n*	Display number of pending, incoming and outgoing mails in the queue and refresh every *n* seconds.
`topin`	View top hosts by number of incoming connections.
`destqueue status` *dom*	Display destination-queue statistics for the domain *dom*.
`rate` *n*	Display in/out connections and recipient statistics every *n* sec.
`hostrate` *domain n*	Similar to rate but limited to a single destination domain.
`hoststatus` *domain*	View *domain* statistics including MX settings and latest 5xx error.
`tophosts`	View the top 20 destination domains in the mail queue.
`featurekey`	View, activate and check for new feature keys.
`dnsstatus`	Show DNS statistics since counter reset / last reboot / ever.
`displayalerts` *n*	Display the last *n* alerts sent by the appliance.
`supportrequeststatus`	Show version and last update of the support request keywords.

Test network and configuration

`ping` or `ping6`	Test network by sending a IPv4/IPv6 ping to a remote host.
`traceroute` or `traceroute6`	View IPv4/IPv6 network path/routing to a remote host.
`telnet`	Telnet to a remote host. Defaults to port 25, not 23!
`dig`	Run DNS queries. Supports batch mode.
`nslookup`	Run DNS queries.
`packetcapture`	Start a packet capture in AsyncOS versions up from 7.2.
`tcpdump`	Start a packet capture in AsyncOS versions up to 7.1.
`tcpservices`	Display information about running TCP/IP services.
`netstat`	Display current network connections, network statistics, interface status, listen queue size or routing table.
`trace`	Trace the mail flow through the system with a virtual test mail.
`ldaptest`	Run an LDAP query against a configured LDAP server.
`ldapflush`	Clear all cached LDAP query results.
`dnslisttest`	Manually test an IP against a DNS-based blacklist.
`dnsflush`	Flush DNS cache.
`tlsverify`	Test and verify a TLS connection to a remote MTA.

General configuration

`systemsetup`	Run the system setup wizard. This will remove any existing listener and associated HAT configuration.
`loadlicense`	Paste a virtual appliance XML license into CLI or load one from file.
`userconfig`	View and manage users and external authentication.
`adminaccessconfig`	Configure banner, restrict access on IP basis, configure XSS and CSRF protection and CLI/Web UI timeouts.
`interfaceconfig`	Add, delete and edit IP interface settings (IPv4 and IPv6).
`etherconfig`	Configure ethernet settings (speed/duplex mode, VLANs , NIC pairing)
`diskquotaconfig`	Configure disk space quotas for several services.
`healthconfig`	View and edit system health checks configuration.
`sethostname`	Set system hostname.
`setgateway`	Set default gateway.
`routeconfig`	Configure static network routes.
`dnsconfig`	Configure DNS servers and domain DNS settings.
`dnshostprefs`	Configure global or per domain DNS resolver preferences.
`dnslistconfig`	Configure global settings for DNS blacklist queries.
`featurekeyconfig`	Enable/disable auto-download and activation of feature keys.
`ldapconfig`	Create, delete and manage LDAP server profiles.
`snmpconfig`	Enable SNMP, set community string and password, define trap targets.
`ntpconfig`	Configure NTP Servers and source interface for NTP queries.
`sshconfig`	Configure sshd settings and view, add, delete or modify SSH user keys.
`sslconfig`	Configure SSL for SMTP and HTTPS GUI access (SSL Versions, Ciphers).
`sslv3config`	Enable/disable SSLv3 for EUQ, LDAP, Updater or Websecurity.
`settz`	Setup time zone.
`tzupdate`	Update time zone rules.
`settime`	Set system time and date as MM/DD/YYYY HH:MM:SS
`setttymode`	Set the TTY mode to interactive or non-interactive.
`generalconfig`	Configure browser settings (IE compatibility override mode).
`reportingconfig`	Configure reporting system.
`alertconfig`	Configure mail alert settings and mail alert recipients.
`trackingconfig`	Configure message tracking settings.
`addressconfig`	Set From: address to be used for mails generated by the system.
`fipsconfig`	Enable FIPS mode to meet FIPS 140-2 requirements.
`resetcounters`	Reset all counters of a single machine.

