How to Use the fwm sic_reset Command
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12487
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 September 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Use the fwm sic_reset Command ).
Important Information

How to Use the \texttt{fwm sic_reset} Command

Objective

Supported Versions

Supported OS

Supported Appliances

Before You Start

Related Documentation and Assumed Knowledge

Impact on the Environment and Warnings

Using the \texttt{fwm sic_reset} Command

Completing the Procedure and Verifying
How to Use the fwm sic_reset Command

Objective

This guide explains how to recreate the Certificate Authority using the `fwm sic_reset` command in Security Management server (or Multi-Domain Security Management server).

Check Point recommends to run this procedure as a final step, and only after consulting with Check Point support engineers.

Supported Versions

Any Check Point version

Supported OS

Any OS

Supported Appliances

Any appliance that can be run as a management server.

Check Point HCL (http://www.checkpoint.com/services/techsupport/hcl/index.html).

Before You Start

<table>
<thead>
<tr>
<th>Earlier Product Names</th>
<th>Newer Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider-1</td>
<td>Multi-Domain Security Management</td>
</tr>
<tr>
<td>MDS</td>
<td>Multi-Domain Server</td>
</tr>
<tr>
<td>CMA</td>
<td>Domain Management Server</td>
</tr>
</tbody>
</table>

Related Documentation and Assumed Knowledge

The Internal Certificate Authority (ICA) solution:

The ICA is an integral part of the Check Point product suite. It is located on the management server. It is created during the installation process, when the management server is configured. CPCA is the process responsible for ICA related operations.

The ICA issues certificates for the management server, Security Gateways, users, and other trusted entities (for example: OPSEC applications that are used in the system).
The ICA issues certificates for:

- **SIC** – To enable secure communication for all Check Point operations (policy installation on gateways, logging, console-server connectivity, and so on). SIC certificates are generated automatically during object creation.

- **VPN (or IKE)** – To enable efficient and seamless strong authentication in VPN tunnel creation. IKE certificates are created on the Security Management server through the GUI and on the gateway with CPconfig. They are managed from the **VPN** tab of the object (IPSec VPN must be enabled) in SmartDashboard.

- **Users** – To enable strong authentication between remote access users and gateways. Each certificate issued by the ICA has a defined validity period. Administrators can revoke a specific certificate. For example: when a user leaves the organization.

For more about the Internal Certificate Authority, see the latest version of the Security Management Server administrator guide.

### Impact on the Environment and Warnings

- Throughout this procedure, you delete and recreate the ICA on the management server.
- This procedure deletes all certificates from a management server. All certificates need to be regenerated and redistributed. You must establish SIC again with all gateways managed by this management server.

  Therefore:

  - Consult with Check Point support engineers before recreating the CA.
  - Test this in a controlled lab first.
  - Make sure you have good backup (or even a snapshot) for the management server and that this procedure is done during downtime.

### Using the **fwm sic_reset** Command

**Step1: Remove IKE certificates.**

Remove the IKE certificates, generated by the ICA, before running **fwm sic_reset**. Otherwise, this error message appears after running the command.

```bash
[Expert@cpmodule]# fwm sic_reset
*****************************************************************************
Warning: ********************
This operation will reset the Secure Internal Communication (SIC).
The internal Certificate Authority will be destroyed and Check Point Components will not be able to communicate.
You will have to perform the following operations to enable communication:
1. Re-initialize the internal Certificate Authority (use cpconfig).
2. Restart Check Point Services (cpstart, cpidstart).
3. Reset SIC on each station that is managed by this Security Management Server.
4. Re-establish Trust with each Station that is managed by this Security Management Server.
*****************************************************************************
This operation will stop all Check Point Services (cpstop)
Are you sure you want to reset? (y/n) [n] ? y

*** Checking IKE Certificates ***
There are IKE Certificates that were generated by the Internal Certificate Authority. Please remove them (using the SmartDashboard) so that the internal Certificate Authority can be destroyed.

SIC Reset operation could not be completed
```

There are different ways to remove IKE certificates from a management server:

- If SmartDashboard is available, use the solution explained in: **sk14532**
  (http://supportcontent.checkpoint.com/documentation_download?ID=sk14532)
- Manually remove all IKE certificates from the database.
  a) Open $FWDIR/conf/objects_5_0.C for editing.
  b) Search for :certificates. Make sure that in each instance, it is empty: :certificates (). If it has value (object has an IKE certificate), remove the value.
  c) Save the changes.
- Create a CPinfo file to extract and replace the objects file with the $FWDIR/conf/objects_5_0.C that currently exists on the system. This file can be extracted from CPinfo (if opened with InfoView).

![InfoView screenshot]

This file is generated without IKE certificates, so you can use it to delete the current CA.
  a) Take the new objects_5_0.C file from the CPinfo.
  b) Backup the current one on the management server, under $FWDIR/conf/, and replace it with the new file.

**Step 2: Run the command and delete the CA.**

After all IKE certificates are removed from the management server that the ICA resides on, run fwm sic_reset.

