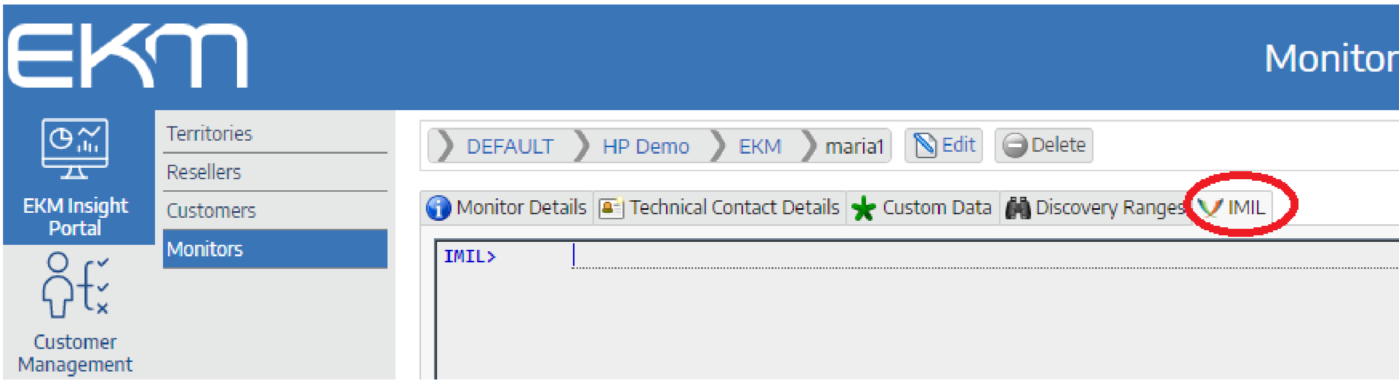
Using SNMP (V3) within EKM Insight – For DCA version 7.21.1.22 and later

EKM Insight has the ability to support and find devices that have been configured to use the SNMP V1/V2 and V3 protocols. Currently access to the SNMP functions is via the IMIL (Insight Management Interface Language) command language. This ensures that only technical staff can configure SNMP settings to reduce issues. SNMP V1 and V2 are defaulted to the community name of 'public'

This document outlines the specific commands used to configure SNMP V3 protocol that can be used alongside the generic commands across all SNMP versions.

IMIL commands are run from a portal using the IMIL tab from the monitor. It is a command level language, please see the IMIL guide for more details of all available commands.

Note: to go straight to a monitor type the monitor name in the search box in the top right of the system



```
IMIL>
```

Since release .22 the DCA uses a list of supplied SNMP credentials to find devices.

The IMIL commands used to work with the SNMP credentials are as follows:

1. `list creds` – This lists both SNMP V1/V2 communities and V3 security credentials

2. `add cred with {param}={value} [, {param}={value}]…` where param may be

`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)

This adds a new SNMP credential to the list.

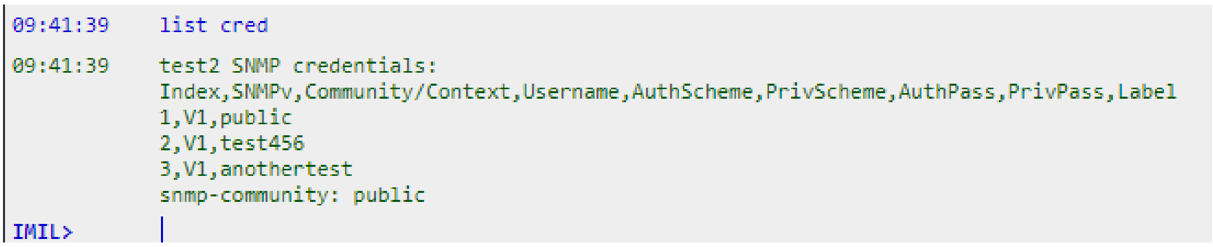
3. `update cred {N} with {param}={value} [, {param}={value}]…`
   Update an existing SNMP credential using the same parameters as above.

4. `delete cred {N}` will delete an existing SNMP credential from the list.

For reference, here is a worked example:

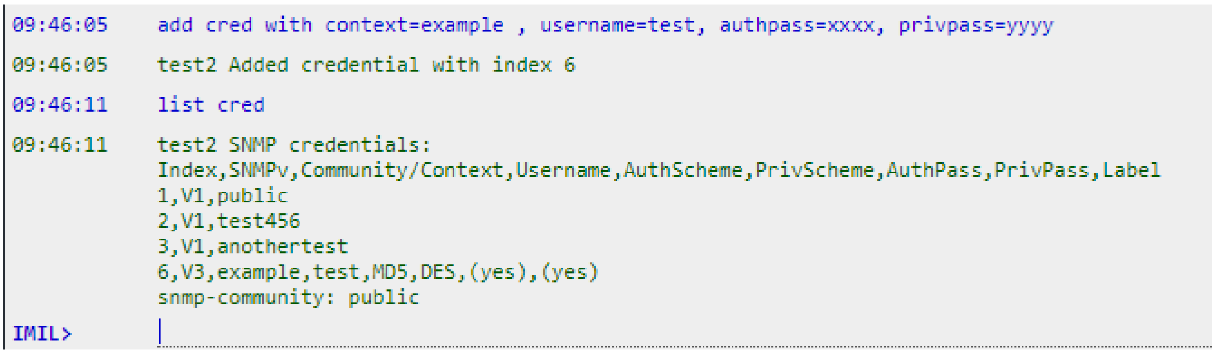
The discovery ranges are added as normal, using the Portal or DCA console or IMIL.