Configuring SMTP

`smtproutes`	Add, delete, edit and view SMTP routing.
`listenerconfig`	Configure and manage public, private or blackhole listeners.
`deliveryconfig`	Configure mail delivery settings.
`destconfig`	Configure destination control limits for a specified domain.
`exceptionconfig`	Configure and manage the domain exception table.
`altsrchost`	View, create and modify virtual gateway mappings for sender addresses or client IPs.
`bounceconfig`	Create and modify bounce profiles.
`policyconfig`	Configure and manage incoming and outgoing mail policies.
`textconfig`	Configure text blocks for use in disclaimers, anti-virus alerts, DLP, encryption notifications or bounces.
`filters`	Create, edit and view message filters.
`sievechar`	Configure Sieve filtering char used in LDAP Accept and Routing.
`dictionaryconfig`	Create and manage content dictionaries.
`sslconfig`	Configure SSL for TLS connections (Versions, Ciphers).
`certconfig`	Manage certificates in PEM format and CRLs and CAs.
`callaheadconfig`	Configure, edit, view and test SMTP Call-Ahead feature.
`smtpauthconfig`	Configure and manage SMTP authentication profiles.
`addresslistconfig`	Configure and manage address lists.
`aliasconfig`	Configure and manage the alias table.
`bvconfig`	Configure bounce verification address tagging.
`domainkeysconfig`	Configure, manage and test tons of DKIM settings.
`quarantineconfig`	Configure and manage system and outbreak quarantines.
`addresslistconfig`	Configure and manage addresslists.
`slblconfig`	Import or export End-User Safelists/Blocklists.
`incomingrelayconfig`	Manage incoming mail relay settings.
`dmarcconfig`	Manage DMARC verification profiles and modify global settings.
`smimeconfig`	Configure S/MIME settings and manage keys.
`localeconfig`	Manage locale modification and enforcement settings.

ESA configuration files

`showconfig`	View XML configuration file as paged output.
`mailconfig`	Send XML configuration file via mail.
`saveconfig`	Save XML configuration file in the `/configuration` directory.
`loadconfig`	Load XML configuration file from the `/configuration` directory or paste it directly into the CLI.
`rollbackconfig`	Roll back to one of the last 10 saved configurations.
`resetconfig`	Reset ALL configurations to factory default.

Managing message queues and mails

`showrecipients`	Show messages from the queue by recipient host name, sender address or all mails in the queue.
`deleterecipients`	Delete messages from the queue by recipient host name, sender address or all mails in the queue.
`bouncerecipients`	Bounce messages from the queue by recipient host name, sender address or all mails in the queue.
`redirectrecipients`	Redirect all mails to a relay host.
`showmessage`	Show a complete message by MID in ASCII.
`archivemessage`	Archive a message by it's MID as mbox file to the /configuration directory.
`removemessage`	Remove a message from work, retry or destination queue.
`oldmessage`	Display Headers and MID of the oldest message in the queue.
`delivernow`	Attempt to deliver pending messages either by domain or simply reschedule all mails.
`unsubscribe`	Manage unsubscribe lists for recipient addresses that will always be bounced or dropped.
`stripheaders`	Strip all headers by name in this table from all mails.
`resetqueue`	Reinitialize queue. DELETES ALL QUEUED MAIL.

Cisco IronPort Support and advanced diagnostics	
supportrequest	Open a support request with Cisco TAC.
supportrequestupdate	Request immediate update of support request keywords.
techsupport	Enable/disable a tunnel for Cisco Support to access the appliance.
diagnostic	Check RAID status, flush DNS/ARP/LDAP caches, test remote SMTP servers, check disk quota and usage or reset configuration.
tarpit	Configure countermeasures and resource conservation mode.
setcorewatch	Configure alert-on-core functionality.
wipedata	Wipe core files from disk and view status from last wipe operation.

Emergency login with user `enablediag` if normal login fails. Same password as "admin".

Working with logs	
grep	Search for a Regular Expression pattern inside a log file.
findevent	Find an event in the logs matching either a message id, a mail address (From: / To:) or a subject. Menu driven or batch mode.
tail	Continuously display new entries from the end of a log file.
rollovernow	Do a rollover on one specific log or simply all log files.
logconfig	Configure and manage log files and delivery methods (FTP, SCP, Syslog). View public RSA/DSS key from users.

