2/2/2015

Intel security

SMC with ISC

Version 5.9

Table of Contents

[Installing SMC 2](#_Toc410661422)

[Prerequisite: 2](#_Toc410661423)

[Generating development license for SMC: 2](#_Toc410661424)

[Installation Wizard: 3](#_Toc410661425)

[Enabling SMC API on the Management Server: 7](#_Toc410661426)

[Creating a New API Client Element 7](#_Toc410661427)

[Defining API Client Permissions: 7](#_Toc410661428)

[Enable SSL for SMC: 8](#_Toc410661429)

[Adding MC in ISC of Type SMC: 11](#_Toc410661430)

# Installing SMC

## Prerequisite:

* Windows Operating System
* Administrator privileges for the user who will install SMC
* You need to have a valid SMC license file.

## Generating development license for SMC:

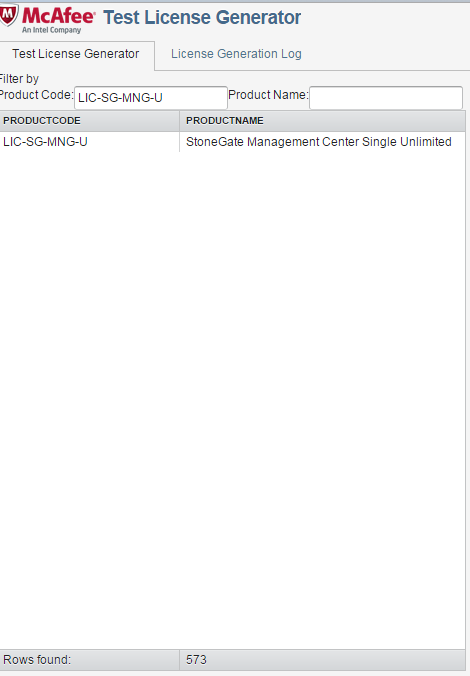
Licenses can be generated at <https://ngfwlicenses-management.corp.nai.org/tlg/>. This is a new link, and the product codes are new. These have been tested and work, but they may have different licensed feature than the previous ones. You may need to use different codes, depending on what you are trying to do.

First of all, if you're using IE for this, add the site to the Trusted Internet sites lists (Tools > Internet Options, Security tab). IE will not let you download a .jar for a site otherwise.

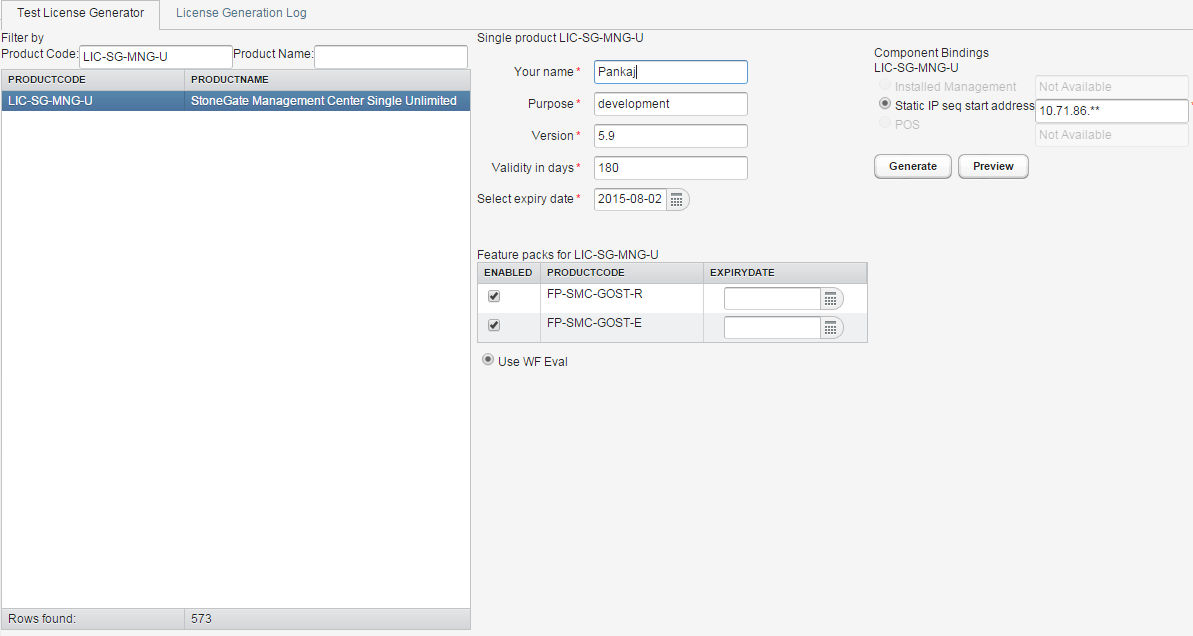
First, generate a license for your SMC. Enter Product Code L-SG-SMC-U, hit return, and select L-SG-SMC-U. Fill out the starred items in the middle, using 6.0 for the version. In the binding section on the right, click "Static IP seq start address" for L-SG-SMC-U and enter the IP address of the SMC. If this is also a log server (the usual case), do the same for SM1CKE-LOG. Then click Generate to create a .jar file containing both licenses. Download this to your SMC and install the license, or install the license when web-starting the client in the following step.

