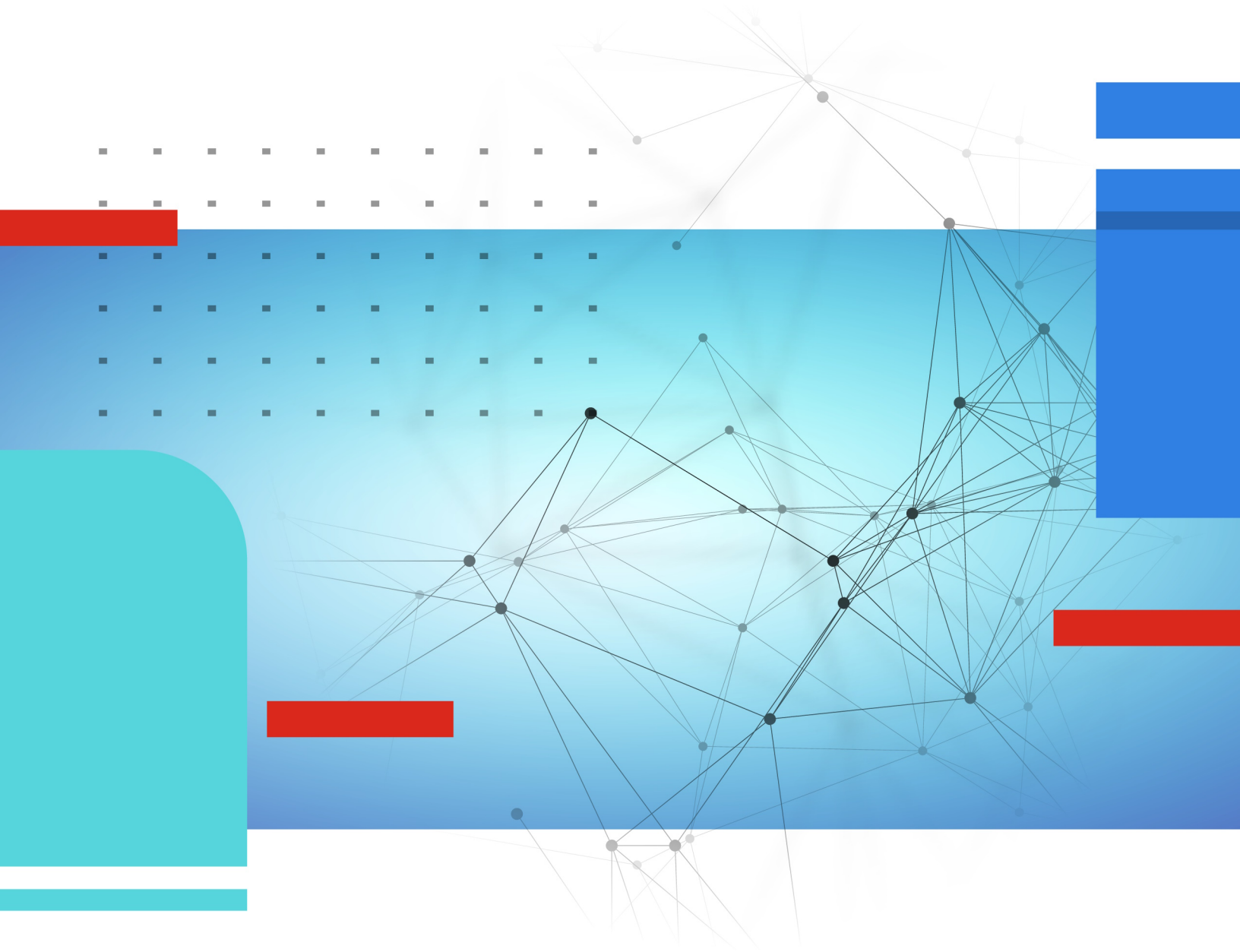
HSM Integration with FortiGate

FortiOS 7.2.8



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2024
FortiOS 7.2.8 HSM Integration with FortiGate
01-728-994917-20241022

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-22	Initial release.

HSM registration and configuration

The feature described in this document is applicable for FortiOS special build 9141 only.

