Oskar Louko

Zero-Touch Deployment of Fortinet Devices

Metropolia University of Applied Sciences
Bachelor of Engineering
Information and Communication Technology
Bachelor’s Thesis
29 April 2021

Abstract

Author:	Oskar Louko
Title:	Zero-Touch Deployment of Fortinet Devices
Number of Pages:	16 pages
Date:	29 April 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Networks and Cloud Services
Supervisors:	Janne Salonen, Head of School (School of ICT) Antti Koskenvoima, Manager, Networking Services

The purpose of this project was to explore whether it is feasible to create a zero-touch deployment system, which can be used on new device deployments for customers.

Zero-Touch deployment in this case means that the device can fetch its configuration from the controller, without the need for the customer to do anything else than connect the device to their company network.

This thesis was commissioned by the company Tietokeskus Finland Oy, which is an IT service company that provides IT solutions for various companies in the private and public sectors.

This thesis presents a project in which zero-touch deployment was configured. In addition, the thesis advises how to configure zero-touch deployment with Fortinet products. The configurations for this project were implemented with Fortinet FortiManager, and the test device used was a FortiWiFi 40F-3G4G.

In conclusion, this project was a success. While true zero-touch deployment was not achieved, a method of deployment was achieved, in which minimal end user configuring of devices is required.

Keywords: Fortinet, Fortigate

Tiivistelmä

Tekijä:	Oskar Louko
Otsikko:	Zero-Touch Deployment of Fortinet Devices
Sivumäärä:	16 sivua
Aika:	29.4.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Information and Communication Technologies
Ammatillinen pääaine:	Networks and Cloud Services
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen Verkkopalveluiden Esimies Antti Koskenvoima

Tämän projektin tarkoituksena oli tutkia, onko zero-touch-käyttöönottoympäristö varteenotettava vaihtoehto, kun tuodaan uusia laitteita ympäristöön.

Tässä tapauksessa zero-touch-käyttöönotto tarkoittaa sitä, että laite pystyy noutamaan konfiguraationsa kontrollerilta ilman, että käyttäjän tarvitsee tehdä mitään muuta kuin kytkeä laite heidän yrityksensä verkkoon.

Tämä opinnäytetyö tehtiin Tietokeskus Finland Oy:lle. Tietokeskus Finland Oy on suomalainen IT-alan yritys, joka tuottaa IT-palveluita niin julkiselle kuin yksityiselle sektorille.

Tässä opinnäytetyössä kuvataan projektia, jossa zero-touch-käyttöönotto konfiguroidaan sekä esitellään, kuinka zero-touch-käyttöönotto luodaan Fortinetin tuotteilla. Ympäristön ja laitteen konfiguraatiot toteutettiin FortiManager-järjestelmällä. Testilaitteena toimi FortiWiFi 40F-3G4G.

Lopputuloksena projekti oli onnistunut. Vaikka täydelliseen zero-touch-käyttöönottoon ei päästykään, niin loppujen lopuksi saatiin luotua käyttöönottojärjestelmä, jossa loppukäyttäjän tarvitsee tehdä mahdollisimman vähän konfigurointia laitteille.

Avainsanat: Fortinet, Fortigate

Contents

List of Abbreviations

ADOM	Fortimanager Administrative Domain
CLI	Command Line Interface
FMG	FortiManager
GUI	Graphical User Interface
IPv4	Internet Protocol version 4
Interface	Network Interface
LAN	Local Area Network
NTP	Network Time Protocol
SaaS	Software as a Service

Preface

This project was commissioned by Tietokeskus Finland Oy. I would like to thank the supervisor of this project, Antti Koskenvoima, for the possibility of carrying out this project and writing this thesis. I would also like to thank Antti for the advice he gave me and the time he used on my project.

I would like to also thank my thesis supervisor, Janne Salonen, for all the support he gave me with my thesis, and Ulla Paatola for proofreading the thesis.

Lastly, I would like to thank my friends and family, who have supported me in my studies and my thesis project. This project was carried out in the Helsinki office of Tietokeskus Oy, the user services department.

In Espoo, April 2021

Oskar Louko

1 Introduction

In the modern age, when both companies, and individuals are more connected to the internet than ever, it is necessary to make the deployment of new networking devices as seamless as possible. As such zero-touch deployment is becoming more necessary than ever, as it answers the challenge posed by the ever-growing need for faster and more secure networking.