To generate firewall licenses, you need the Proof of License value from the installed SMC license (Administration->License->All Licenses; Then click on Management Server). Then, enter product code L-NGN-EVAL-R. Fill out the starred items in the middle, using 6.0 for the version. In the binding section on the right, click "Installed Management" and enter the Proof of License. Then click generate. You can click generate multiple times if you need multiple firewall licenses; you will create a separate .jar file for each.

* Go to 🡺 <https://intratools.stonesoft.com/tlg/> using a browser
* Type “**L-SG-SMC-U**” (for SMC) in the product code text field and press enter. Select the following row
* Repeat same for the FW using “**L-NGN-EVAL-R**”



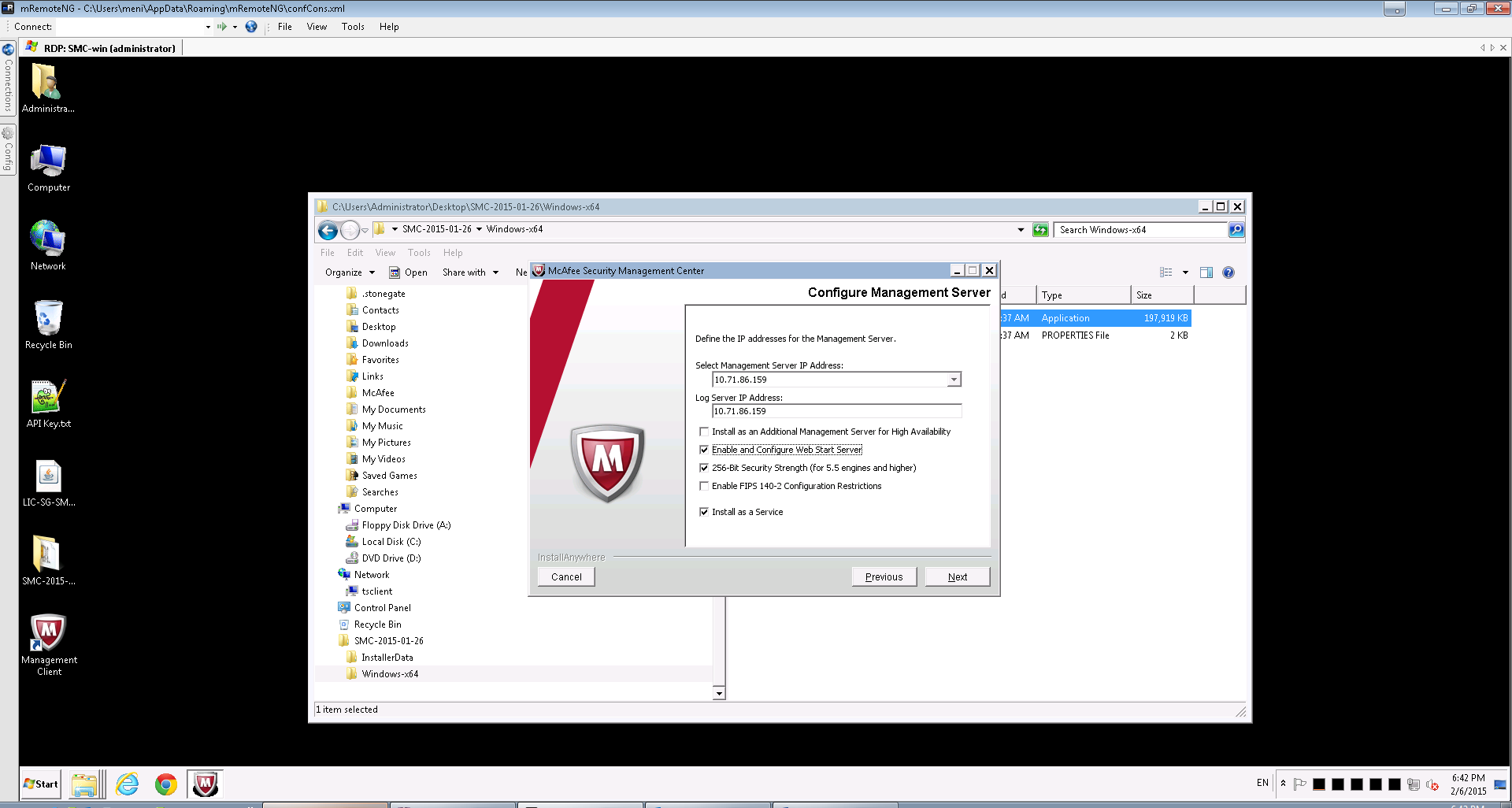
* Once selected you will see a form on the right hand side of the window. Fill the information as displayed in given screen shot.