The following steps are used for HSM registration and configuration:

1. Out-of-box registration to obtain a setup password (temporary valid) and HSM information (HSM hostname, partition, slot id, pkcs11-pin etc).
2. Client registration to HSM server. Use the registration tool Ppin to retrieve *.secrets.cfg* (permanent secret) and *primus.cfg* (Primus PKCS#11 configuration). These files are required for the Primus PKCS#11 provider to initialize and establish a connection with the HSM server.
3. Use CLI commands to import *primus.cfg* and configure the secret.

The first two steps are performed off the FortiGate as part of the Primus registration procedure defined by the HSM vendor. The third step is performed on the FortiGate.

To import primus.cfg and configure the secret:

1. Upload primus.cfg through TFTP:

```
# execute nethsm upload-config primus  <config filename> <tftp server>
```

2. Enable HSM feature and configure the HSM server information and secret connectivity:

```
config system nethsm
    set status enable
    set primus-cfg <primus.cfg, escaped>
    set secret-content <.secrets.cfg as base4>
    config partitions
        edit "PRIMUSDEV270"
            set slot-id 1
            set pkcs11-pin PRIMUSDEV
        next
        edit "PRIMUSDEV368"
            set slot-id 0
            set pkcs11-pin PRIMUSDEV
        next
    end
end
```

- This is global level configuration.
- The maximum secret length supported is 3K bytes.
- Multiple HSM partitions are supported. PRIMUSDEV270 and PRIMUSDEV368 refers to the partition name.

CA certificate generation with HSM key

To generate a CA certificate with an HSM key:

1. Generate a certificate signing request (CSR):

   ```
   # execute vpn certificate hsm generate <key-type> <hsm-partition>  <certname> ...
   ```

2. Sign the CSR by the Customer Certificate Authority and import the signed certificate to the FortiGate.
   This certificate will be used as:
   - Intermediate CA certificate, also known as MITM issuing CA.
   - Admin-server certificate for HTTPS administrative access.

Certificate usage

WAD deep inspection in explicit proxy policy

The intermediate CA certificate generated in CA certificate generation with HSM key on page 6 will be configured in deep inspection profiles for MITM domain certificate resigning.

To configure the certificate in deep inspection profiles:

```
config firewall ssl-ssh-profile
    edit "deep-inspection-hsm"
        set caname "<hsm_CA_cert>"
    next
end
config firewall proxy-policy
    edit 1
        set proxy explicit-web
        set ssl-ssh-profile "deep-inspection-hsm"
    next
end
```

FortiGate HTTPs administrative access

This addresses the second use case, requiring the HSM generated certificate for FortiGate GUI login.

To use the certificate for logging in:

```
config system global
    set admin-server-cert "<hsm_CA_cert>"
end
```

CLI details

The following are the CLI and syntax changes implemented for this HSM project:

Sample full configuration of `system nethsm`

```
# show full system nethsm
config system nethsm
    set status enable
    set primus-cfg "version = \"1.0\";
primus:
{
    connect_on_init = true; wait_max_tries = 5;
    wait_delay = 250; hsms:
    {
        hsm0:
        {
            port = \"2410\";
            host = \"82.197.162.10\";
            slots:
            {
                slot0:
                {
                    id = 0;
                    client_id = \"FortiGate00\"; user_name = \"PRIMUSDEV368\";
                };
            };
        };
        hsm1:
        {
            port = \"2411\";
            host = \"82.197.162.10\";
            slots:
            {
                slot0:
                {
                    id = 0;
                    client_id = \"FortiGate01\"; user_name = \"PRIMUSDEV368\"; priority = 1;
                };
            };
        };
        hsm2:
        {
            port = \"2410\";
            host = \"82.197.162.10\";
            slots:
            {
                slot0:
                {
```

```
                    id = 1;
                    client_id = \"FortiGate00\"; user_name = \"PRIMUSDEV270\";
                };
            };
        };
        hsm3:
        {
            port = \"2411\";
            host = \"82.197.162.10\";
            slots:
            {
                slot0:
                {
                    id = 1;
                    client_id = \"FortiGate01\"; user_name = \"PRIMUSDEV270\"; priority = 1;
                };
            };
        };
    };
    log:
    {
        trace_function = true;
        trace_inout = false;
        trace_pid = true;
        trace_timestamp = true;
        file = \"/tmp/primus.log\";
        trace_filename = false;
        trace_linenumber = false;
        trace_mask = 0x01;
        trace_level = 4;
        write_syslog = false;
    };
};
"
set secret-content ENC

J/N1pjaMxGYGK/9ZxY20/jS36vxNWDcQgAdkR7pSUwhLAZvsGZLt2tQhCrcA14TOAYkHHR9Kt3umDfMNol
URWhaPXBJutrrtwsxpps7wiFPybLvh7nZWi8Zr2y/E8Z+9qsdfD11JPEQWSom2l+iHVW2YGsekpv6GehJTGM
XqWDh6ly4BXGBb6NierTkK3pe9tsnZ/DUp0UvJ96qL/i0D23Jv7+9jyq8Pzd4TM6FqScIYLYsBCrwOFm/v9wvj
r+izsdwUKJX7ZY/2XumrjYPHCcdbpnYmPS3+b5d+mCITIB0DFYQJmJyfCYw/8mRqar1MUZVRwzgoqQq6TXJ
vwfNf9ldrLKzmQv2bLTYOKxvzUiF8TZshPMQZcX3xH2KQ2uXLYEBLccxLGat/Md1tlqT7DxoEypgEs1VAQChd
OACJwJdDEYRKsoPt7WCdk6sNBluQ/zx643FrmE/JVx7TZrTMcsSwHj/dB74DFeOOWklhR8uXh4HIRMVTwJ/
N/RnWzNwTws6n08dndgef55JngxJBiOWxjVRpBHFFGFj9lHiVOD2YrRHLykyct3ir1f4KRXtg5pEpLB4eOgQs5
xMgb2XrrYDQ+vBvIZU8/yOcfos6waza7CPVCo4DdSgGD6wMvjmMB4kcf6A6ivP0guFC/BqXLjCNr9cz0DXXB
daLYbnu9aC0G6ThuZZMGri/Lt/iOAG8cQCeBr1vCdUSe7B0WY6HRCitGzAXFuWCHh1ctV6/lnILL7XtAXbdp1
izDFQuBIb/I+iSqRQ7aLUVlqOIK6WeFZg2cm5SuzV06KeN1OaoizU8czgAxy1xp+lJB8vBylpTdxS6qlyBFYVZRn
V8Qk9kzxpM8TIqFs3FR0mJYGBM/i0jx4Jjc+F3nbocckEmTxjYM/1wTZR+7l75UAmJr6Wq+HH2qD2XFiMypd
aa4NWC9iWvgSbrDy+qgxo8dB1cGd2vtSWA7qnLL1vtFOxfXsmk3WRfWHQEdmDr+tLIZdhOSxijkIEScHvJW
PIUzagAflWxldJSEz+wWAlD8Fuuj6bEVi+N4nyckTpc7+POGzc2SHQPFKptvgOshTqHdrJwvTF91PGTcL2vpb8
Gu7/XIpT3PLSs/OS1qpnvN3C3UcBC+RQaACkJEnrPUCO61i+hDpOzGe6vjbjR+XaVQyXD4z8uNLt5rLvjDqJ/X
tEoMWQ0Qm6N3YpBG9/L/HT8CI2Gt4RTpQZLBw684iXQswD70c9k2NM8wCs8xY+IG23gKTq3COG8SuocZO1L63eb1+HYw
Yw8S3fXrx7pmYxJiJCrmTCGSNAwMAGdYOqaU3E+s/bJP1ciJ/lgCjr+vwUH6y+QQ7CKIhl4n
X2p4u2E5CfYAUGjCMUjj3lhP4lqIQMqKy2OvfcVR48UT4dELwST8LGnICLgTJTJ1BiNb2AIHg7jrNfIS2YFO1nl
O9/L3QyIFlc25witEHEOt2vBaRS7AhOvgd8Lo9i7Ki9wtcaSK+4Y0V3/7pA6IIdPTBA+lvhfY4Fjo/RdzyRDCNqu
oHJkgKBTC+y35+4imkYFm7c2UMp3xps8fKPjrBN1VKW11Vm/+tgftKwhGUmyDyiQrK+X+feOM2x0R642R7
3K16TKVL6MpGdJE0Pu+Nmn8FZYOzNad6008yrwCZkTdZRn9sgph4pDYG0Zc+qgs260Y3TsGfOOLrrdZDIV9
```