The aim of this thesis was to examine and to analyze a zero-touch deployment project, how it benefits the commissioning company, Tietokeskus, and their customers.

The objective of this project was to investigate whether it is possible to deploy Fortinet devices to customers without the need for the customer to do anything else than to connect the device to the company network. This was deemed necessary because the current way of doing device deployments is not as efficient as it could be, and there is a greater possibility for human mistakes than with a zero-touch deployment system.

The project was conducted by using a test device, in this case a FORTINET FortiWiFi 40F-3G4G and the FortiManager Central Management system. FortiWiFi is an SD-WAN system, which was only used as a proof-of-concept device for this project. The same methods that were used in this project can be applied to other devices produced by Fortinet.

2 Tietokeskus

Tietokeskus Finland Oy is a Finland-based IT services company, which was founded in 1989. Tietokeskus provides IT solutions, ranging from workstation support and sale of service devices to cloud-based solutions. Tietokeskus provides these services mainly for small to medium-sized companies and to the public sector in Finland. [1]

There are approximately 300 employees at Tietokeskus, and they have local support available in 11 different cities in Finland. [1]

3 Why Fortinet

The project came from the need to develop a system which would be used to deploy new devices to the customers of Tietokeskus, as the current system was seen as hard to work with. It also required people from multiple departments, and it was prone to human mistakes. Thus, it did not serve Tietokeskus nor their customers in the best possible way. At Tietokeskus, there was a need for a more straightforward system, which would also be easier to deploy and manage, than what had previously been used. The old system was hard to work with when it came to new deployments, as sometimes there needed to be multiple people involved for a singular device deployment. As such Tietokeskus started looking into alternatives when it comes to firewalls, SD-WAN systems, and central management systems.

Tietokeskus started looking into different options, which would answer the demand for a way of deploying devices, which in turn would simplify deployments. The company was also interested in the ease of management of new devices from the company’s and the customers’ perspective. After an assessment was made of the advantages and disadvantages of different companies' products, when it comes to cost, ease of use and management, Fortinet’s products were chosen, as they offer an easy-to-use deployment and management system, and up-to-date, modern devices, which could easily be managed by the Fortimanager management system. These requirements can be seen from figure 1.

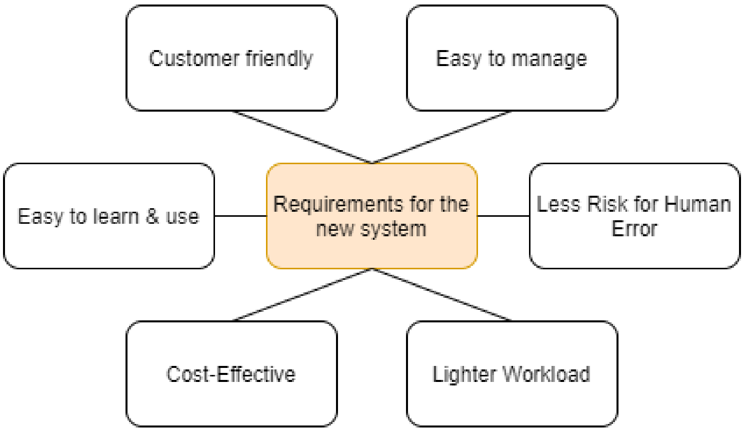


Figure 1: Requirements for the new system

4 Devices Used

The devices used in this project were FortiManager and FortiWiFi 40F-3G4G. In this project, Fortimanager was used for the centralized management and configuration of the test device. Most of the testing and configuration in this project was done in the FortiManager GUI.

FortiWiFi 40F-3G4G was the test device that was used to determine whether the configured model device in FortiManager was working properly, and that connection could be made successfully.

4.1 FortiManager

Fortimanager is a device, with which it is possible to control devices manufactured by Fortinet from a centralized location. There are multiple uses for Fortimanager; for example, it is used to configure devices, make changes to firewall rules, and to create firewall rules.

Fortinet’s devices can also be connected to FortiManager through the public internet, and therefore connecting new devices is quick and easy.

Fortimanager can be run from a physical device, such as the one shown in Figure 2, from a virtual machine, or as a cloud-based service.

