DCA IMIL Commands – DCA v.20.2.22 and above, Jan 2020

The commands here are selected based on their operational relevance. No attempt has been made to document the full IMIL command set.

Required terms are enclosed in curly braces: `{required_term}`. Optional terms are enclosed in square braces: `[optional_term]` with optional repetitions signified by a trailing ellipsis: `...` Terms with multiple valid choices are separated by a bar: `{this|that}`.

Command	Description	Admin	Examples	Notes
Operational Status				
status	Overall status summary			Includes DCA version, local time and last reboot time, memory and thread stats, XMPP connection settings and message queue size, number of contactable/non-contactable devices.
get host	Host name and address of machine running the DCA, plus licence key code.			
Service Control				
restart service please	Restarts the DCA	Y		
restart discovery please	Restarts the discovery process	Y		Restarts from the first discovery range.
doupdatecheck	Checks for available program updates. If an update is available it will be downloaded and installed in the background.	Y		DCA v.20.2.2 and above.
Device Status				
list devices	Readout of device details			
list counts using {N|serial}	Latest count records for device with ID N or find by serial number		list counts using 3	
list levels using {N|serial}	Latest consumable levels for device ID N or find by serial #		list levels using VNH5312804	
list alerts using {N|serial}	Current alerts for device ID N or find by serial number			
Device Discovery				
getlastds	Details of last device discovery attempt (IP address and time)			
list disc	List of configured discovery scan ranges			

add disc {name},{oct1},{oct2},{oct3},{start_oct4},{end_oct4}	Add a discovery IP address scan range with the given (zone) name and IP address range	Y	add disc office,192,168,1,1,254	

update disc {N} with {n|s|f|r|l}={val}	Update one or more properties of a discovery scan range.
	n=name
	s=start octet 4
	f=end octet 4
	r=run status (R or Y = enabled, F = fast, N = disabled)
	l=SNMP level (0,1,3)
		Y	update disc 3 with f=254,r=F	Use 'list disc' to obtain row index number for {N}
				Since v.20.2.22 SNMP level 0 means auto, 1 means only use SNMPv1, 3 means only use SNMPv3.

delete disc {N}	Delete a discovery scan range	Y		Use 'list disc' to obtain row index number for {N}
list lookups	List point discoveries and their status			Point discoveries (lookups) are active until a device is discovered, after which their status will show as N.
add lookup {name},{host|IP}	Add a point discovery with the given (zone) name	Y	add lookup office,192.168.1.20 add lookup office,hp2.mynet.int	
delete lookup {N}	Deletes a point discovery with the given row number.	Y		Use 'list lookups' to obtain the row number for {N}
Debugging				
list logs [using {filter}[,N]]	Display recent application log entries		list logs using SU – show the last startup and XMPP connection messages. list logs using MU,20 – show the last 20 device monitoring log messages.	This is a limited subset of the information written to the application log files.
list logfile [using {N}]	Display latest content of the application trace log file (i2emfw.log).		list logifile using 10 – show last 10 'pages' of log content.	DCA v.20.2.5 and above.

`get mib using {N|IP} [timeout T] [start|block {OID}] [community {C}] [cred {N}]`	Obtain a MIB walk from a printer.		get mib using 2 timeout 180 – MIB walk for device ID 2 with 3 minute timeout. get mib using 192.168.1.1 – MIB walk for device at arbitrary IP address. get mib using 2 block 1.3.6.1.2.1.43.11.1 – read the prtMarkerSuppliesTable from the MIB for device 2.	Default timeout is 30 secs. If read incomplete at this time the response ends "Read abandoned after exceeding time limit…" May be used as a simple test to confirm if a printer is reachable. start, block and community parameters available from DCA v.20.2.5. cred parameter introduced v.20.2.22; allows specifying an SNMP credential from the creds list to be used for the walk.
`test snmp using {N|IP} [cred {N}]`	Test SNMP connectivity to a device or IP address using all available credentials or a specified credential from the list.		test snmp using 10.1.1.14	Available since v.20.2.22. 'test mib' is an alias for the same command. Use 'list creds' to obtain credential index number for {N}.
Device Editing				
`resend device {N}`	Resend device ID N discovery details to the Portal.			May be used to provide data for "To be identified" device entries at the Portal.
`resend device {N} counts`	Sends latest count records for device ID N to the Portal.			Note: does not query the printer, sends most recent from DB.
`resend device {N} cons`	Sends latest consumable records for device ID N to the Portal.			Note: does not query the printer, sends most recent from DB. May be useful to restore missing data at Portal.
`set mon to {X|Y} for {N}`	Set device ID N monitoring state. X = disabled, Y = enabled	Y		Disable monitoring of a discovered device.
`update device {N} set {ip|mac|serial|hostname|community} [to] {value|null}`	Modifies device identity data fields or SNMP v1/v2 community name	Y		May be used to remotely resolve moves, changes and identity differences, e.g. change of serial number or device move. Setting community available since v.20.2.13.
`reset device {N} [mon|cons|counts|alerts|all]`	Clear selected monitoring data for device ID N.	Y	reset device 3 counts	May be used to resolve an incorrectly diagnosed count model, force a rediscovery of consumables etc. Use with caution, on advice from EKM support.