set secret-content ENC

```
kLUYABsFkQAdEGRYftCQ30A5eqEpMnZLmBuTP0f9wrwf2ZsIZrzAhwmWRZcWslOWe2sSP3JRBhS7GsGAjt
0WWgrGusOipre5rTBtsD6IG3ezqTm5TXP1WtF/TSSXMlvCLfpI1ZcKMfSB6F7HOBskNtIMvx1r0Z2bV8uaTZo
eVoaJNnKEX6Kj7f4RaHkRBhZN/nTLiGNmra6shvJGVh3mxtserv5gxi1CMWSNcHRrwmFFAt9NEArr5DqT2v
UqBBEZ66362uOsbUZAkIk4acqEaS5OoSBusvY9+ozsKVFgc8rrmPSHLVUMoGZmCOIWpM+3c+M8PQd17g
mjNckd7zKXRruHYU7kbyLtPCycYXOCj/qfwYEk8TbRLe9jv6AjSX2LRH5ufwhOUauG9g6WjOh+ijWXn+U1/H
UpU98crSts9FKn1qKtjK0upK6y64IJefYaugBxQA2hCI/xqynCHIKVSTxmbszWjb7W48B57PFhr/Yp2XthgEcyf
w+tYqyowQrmF6n8F1MR9/lXI1xXSKaTwZ58iZOYrKIe2H+0CeLo+U97H69N+a6nRleKBXQhmUTWaNKxtiR
Ae7RXHhgEfwMeZVZdw2wHYlV9xRCxvq/lSXjyBclh69ZL9rLjS5MKwx/ykYb92qHeA4IjZ8Iq4KbAgxq5qbMlq
M4AxuUIYeh8zfFKUEpLhQvoZUM+ch8Bu4cskh/JWdUpiC9WWGpvqqwglY0wI4RZq346jz7H+hkessx12Aa
D+xehIjLAf4lIRgRBiEInk35sicAwbfiipVM9wzSKK7Z6gowwzootdXsFvyOP8ABvB+JwjORoQt94MFekTesn8N
AcnIgcyrm16sLA8BhyT88WjeCKSDeWK9OwtEvyOa1f2uWicLoDHmmi5TAlVtpYEq6dhdUPboIHW54ytoo3r
j0PNiNdnvI2e+QPbsNLFQFy37FInqNiOHqxuyigxDSiBPwGqnRgOejMn487RWiiXrJPHM/Co49euE9az0YCxK
sP9zCi/vvydFiOT9r2mBk7/rHeqqxVpgDOsfv9GMUR1wPAfa5s6udKLzKV1m52k8cUyxEWx8SuD1kKxwrPv5
xEzIUTGFZnQNPlPsswV29tPYLvBaaMEznb1v7TVcgl167TNKqGhV2ySIjKtRvkWYw7gZnubPAP4DuE0zXJAZX
9yDreYq6luv071MZSZq9lbIXErWZIwfF4SBuWH8BAv0xgSnrz8dUO3q1IkJTz8SZGZVVaUiyNcwmrI+Teq7Crc
N7WNIgB5SjqF8Ns64zJm0U+TlGbm6ygVezGMPYZXFr5LnhF/3NZgJiZDuurXZc8nt1oDYhZ8x9b8BapsweYX
NtlTLUFrTrYLOH3E/ZKbt38oha6QjfYt1qzKsUoed6EW6LHf/Sg5lyFQBc2lmuNVhkEogvo9NW1w8LkAk8tWz
1N5aOVpxvxhg2skJJ43tdfXY4sMqXPiWBYOGxcwc1V9FhK4pJad84Af1x82bp4Zbc+mxGrxk1nA4CbAShEyl8
CHw8asmCBXjZ5R3GIFXX+XTQaMSyrL5LOVjHhEAmphuxvAw0iqPNOhU8U7hquGxDVDJhy2ew/ttDrHbeC
1tM3ObjxNdADi7taK8disoJLe9V8FuSZXt5dFeNGw3iyecpea07PhEECmva/R3/IWgFpktCEw/ja5A5esU8Ah8
Qjr627yEuhCCkoF/DLUP4r32GpU6h7F6UMGA8N4S+mxagZOD+J30qOYkun5hvjKmnZwvoRlgNTI9++pkyUj
qi0BnPFcOoCYFq09y4sIF6rxeJIgIIjUxFJUWMlyaMFiPPxURzaK9eYEeWDa/riaBcZc+dK6R1x7011SefWc/Qm
74FZTJw9ObICiNITt4x37XY5bhaKSM+a3at28V9SJXIiTNrv0WO4uGH1kHoa4iH/YYm/Am6Ibg+p8uh+Wvof
ux0JyCH4GcV8p7FlxMVfnRddcPm/PBUAQ7IMvR95Ao/QPVGrYx8fQedOsuEkl0ceZjxRC2oQTP1l0bncCf2bJ
XMCo4CFi+cg88QJWTBF65zG3X0pgBBbPYIkWRMVbDyw3v8tJoLpRPXdBAtCk1eOTqPwjw1M1T9e9Q51b
uN/f44R4E1hYk0okdhjDIMl3A1eUJlcrhMoKlQS4QOJ9NmflsVSTFU2YXeIaszw7qFLRuli068gy6onKbJ42pvw+oI2b