Managing security services	
updateconfig	Configure update URLs and HTTP/HTTPS proxies to use. This will also affect AsyncOS updates.
updatenow updatenow force	Manually update all components. Force updating with the option *force*. The *force* option also works with all other update commands.
antispamconfig	Configure IronPort anti-spam and Intelligent Multi-Scan.
antispamupdate	Manually request immediate anti-spam rules update.
antivirusconfig	Configure and view anti-virus settings and scanners.
antivirusupdate	Manually request immediate anti-virus definitions update.
contentscannerupdate	Request immediate content scanner engine update.
scanconfig	Configure scanner options like skipped file types, scanning depth (nesting), maximum scan size, scanner timeout.
verdictcacheconfig	Configure CASE and SPF verdict caching.
outbreakconfig	Enable, disable and configure Outbreak Filters.
outbreakupdate	Request immediate update of CASE rules and engine.
outbreakflush	Clear the current in-memory and disk-cached Outbreak Rules.
encryptionconfig	Configure IronPort PXE mail encryption.
encryptionupdate	Manually request immediate PXE engine update.
dlpupdate	Manually request immediate RSA DLP engine update.
dlprollback	Rollback RSA DLP engine and config to the previous version.
emconfig	Configure RSA Enterprise Manager integration.
emdiagnostic	RSA Enterprise Manager integration diagnostics.
ecconfig	Configure enrollment client used to obtain certificates for URL filtering.
ecupdate	Request immediate update of the enrollment client.
graymailconfig	Configure Graymail Detection and Safe Unsubscribe settings.
graymailupdate	Request manual update of graymail files.
repengupdate	Manually request immediate SBRS engine update.
senderbaseconfig	Configure SenderBase SBNP statistics sharing status.
ampconfig	Configure advanced malware scanning and clear file reputation cache.
websecurityconfig	Configure basic settings for URL filtering. For more advanced configuration use `websecurityadvancedconfig`.
webcacheflush	Flush the URL filtering cache.
urllistconfig	Manage URL whitelists for skipping category and reputation checks.
imageanalysisconfig	Configure the IronPort Image Analysis settings and thresholds.
aggregatorconfig	Set the address of the Cisco Aggregator Server.
slblconfig	Import or export End-User Safelists/Blocklists.
fulldatasharing	Configure SenderBase statistics-sharing with unhashed filename.

AsyncOS management	
updateconfig	Configure update URLs and HTTP/HTTPS proxies to use. This will also affect Anti-Spam and Anti-Virus updates.
upgrade	List all available AsyncOS versions and perform an upgrade.
revert	Revert the appliance to a previously used AsyncOS version. Except network settings ALL configurations and logs will be lost.

Suspending and resuming receiving and/or delivering mails	
workqueue pause	Pause working queue.
workqueue resume	Resume working queue.
suspendlistener	Stop accepting mails on one, several or all listeners.
resumelistener	Resume accepting mails on one, several or all listeners.
suspenddel	Suspend delivering mails.
resumedel	Resume delivering mails.
suspend	Suspend receiving and delivering all mails.
resume	Resume receiving and delivering all mails.

Centralized Management Cluster	
clusterconfig	Create SSH or CSS clusters, add or remove single ESAs to or from a cluster. Create and manage cluster groups. List machines in cluster and view cluster and connection status.
clustercheck	Check configuration databases for inconsistencies and resolve them if necessary.
clusterdiag	Configure cluster diagnostic settings.
_clusterjoin	There is nothing to see here, move on.

Message Filter conditions (Excerpt. See "ESA User Guide" for more info + examples)	
subject	Tests subject against a RegExp.
body-size	Tests size of entire message in bytes.
mail-from	Tests envelope sender against a RegExp.
mail-from-group	Tests envelope sender against LDAP group.
sendergroup	Tests against a HAT sendergroup name.
rcpt-to	Tests envelope recipients against a RegExp.
rcpt-to-group	Tests envelope recipients with LDAP group.
remote-ip	Tests client IP for exact or IP range match.
recv-int or recv-listener	Matches mails received on the named interface/listener.
date	Tests current date against value in US date format: MM/DD/YYYY HH:MM:SS
header(<*string*>)	Tests the given header against a RegExp.
random(<*integer*>)	Compares a random integer to given value.
rcpt-count	Checks recipient count against value.
addr-count()	Compares recipient count from header (To: and/or Cc:) against value.
spf-status	Checks the SPF status.
spf-passed	Checks if SPF verification was successful.
image-verdict	Scans attached images for category match.
workqueue-count	Checks number of mails in the workqueue.
body-contains(<*regexp*>)	Checks mail and attachments for a RegExp.
only-body-contains(<*regexp*>)	Checks message body for a RegExp.
encrypted	Tests if a message is S/MIME or PGP encrypted.
attachment-<trait>	Checks if a attachment matches a characteristic <trait>. <trait> can be `filename`, `size`, `type` (MIME signature), `filetype` (fingerprint) or `mimetype` (MIME header)
attachment-protected	Looks for passworded/encrypted attachments.
attachment-unprotected	Looks for unprotected attachments.
attachment-contains()	Tests attachment for the given pattern.
attachment-binary-contains()	Tests raw binary attachment for pattern.
every-attachment-contains()	Tests every attachment of a message for a given pattern.
attachment-size	Matches attachments by size in B, K or M.
dnslist(<*server*>)	Looks at server for a match in a DNSBL.