Figure 2: FortiManager 200G. Copied from Avfirewalls website [2].

4.2 FortiWiFi 40F-3G4G

The FortiWiFi 40F-3G4G is an SD-WAN device, which doubles as a firewall and networking appliance. It is designed for medium to large-sized companies. As a fail-safe, in case of the wired connection crashing, it also has a 3G/4G/LTE cellular modem built into it.

Figure 3: FortiWiFi 40F-3G4G

5 Project Start

Before starting work on the project, reviews were made on what different methods could be utilized with Fortinet's products when it comes to zero-touch-deployment.

The research was done by getting acquainted with Fortinet's documentation which they offer on their website [3], the internal documentation of Tietokeskus [4], experimenting within FortiManager, and a short demo provided by Fortinet.

Quite early into research it was found out that there were three options for zero-touch deployment, of which two were viable. These three options were zero-touch deployment by using the serial number of the device, zero-touch deployment by using a pre-shared key or using FortiDeploy. The use of FortiDeploy was ruled out, due to the requirement of factory reset, and usage of FortiGateCloud when using this method. [5.]

After this testing of the serial-number method, the pre-shared key method started, as both were deemed viable options for this project. As testing progressed, it quickly became clear that the serial-number method was more viable of these two, even though both work almost exactly in the same way. This was due to fewer configuration requirements for the devices themselves on the customers' end. With the serial-number method there was less of a risk of human error, and as such this method would take priority in testing.

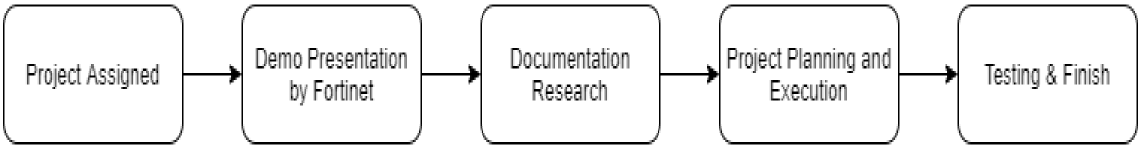


Figure 4: Process of the project

6 Device Deployment

In the old model, which had been in use for years, most of the work was done manually, when it comes to device configurations and device deployments. For example, the old configurations needed to be extracted from the device to be replaced, and then modified and run into the new device to be deployed.

When Fortinet's devices were starting to be used, most of the work was still done manually, per-device basis. It was acknowledged that this method of deploying devices could be improved, and thus work was begun to look for a more efficient way of deployment.

It was decided that efforts should be made to investigate whether a zero-touch solution was a viable method for the deployment of Fortinet’s devices. Thus, the project was assigned to me, and work began on finding the best method of zero-touch deployment, and how this could be done.

6.1 Old Model

Before Fortinet’s devices were used, the deployment of the devices was mostly manual work, and almost all configurations needed to be entered to the devices by hand, or the configurations needed to be copied from an existing device, and then modified by hand for them to work in the new device. This method of device configuration was prone to human error.

For example, when a Juniper SRX100 model was deployed to customers, it was done in the way described above: the old device was taken, the configuration from the old device was copied, parts of the configuration which can be used to in the new device, were copied over to the new device, and the modified configuration was deployed to the new device.

Problems also arose when there were multiple different models of the same vendor’s device on the network, such as Juniper SRX100 and Juniper SRX300. There are major differences between these two models, when it comes to the configuration of routing and interfaces, and if the old configuration is used from the older model, even when modified, it can cause unexpected issues with the device.

In addition to the possible issues mentioned above, the firmware of the device needed to be updated by hand prior to delivery, usually by downloading the new version of the firmware from the vendor portal of the said device, after which it was necessary to move the update files to a USB stick and flash the update from USB. Management connections and configuration backups also needed to be done by hand, and monitoring of the device needed to be done manually.

When all the updates and pre-configurations were finished for the device, and time came to deploy the device to a customer, there needed to be someone locally present on the customer’s premises, as well as and a specialist available in order to deploy the device. This caused a major bottleneck when it came to deploying devices to customers, and there was a need for a more efficient way of device deployment.