Jcr7q5pxj7XQgwQ3lhhOCXji6IY0nft77ZioEg95MXdbIWqlJ7wNq0KWPMg3Ccq4iDTCEnzPpt6rsomw90ay9a/KQ6ug
ytWq3SHVVw9HBl3RD3wsDCmc9GK5mNBOrAyoS1TtAUgKmb4Y420c1cp/906kvJs9lnoQT2I
wYAdAKNhlad0uvLNk+8/t2wo/2e4Aarf83fqBpyN4Vj3soDE8cwqg/IvUEVVFA4JCcJeqj40BaqDMSN0vv61k
8U0h7WtxAoDh9QW/cEALYe7rw4fbiIiVaMDrC05nRN2b0pgtxPsxmTOHUTOIUFGcEY+vdlX0pghH0WpUuZ
PMMMB5gth40kZv0sXdfTQ+jlzaT3CSTVoxdobKVSG3MF1dj7z+DMy7mfQkBgeJEfenBx7EeO2fTiyvd+QZw
9uXduzzTTeKgC1GNnel8Bx/2sd3WS1T9Xok4w2VI2CuHy0AbIU7JLuriTYp9n7CsyHyy6bGAAclHRrYZVav/oj
Ta40Wk0gpHWdTYgiyVSxFn9hi0/BtwCJnSe/T8BeqyuVZ7a+MfwcZm6IPF5nE2YDUovx9VQ2Ll10IEPzGrK1F
O0qu6LXY/Gh7xmQ94/DuvJqHq3YLPsah0CCcJH8Izof3Hcri4g9AdomptqKjDhUXAx92c88KYR0uGwX+H9CIj
7OY4k3Es+UlHVeaZOhJd1jpJHbKvkXdNlkyYOTfmRN0EkDPw6L9+6J1CDrxn3S2eHSjNW5WBCaDUSuMX8e
X0kVonUp9TY13bgxN9AEL68KlHDd6pNXPL4j5VcEA0CobfFUztc1R0jCkW+TZ8mzvOeUiDmioqF9GEbzeJW
Be2109Px1dggbhz2ucv/X4ULVu8ZNrAFJI4eocfgRRxJvLV90QJ7XqQYMgWGDoi5xG5vIz7qruRzsKx0NfhGjM
eJRFi5+wIxoxbH5auMXwu3yX2+BrdtZQyKtJo/bwJSjhLZaxbUFekAh1qKs1rFeHSisJr++57fClC+6J3FSM01po
sX7hgkcJdjxObuT8Cx9kiXRKESnhQ8xj5wK9uZZjdwFdh39FtatIpLYlWmjJBKzlZ+4wkkKfxXprQjSDUI/wJeOg/
ktjofuQYRRnnELpuMO0Ue2SoLJhAsg1X/dDHH8OlzjbotLuxz+MfW5AiU0V01bmza3Ns3QrZH5ljowdPaBILI
n6FMvACDxjPSYnXuDyK1vh/94ww6E0rbpvq3sEVAX0Q4kilcLpyW/NmXxRVIbQz331opYpa1mVfSwDN7z/
gEypKiIPIhE62G7wxz1pHdltRJeXZY8E636zE06QCSk6dFbrf96CvCtmMgRL6M7/Tdj5WaxnFWWEOX4LxUZ0
BX5MIj3jnqmwTsZM9OZ232LCoru1MknrgKvqZUAaFnxORyVnXooBze9aLlJFY+TREAmHGvQQTqVua4cSPt
77Sr08t2VBSKuZL11oXVtI6agOoMBDmByCg/Vbmno8Z19KpffIxrpxuPb2iXHc12wpS/dLPFSxvZRE+3GcxkK6
18WjKb7kQwVPwId4thJ1iAKTkDFRvgHhNnhgYLJYToUTv/NRtzWFoVFT7Sd73WvQyMVc=
    config partitions
        edit "PRIMUSDEV270"
            set slot-id 1
            set pkcs11-pin ENC
ojXICIGTr2ET1B+YXWYOht/y46o/JoumSOUl6ne9HVU+gySq9gUVWnBVYIzcCsB+Hmc4AtvMqYpMq4c6fw2JckxShzkz
ztIZH047PYuw3vxJM1i0wx2a4299dfbcyDAwrkP5aaf0nMVCIZJs249FFNK4knOlvjfrVWzFL6FJwL
yDe6c9wzJMOM7n/DS9K86XrqhH0A==
        next
        edit "PRIMUSDEV368"
            set slot-id 0
            set pkcs11-pin ENC
```

```
pErCu2Yx5dnJNJNi/OQXl0snz3KOO7ISFUGGZAj6wmsr5UrQDlBq+uIRUACHo3jjE73u8s2THipQymSxufD64
PsVYLUWydXn5yvG+IUNcDyqiic3sDuPzNAa0pPxB/0FsWqkkswqOrI82hvKQoXYUOACIeBmeGpgP68ctvfzB
o/7bhjVcTJ9YLWxen6qrOYsAdyl4w==
        next
    end
end
```