This operation deletes the ICA.
After the command runs successfully, a warning appears.

```
[Expert@cpmodule]$ fwm sic_reset
************************** Warning: **************************
This operation will reset the Secure Internal Communication (SIC).
The internal Certificate Authority will be destroyed and Check Point Components
will not be able to communicate.
You will have to perform the following operations to enable communication:
1. Re-initialise the internal Certificate Authority (use cpconfig).
2. Restart Check Point Services (cpstart, cpidstart).
3. Reset SIC on each Station that is managed by this Security Management Server.
4. Re-establish Trust with each Station that is managed by
   this Security Management Server.
**************************
This operation will stop all Check Point Services (cpstop)
Are you sure you want to reset? (y/n) [n] ? y

*** Checking IKE Certificates ***

*** Stopping services ***
   Local host is not a FireWall-1 module
Advanced Routing Suite is now stopped.
evstop: Stopping product - SmartEvent Correlation Unit
Check Point SmartEvent Correlation Unit stopped.
Stopping SmartReporter...
Stopping the SmartReporter Server.
Stopping the SmartReporter Log Consolodator.
Stopping SmartReporter Database.
Note: Database shutdown takes a few minutes. rmstart will fail while
      shutdown is in progress.
SmartView Monitor: Management stopped
VPR-1/FW-1 stopped
SVN Foundation: cpd stopped
SVN Foundation: cpWatchDog stopped
SVN Foundation: Stopping PostgreSQL Database
SVN Foundation stopped.
cpridstop: cprrid watchdog stopped.
cpuridstop: cprrid stopped.

*** Destroying internal Certificate Authority ***

*** Updating objects database ***

SIC Reset operation completed successfully
```

The management server does not contain a CA now. It cannot perform any secured communication with other Check Point or OPSEC devices.

You can also run the `fwm sic_reset` command on Multi-Domain Security Management environments. It is important to run it on the relevant level.

- **On Domain Management Server:** `# mdserv <cma_ip_or_name>
- **On Multi-Domain Server:** `# mdserv`

For further information, refer to steps 1-2 in sk32491

**Step 3:** Recreate the Internal CA.
To recreate the ICA on a Security Management server:
1. Run: `cpconfig`

   ![cpconfig output]

   **Configuration Options:**
   1. Licenses and contracts
   2. Administrator
   3. GUI Clients
   4. SNMP Extension
   5. Random Pool
   6. Certificate Authority
   7. Certificate's Fingerprint
   8. Disable Advanced Routing
   9. Automatic start of Check Point Products
   10. Exit

2. Select option (6) **Certificate Authority**.
   The ICA name is verified. You are prompted to start the ICA.

   ![Certificate Authority configuration]

   **Enter your choice (1-10) :6**

   **Configuring Certificate Authority...**

   **The Internal CA will now be initialized with the following name: cpmodule**

   **Is it OK (y/n) [y] ? y**

   Initializing the Internal CA...(may take several minutes)
   Internal Certificate Authority created successfully
   Certificate was created successfully
   Certificate Authority initialization ended successfully
   Trying to contact Certificate Authority. It might take a while...
   cpmodule was successfully set to the Internal CA

   **Done**

3. Press `y` and wait for the ICA to start.
4. Run: `# cpstart`

To recreate the ICA on a Domain Management Server:

To recreate the ICA on a Multi-Domain Server:
1. Go to the Multi-domain Server level with: `# mdsenv`
2. Go to the Multi-domain Server configuration program with: `# mdsconfig`
3. Select option 5 **Certificate Authority**, to recreate the CA.
4. Run: `# mdsstart -m`
Completing the Procedure and Verifying

Verify the successful completion of the procedure:

- Make sure all watch-dog processes are up and running with: `# cpwd_admin list` 
- Make sure the CPCA process is up and running with: `# ps -ef | grep cpca` 
- Make sure that option 7 in `cpconfig` produces a fingerprint output.

```
Enter your choice (1-9) : 7

Configuring Certificate's Fingerprint...

The following text is the fingerprint of this Security Management Server:
JADE FADE COOL KNOB HERD GRAY HUCK VETO UN SEAT INN SIT
```

- Make sure the management server has a valid certificate (search for `cp_mgmt` in the **CN** field) with: `# cpca_client lscert -kind SIC -stat Valid`

```
[Expert@cpmodule]# cpca_client lscert -kind SIC -stat Valid
Operation succeeded. rc=0. 4 certs found.

Subject = CN=NTSRVFW1,O=vntrsv66.pck.de.kwhxwn
Status = Valid  Kind = SIC  Serial = 89212  DP = 0

Subject = CN=NTSRVFW2,O=vntrsv66.pck.de.kwhxwn
Status = Valid  Kind = SIC  Serial = 35493  DP = 0

Subject = CN=test_gw,O=vntrsv66.pck.de.kwhxwn
Status = Valid  Kind = SIC  Serial = 79023  DP = 0
Not_Before: Mon Jul 11 09:09:02 2011  Not_After: Sun Jul 10 09:09:02 2016

Subject = CN=cp_mgmt,O=vntrsv66.pck.de.kwhxwn
Status = Valid  Kind = SIC  Serial = 78186  DP = 0
```