6.2 Current Deployment of Fortinet-Devices

The challenges mentioned have, however, been alleviated by the current deployment of the Fortinet devices. Currently, when a customer orders a Fortinet device from Tietokeskus, the device is ordered to the selected office closest to the customer, and then a specialist starts configuring it by hand using a console cable. At the moment, there is a need to configure the interfaces for the public network and LAN, the DNS settings, the DHCP settings, if applicable to the customer’s network, and to configure the NTP. The specialist who is configuring the device also needs to allow Tietokeskus to monitor the SNMP-traffic and to configure the logging to the appropriate level. [4]

All of this is a lot of work, and it was decided that this would be best done by pushing the configurations from FortiManager to the devices automatically, for example by using a template on a per-customer basis, as this minimizes the risk of human error in the configurations of the devices which get sent to customers.

6.3 Zero-Touch Deployment

In this section, different methods of achieving zero-touch deployment are highlighted in more detail. The methods which will be covered are deployment with serial number, deployment with pre-shared key and deployment with FortiDeploy.

6.3.1 With Serial Number

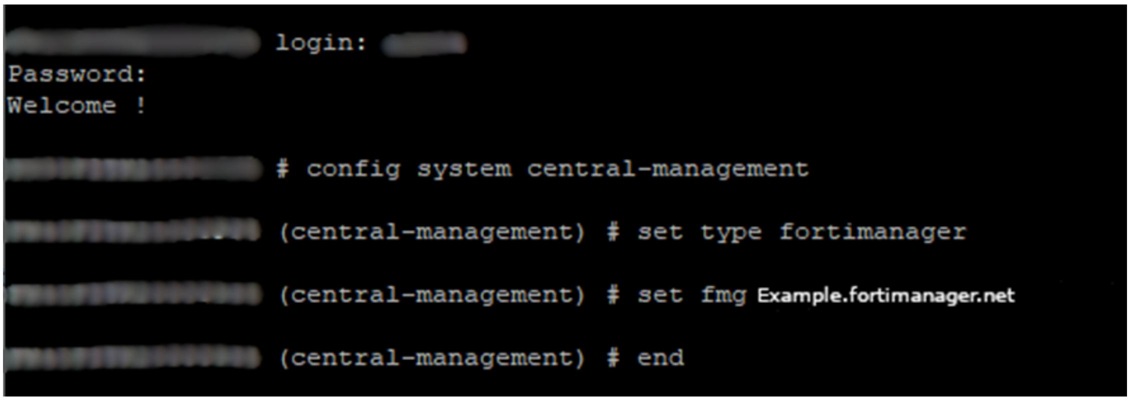
Because of the challenges presented in the previous sections, Tietokeskus started looking into whether zero-touch deployment was a feasible option for the deployment of the devices sent to the customers.

Zero-touch deployment would save the time previously used for configuring the devices for other necessary work, and would be more cost effective for the customers, since a technician does not necessarily need to go to the customers office and install the device, thus saving the customer money in installation costs.

The risk for errors with the configurations is also mitigated by this method of deployment, as the configurations could be peer-reviewed by other experts before deployment of the devices to the customers.

Other benefits include the ease of use for the customer; they only need to input a few lines of commands to the Fortinet device via a console cable, and they do not necessarily need a technician to their office, when the time for deploying the device comes, which saves the customer money and time.

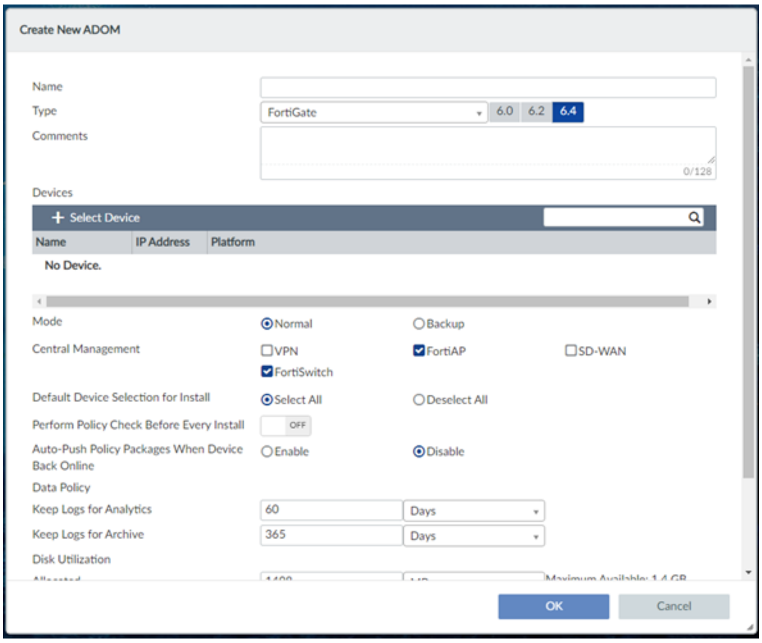
Figure 5 shows the basic configuration that the customer needs to do for the device to connect to the FortiManager.



```
[redacted] login: [redacted]
Password:
Welcome !

[redacted] # config system central-management

[redacted] (central-management) # set type fortimanager

[redacted] (central-management) # set fmg Example.fortimanager.net

[redacted] (central-management) # end
```