1. The `primus-cfg` is a new setting, and this field is imported from TFTP.
2. `set secret-content` and the entire `config partitions` section are new CLI.

HSM execute CLI

```
# execute nethsm
clear-pkcs-provider-log            Clear logs from /tmp/pkcs11.log, generated by pkcs11.so, the
OpenSSL provider.
clear-primus-log            Clear logs from /tmp/primus.log, generated by libprimusP11.so.
delete-object               Delete Hardware Security Module object(s).
dump-pkcs-provider-log      Dump logs from /tmp/pkcs11.log, generated by pkcs11.so, the
OpenSSL provider.
dump-primus-log                    Dump logs from /tmp/primus.log, generated by libprimusP11.so.
inspect-primus-library-info  Display information about the integrated libprimusP11.so
library.
list-objects                List Hardware Security Module objects.
upload-primus-cfg           Upload nethsm primus.cfg file.
upload-primus-cfg-raw       Upload nethsm primus.cfg file.
```

List all objects/keys on HSM

```
# execute nethsm list-objects <Enter>
PRIMUSDEV270:
    rsa_sub_ca_2       // the object list retrieved from the remote HSM
    rsa_subca_vdom1_jun14
    EC_GLOBAL_VDOM_ENABLED
    ec_subca_vdom1_june21
```

Delete an object on remote HSM

```
# execute nethsm delete-object rsa_sub_ca_2
This will delete any/all HSM objects matching the label. Do you want to continue? (y/n)y
```