Message Filter conditions (Excerpt. See "ESA User Guide" for more info + examples)	
[url-]reputation	Compares sender's SB or a URL reputation to value.
[url-]no-reputation	True when SB rep. is "none" or a URL rep. is unavailable.
url-category	Checks all URLs in a message for the specified category.
dictionary-match(<*dict*>)	Look in body for RegExp match from dictionary <*dict*>.
<position>-dictionary-match(<*dict*>)	Looks in <position> of a message for a RegExp match from the dictionary named <dict>. <position> can be: `subject`, `mail-from`, `rcpt-to`, `attachment`, `body`.
header-dictionary-match(<*dict*>, <*header*>)	Looks in header <*header*> for RegExp match from dictionary named <*dict*>.
smtp-auth-id-matches(<*header*> *[, <sieve-char>]*)	Checks sender in envelope and mail header (From: or Sender:) against the sender's SMTP auth user ID.
true	True is true and therefore matches all mails.
valid	Tests mail for complete MIME validity.
signed	Tests if the message is S/MIME signed.
signed-certificate(<field> [<operator> <regexp>])	Check if the `issuer` or `signer` <field> in the certificate of a S/MIME message matches/does not match (== or != as <operator>) a certain <regexp>.

Message Filter actions (Excerpt. See "ESA User Guide" for more info + examples)	
alt-src-host()	Deliver mail from this named interface.
alt-rcpt-to()	Change all recipients of a message.
alt-mailhost()	Deliver mail via alternate mail host.
notify() notify-copy()	Notify specified recipient about a message (and include a copy of the original message).
bcc() bcc-scan()	Send a copy of this message to a new recipient. Treat the copy like a new mail and scan again.
log-entry()	Add a log message at INFO level to mail logs.
quarantine(<name>)	Send this mail to the named quarantine.
archive(<filename>)	Save copy of the message in mbox format file.
duplicate-quarantine(<name>)	Send copy of this mail to the named quarantine.
strip-header()	Look for a header and remove it.
insert-header()	Insert a header and its value into the mail.
add-footer(<footer>)	Add the footer named <footer> to the mail.
add-heading(<heading>)	Add text resource <heading> as a heading to a message.
bounce-profile()	Apply a bounce profile to the mail.
encrypt-deferred(<profile>)	Encrypt message before final delivery.
tag-message(<name>)	Add tag <name> for RSA DLS policy filtering.
skip-filters()	Skip all remaining message filters.
skip-<scanner>()	Skip all checks of <scanner> for this mail. <scanner> can be `spamcheck`, `marketingcheck`, `socialcheck`, `bulkcheck`, `viruscheck`, `ampcheck`, `vofcheck`.
drop-attachments-by-<trait>()	Drop attachments matching a characteristic *<trait>* which can be `name`, `size`, `type`, `filetype` or `mimetype`.
drop-attachments-where-contains(<regexp>)	Drop attachments that match a Regular Expression. Also matches files in archives and drops whole archive.
drop-attachments-where-dictionary-match(<dict>)	Drop attachments that match a term in the dictionary <dict>.
html-convert()	Strip all HTML tags from a message.
edit-header-text()	Substitute a matched RegExp within a header.
edit-body-text()	Substitute a matched RegExp within a body.
deliver()	Deliver the message. Final action.
drop()	Drop the message. Final action.
bounce()	Bounce the message. Final action.

Message Filter example

```
drop_huge_presentations:
if (mail-from-group == "Sales") AND (attachment-filename ==
"(?i)\\.(ppt|pptx)$") AND (attachment-size >= 10M) {
drop-attachments-where-contains ("(?i)\\.(ppt|pptx)$", "Large presentation
dropped.");
}
```