Figure 5: Example of end-user commands to Fortinet device

The FortiManager side of configuration is also simple. Once logged in to the FortiManager, a new ADOM needs to be created. ADOM stands for an Administrative Domain, which is used to separate logical environments, for example Customer1 and Customer 2, which makes it possible to maintain separate sets of Fortinet devices.



Create New ADOM

Name
Type: FortiGate | 6.0 | 6.2 | 6.4
Comments: 0/128

Devices
+ Select Device

Name	IP Address	Platform
No Device.		

Mode: ● Normal ○ Backup
Central Management: □ VPN ☑ FortiAP □ SD-WAN ☑ FortiSwitch
Default Device Selection for Install: ● Select All ○ Deselect All
Perform Policy Check Before Every Install: OFF
Auto-Push Policy Packages When Device Back Online: ○ Enable ● Disable
Data Policy
Keep Logs for Analytics: 60 Days
Keep Logs for Archive: 365 Days
Disk Utilization
Allocated: 1400 MB Maximum Available: 1.4 GB

Figure 6: Interface for creating a new ADOM

Once the ADOM is created, a model device needs to be configured. To do this, the Device Manager needs to be selected from the GUI, which opens after opening the ADOM. The GUI can be seen in Figure 7.

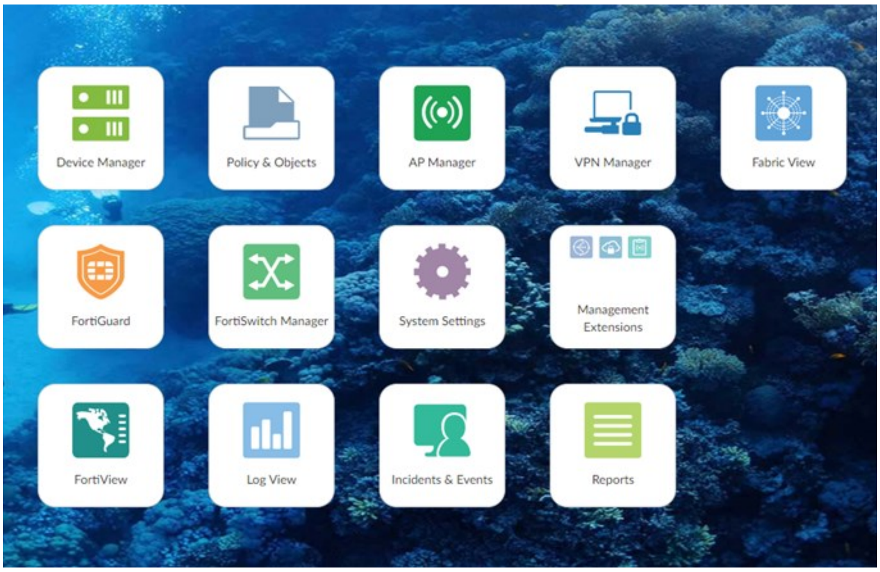
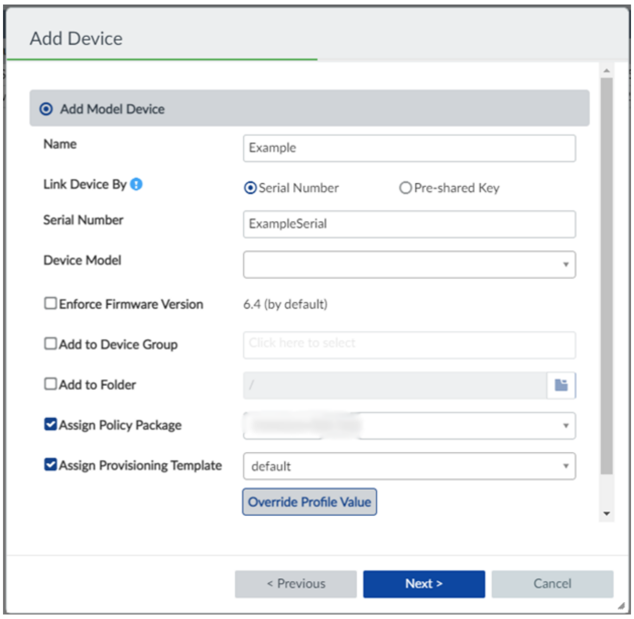