To list the currently set credentials



```
09:41:39    list cred
09:41:39    test2 SNMP credentials:
            Index,SNMPv,Community/Context,Username,AuthScheme,PrivScheme,AuthPass,PrivPass,Label
            1,V1,public
            2,V1,test456
            3,V1,anothertest
            snmp-community: public
IMIL>
```

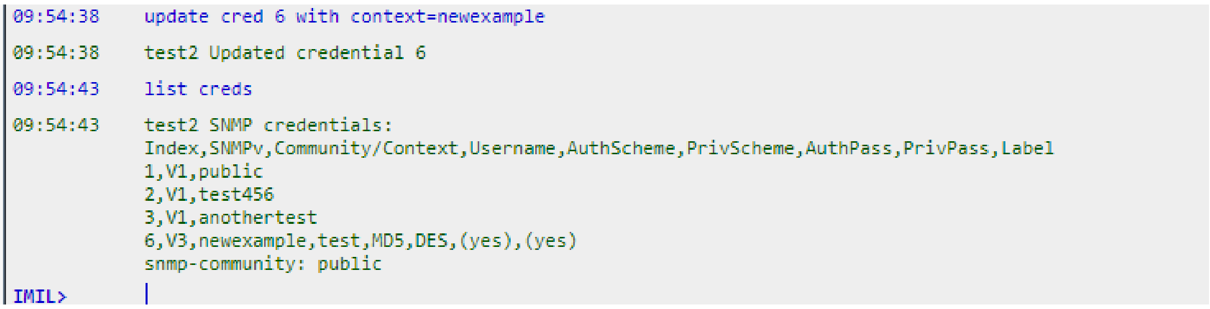
To add an SNMP V3 credential use “add cred”, note we are allowing the AuthScheme and PrivScheme to default to MD5 and DES



```
09:46:05    add cred with context=example , username=test, authpass=xxxx, privpass=yyyy
09:46:05    test2 Added credential with index 6
09:46:11    list cred
09:46:11    test2 SNMP credentials:
            Index,SNMPv,Community/Context,Username,AuthScheme,PrivScheme,AuthPass,PrivPass,Label
            1,V1,public
            2,V1,test456
            3,V1,anothertest
            6,V3,example,test,MD5,DES,(yes),(yes)
            snmp-community: public
IMIL>
```

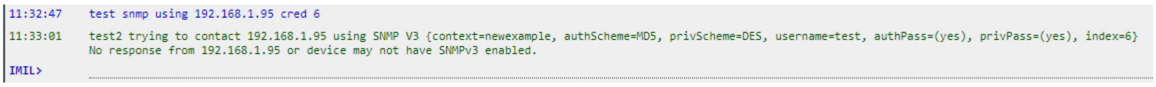
The DCA will now add that SNMP v3 credential to the list of credentials that will be used to find and monitor printers. When looking for printers, each of the credentials are tried in turn in the numbered order shown (1,2,3,6).

You can update the credentials if required using the “update cred” command



```
09:54:38    update cred 6 with context=newexample
09:54:38    test2 Updated credential 6
09:54:43    list creds
09:54:43    test2 SNMP credentials:
            Index,SNMPv,Community/Context,Username,AuthScheme,PrivScheme,AuthPass,PrivPass,Label
            1,V1,public
            2,V1,test456
            3,V1,anothertest
            6,V3,newexample,test,MD5,DES,(yes),(yes)
            snmp-community: public
IMIL>
```

To test straight away if the credentials allow access to a device try an SNMP Test to its IP address:



```
11:32:47    test snmp using 192.168.1.95 cred 6
11:33:01    test2 trying to contact 192.168.1.95 using SNMP V3 {context=newexample, authScheme=MD5, privScheme=DES, username=test, authPass=(yes), privPass=(yes), index=6}
            No response from 192.168.1.95 or device may not have SNMPv3 enabled.
IMIL>
```

Notice the response tells you if it was using SNMPV3 and which credentials were successful. If the test reports that there was no response then either no set of credentials in the list is correct, or the device may not be configured to allow SNMP.

SNMP V3 Context Names

Some vendors use a fixed value for the SNMP V3 context name and do not allow it to be reconfigured; for others it must be left unset (blank). The table below lists the major vendor defaults:

Vendor	V3 Context Name
Brother	(user defined)
Dell	(blank)
Epson	**EPSON**
HP	**Jetdirect**
Konica Minolta	(user defined)
Kyocera	(blank)
Ricoh	**GWNCS**
Lexmark	(blank)
Samsung	(blank)
Sharp	**mfpdirect**
Toshiba	**MFP**
Xerox	(blank)

Note:

HP have confirmed an issue in the JAMC where it is not correctly mixing SNMP credentials configured and supplied by the DCA with any set separately at the Portal for EWS Admin. This issue is still unresolved by HP, so until then we advise customers using SNMPv3 or non-standard SNMP v1/v2 community names to enter these along with EWS Admin credentials at the JAMC itself using its admin page. Alternatively, please contact EKM Support for advice and assistance on alternative approaches.