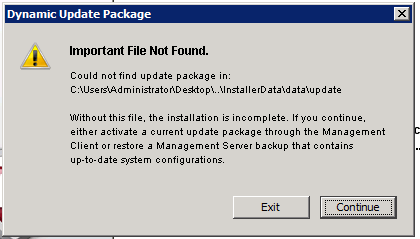
* Click generate – This will give you a license file which will be used during the SMC installation.

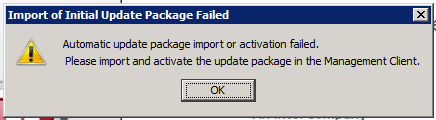
## Installation Wizard:

1. Download setup.exe from:
   1. <http://ssm-stp.scur.com/sdn_build/SMC/20150126/>
   2. <http://ssm-stp.scur.com/sdn_build/engine/20150126/>
2. Double click setup.exe:
   1. Select all **default options** throughout installation wizard.
   2. Ensure to check both Web Start and 256-Bit options.



* 1. Enter username and password when asked for the management
  2. If you encounter the following just click ok/continue.

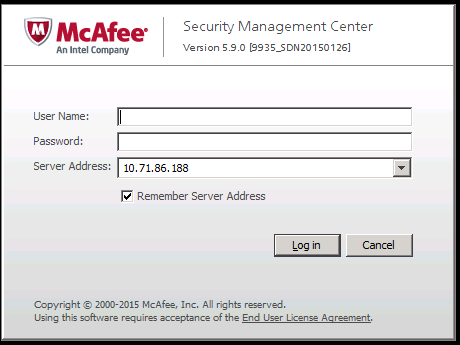




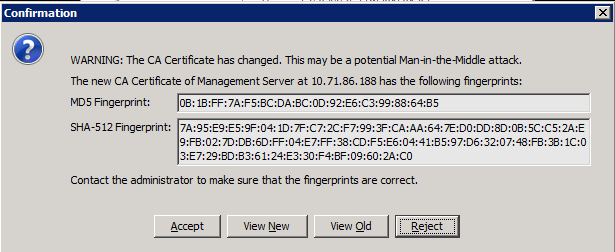
1. Once installation is successful verify the following services are there and are running:



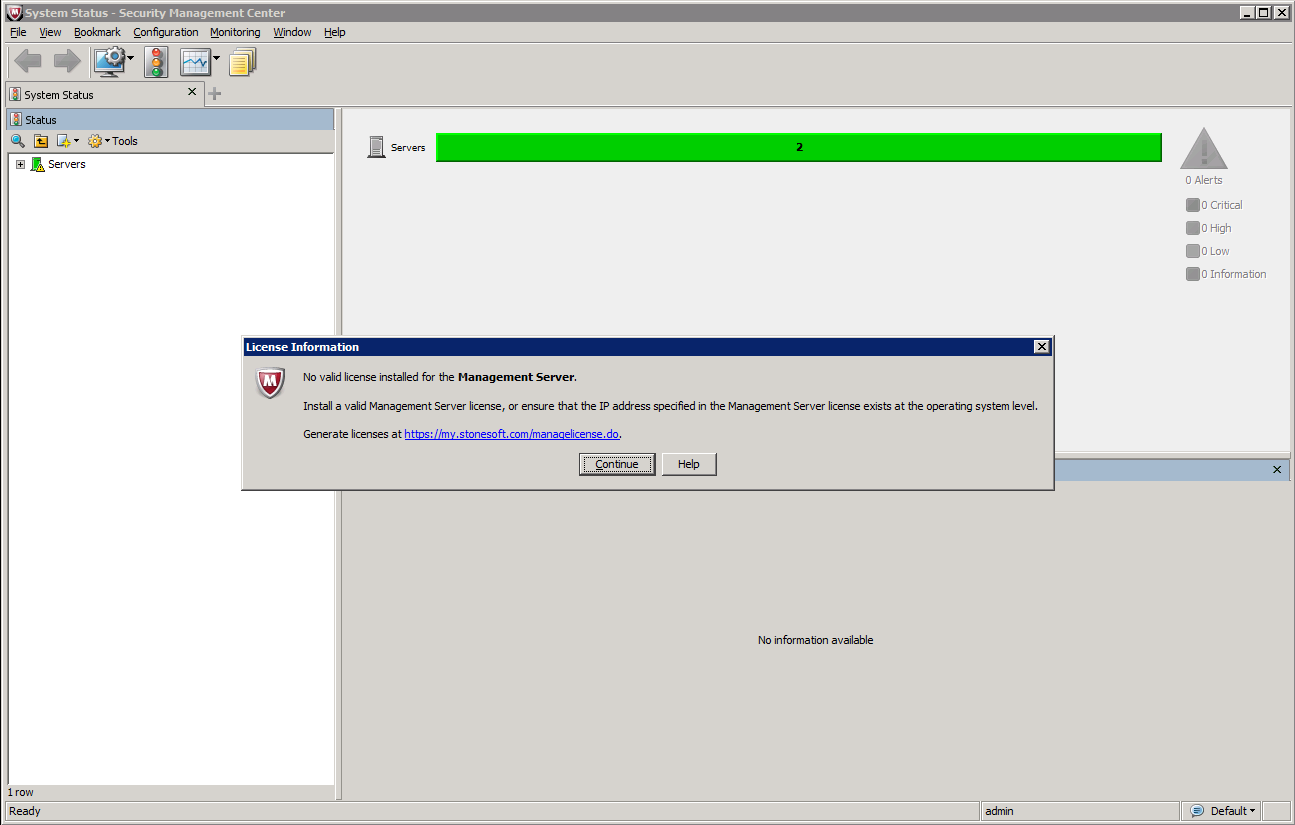
1. Now click Management Client icon from your start menu:
   1. Login using username/password provided during installation.