Upload primus.cfg through TFTP

Upload the primus.cfg file with validation:

```
# execute nethsm upload-primus-config primus1.cfg 172.18.5.30
```

Alternatively, use the option upload-primus-cfg-raw to upload the primus.cfg. The raw version skips the validation/automatic edit.

```
# execute nethsm upload-primus-cfg-raw primus2.cfg 172.18.5.30
```

Execute commands for library debugs

Dumps the Securosys library logs from /tmp/primus.log

```
# execute nethsm dump-primus-log
2024-09-24 23:17:24.992 - node[3316:3316] - 4 - loadConfig() - Primus API PKCS#11 v2.2.4
2024-09-24 23:17:24.992 - node[3316:3316] - 4 - getSecretsConfigFilenameUnix() -
…
```

Dumps the open-source OpenSSL provider logs from /tmp/pkcs11.log

```
# execute nethsm dump-pkcs-provider-log [../src/provider.c:1438] OSSL_provider_init():
Provided config params:
[../src/provider.c:1448] OSSL_provider_init(): pkcs11-module-path: /lib/libprimusP11.so
…
```

Clear the Securosys library logs from /tmp/primus.log

```
# execute nethsm clear-primus-log
```

Clear the open-source OpenSSL provider logs from /tmp/pkcs11.log

```
# execute nethsm clear-pkcs-provider-log
```

Inspect command for printing vendor information and library version

```
# execute nethsm inspect-primus-library-info
Vendor: Securosys SA
Library Version: 2.2
```

Certificate CLI

```
# execute vpn certificate {ca | crl | ems_ca | hsm | local | remote}
```

Generate RSA certificate

```
# execute vpn certificate hsm generate rsa PRIMUSDEV270 rsacert1 2048 rsacert1.devqa.net ca
bc burnaby devqa top3 xxx@fortinet.com dns:rsacert.devqa.net
```

Generate EC certificate

```
# execute vpn certificate hsm generate ec PRIMUSDEV270 eccert1 secp521r1 ecacert1.devqa.net
ca bc burnaby devqa top3 xxx@fortinet.com dns:ecacert.devqa.net
```

Load a certificate/key-pair from the HSM

```
# execute vpn certificate hsm load-key <key-name>
```

Sample fill configuration of HSM certificate

```
# show full-configuration vpn certificate local rsacert1
config vpn certificate local
    edit "rsacert1"
        set password ENC
1H2wgP97I/jAk7+aR0Sl5zcimpfKbbYKuiDkfcfP7Uh4DEvbppfkcEqYJM0WEonaezl8zALVSYcHOZbQU41wlmvScoEU
7sLNypAXkxz9749IkyIe22WFYTn5jmdLR0ydaagUY6447WirSNfiCckH82kWYkLVWH89Hi3Cngvc0Xn
YuIQWnlI5aYgwvuIXPWvdegfw0w==
        set comments ''
        set private-key "-----BEGIN PKCS#11 PROVIDER URI-----
            …
        -----END PKCS#11 PROVIDER URI-----"    //since the private key resides on the HSM
server, CMDB only stores the private key's reference/URI.
        set certificate "-----BEGIN CERTIFICATE-----
            …
        -----END CERTIFICATE-----"
        set range global set source user
        set source-ip 0.0.0.0
        set enroll-protocol none
        set storage nethsm              // new attribute
        set hsm-slot "PRIMUSDEV270" // new attribute
        set hsm-keytype rsa    // new attribute
    next
end
```

WAD CLI

```
config sys global
    set resigned-pkey-period 100       // resigned cert private key regeneration period in hours
(0 - 600 hours, 0 means static config)
end
config web-proxy global
    set use-dynamic-key enable/disable //disable means using disk stored key-pair for
certificate signing; enable means the key-pair is only saved in RAM. The default value is
disable.
end
```

The setting `use-dynamic-key` is only visible after `resigned-pkey-period` is set.

```
config firewall ssl-ssh-profile
    set resigned-cert-valid-days 10    // resigned cert valid days (0 - 10 days, 0 means keep
```

```
the original
end
```

www.fortinet.com