Alert Handler Settings				
`list ah`	Display the current set of alert class handling options.			Also displays the available classes, manufacturers and handling options with their numeric codes – as needed by the update and delete commands.
`update ah {class},{eoid},{handling}`	Update (or add) an alert handling rule for the given class code and manufacturer number.	Y		
`delete ah {class},{eoid}`	Delete the alert handling rule for the given class code and manufacturer number.	Y		
Settings Parameters				
`get value of {param}`	Displays the current value of a named settings parameter.			

`set value of {param} to {value}`
- *or* -
`set value {param}={value}`
	Updates the value of a named settings parameter.	Y	set value of snmp-community to Private	If {param} does not exist it is automatically created with the given value. There is no ‘delete parameter’ command.

HP JAMC Integration				
`jamcstatus`	Shows current JAMC version, operational state and result of JAMC connectivity test.			
`list jamclogfile [using {N}]`	Display the most recent N pages of content of the JAMC trace log file.			
`restart jamc please`	Restarts the HP JetAdvantage Management Connector Windows service.	Y		Can also be used to restart a crashed JAMC.
`queuejamcupgrade using {V}`	Requests JAMC to upgrade to version V.	Y	queuejamcupgrade using 4.1.3082	
SNMPv3 Configuration **(v.20.2.22 and above)**				
`list creds`	List of configured SNMP credentials.			The credentials list includes both SNMP v1/v2 community names and SNMPv3 security credentials. The DCA tries the credentials in the list in index order when trying to communicate with devices.

`add cred with {param}={value} [,{param}={value}]...`	Add a new SNMP credential to the list. Valid {param} names: `community` – SNMP v1 community name `context` – SNMP v3 context name `username` – v3 username `authpass` – v3 authentication password `privpass` – v3 privacy password `authscheme` – v3 auth hash scheme, MD5 or SHA1 (optional, default MD5) privscheme – v3 encryption scheme, DES or AES (optional, default DES) `index` – list index for the new cred (optional, defaults to end of list) `label` – descriptive label for the cred (optional)		add cred with community=NotPublic add cred with context=Jetdirect,username=snmpv3user,authpass=v3authpass,privpass=v3privpass	Commas in parameter values must to be escaped by preceding them with a backslash (e.g. authpass=m!y**\,**paz!) To unset a value set it to a blank after the equals sign, e.g. ‘context=’
`update cred {N} with {param}={value} [,{param}={value}]...`	Update an existing SNMP credential. For valid {param} names see ‘add cred’ above.		update cred 2 with authpass=newpass, privpass=newpass update cred 3 with index=1 (moves the existing credential at index 3 to index 1, shuffling any existing credentials to make room)	
`delete cred {N}`	Delete an existing SNMP credential from the list.			Use ‘list creds’ to find the index number of the credential to delete.
`update v3creds using {N} with {param}={value} [,{param}={value}]...`	Sets SNMPv3 credentials for an individual device. {param} may be `context`, `username`, `authpass`, `privpass`, `authscheme` or `privscheme`.	Y		From v.20.2.22 the recommended method to manage SNMP credentials is via the ‘add/update cred’ commands.

The DCA has a list of valid XMPP user names from which it will accept admin level commands (marked with Admin Y in the above table). By default this list includes the Portal (through the Monitor IMIL tab) and the additional account name xmppadmin.