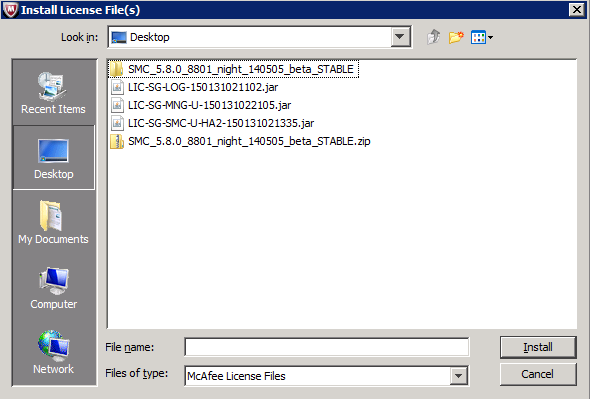
* 1. Accept certificate



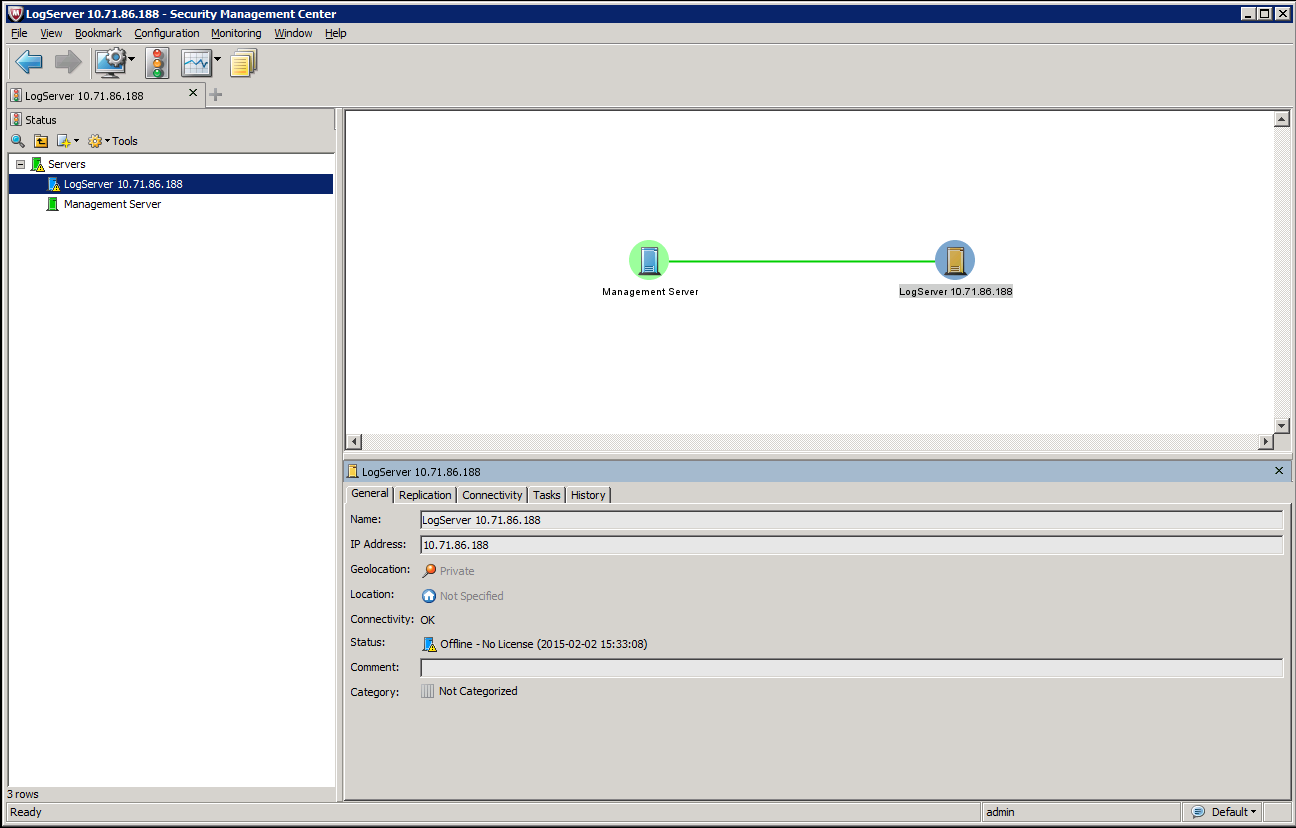
* 1. Click Continue:



* 1. Select license file:



* 1. Once the license is installed Installation is completed and upon clicking this icon you should see like this:
  2. Import FW license the same way and once appliances are deployed, you’ll need to bind the deployed virtual engines.



# Enabling SMC API on the Management Server:

* Right-click the Management Server and select **Properties**. The Management Server Properties dialog opens.
* Switch to the **SMC API** tab.
* Select **Enable** to activate the SMC API.
* (*Optional*) Enter the **Host Name** that the SMC API service uses.
* (*Optional*) Change the (TCP) **Port Number** that the SMC API service listens to.
  + By default, port 8082 is used.
  + In Linux the value of this parameter must always be higher than 1024.
* (*Optional*) If the Management Server has several addresses and you want to restrict access to one address, specify the IP address to use in the **Listen Only on Address** field.
* (*Optional*) Click **Select** and select an existing Server Credentials element or create a new Server Credentials element.
* (*Optional*) Select **Use SSL for Session ID** to track sessions to the Management Server in your application. Do not select the option if your network requires you to use cookies or URLs for session tracking.
* Click **OK**.

# Creating a New API Client Element

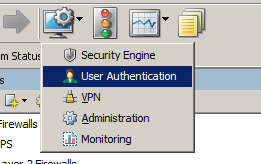
* Select **Configuration→Configuration→Administration**. The Administration Configuration view opens.
* Right-click **Access Rights** and select **New→API Client**. The API Client Properties dialog opens.
* Give the API Client a unique **Name**. (i.e. isc-api-client)
* (*Optional*) Click **Generate Authentication Key** to generate a new Authentication Key. A random 24-digit alphanumeric authentication key is automatically generated.
  + The API Client uses the authentication key to log in to the SMC API.

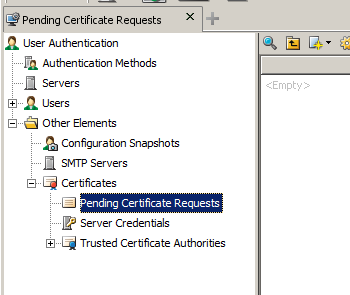
# Defining API Client Permissions:

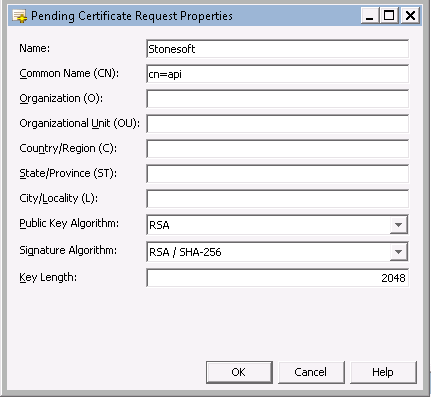
* Switch to the **Permissions** tab in the API Client element’s properties.
* Select one of the following options:
  + **Unrestricted Permissions (Superuser)**: The API Client can manage all elements and perform all actions without any restrictions.
  + **Restricted Permissions**: The API Client has a limited set of rights that apply only to the elements granted to the administrator.

# Enable SSL for SMC:

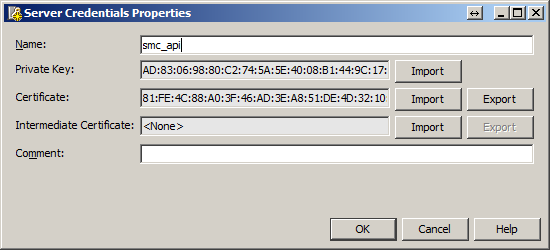
* Go to:



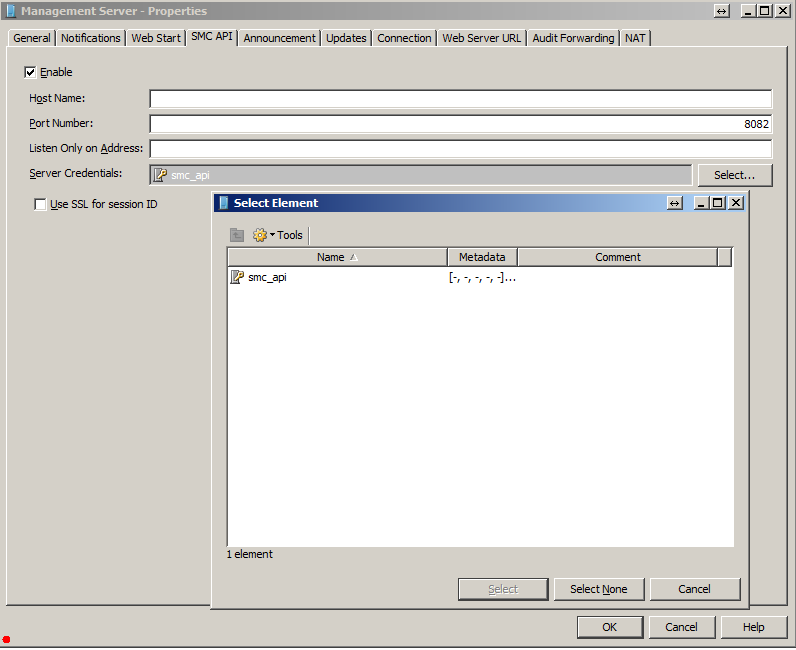




* Right click on the created element -> Self-sign:



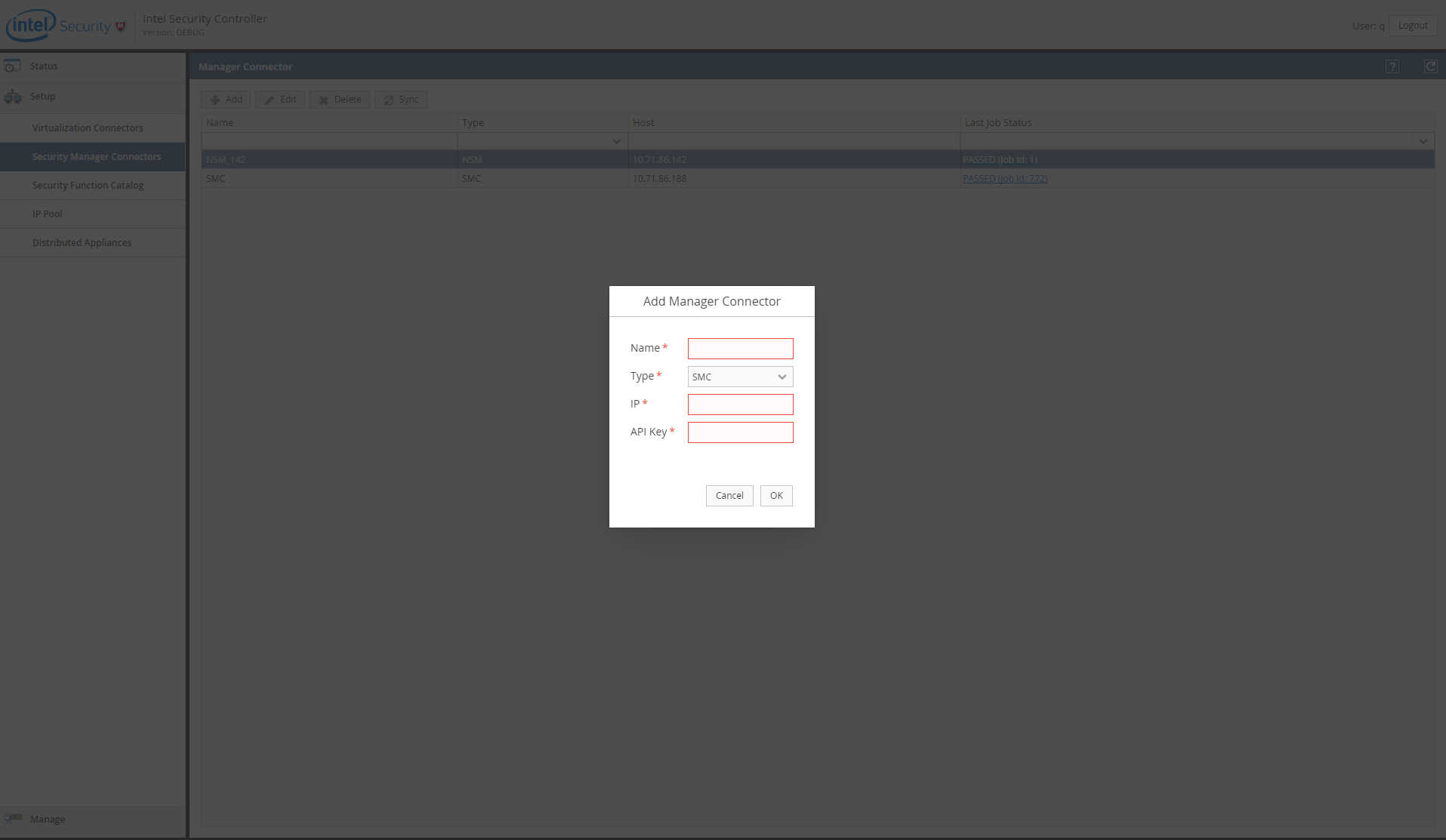
* You could select remove the request, to obtain in User Authentication -> Other Elements -> Certificates -> Server Credentials
* The smc\_api server credentials.
* Now from the mgt server properties:



* It is recommended to restart the mgt server after these changes.
* After these changes, you need to use https instead of http in your REST calls.
* e.g <https://localhost:8082/api> instead of <http://localhost:8082/api> and so all your traffic will be of course encrypted.

# Adding MC in ISC of Type SMC:

* Goto 🡪 Security Manager Connector tab and click ADD:



* Provide
  + Name
  + IP of the SMC we just installed
  + API key we created during API user creation.
* Click ok will trigger a new job.
* If the information is correct and no connectivity issue ISC should be able to sync Policies from SMC installation.