Figure 7: Fortimanager GUI

Once the Device Manager has opened / has been opened, a new model device needs to be added. This can be done by clicking “add device” - button, after which “Add Model Device” needs to be selected. After doing this, the wizard for adding a new device is presented to the user, as seen in Figure 8.



Add Device

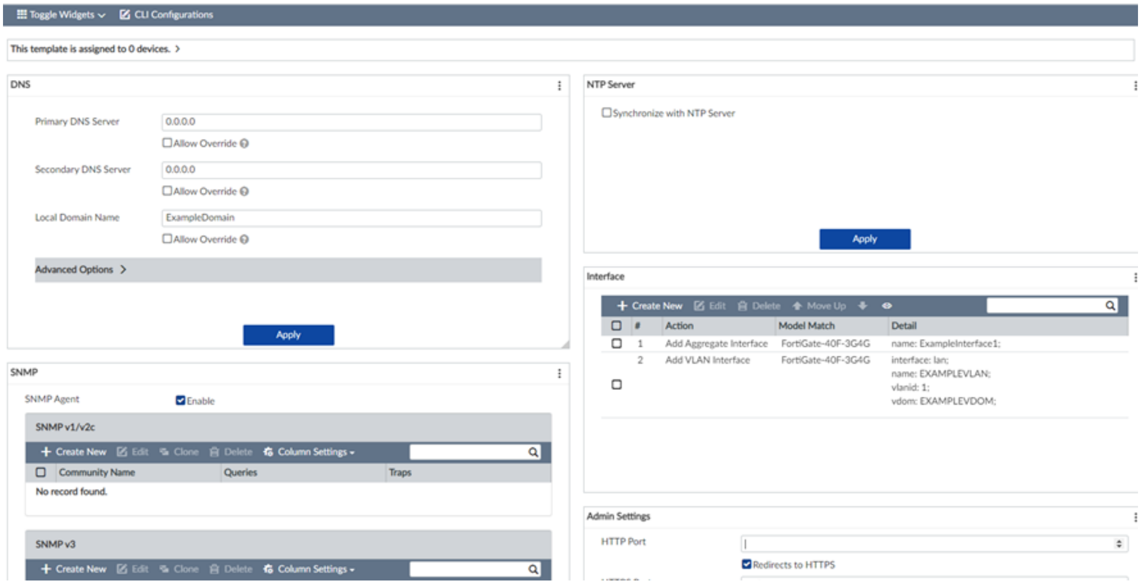
● Add Model Device

Name	Example
Link Device By	● Serial Number ○ Pre-shared Key
Serial Number	ExampleSerial
Device Model	
□ Enforce Firmware Version	6.4 (by default)
□ Add to Device Group	Click here to select
□ Add to Folder	/
☑ Assign Policy Package	[redacted]
☑ Assign Provisioning Template	default

Figure 8: Adding a model device interface

Once the model device has been created with the specifications seen in Figure 8, FortiManager will detect when a device with the serial “ExampleSerial” is connected to the network. FortiManager will detect the device only if the required commands, as seen in Figure 5, are given to the device that will be connected to FortiManager. Once the device is connected to FortiManager, it will assign the Policy Packages and Provisioning Templates that are defined for the model device.

Policy packages are collections of policies which define what security protocols are enforced on traffic passing through the devices which are connected to FortiManager. These devices are assigned the policy package. The policy packages can include, but are not limited to, IPv4 policies, interface policies, and proxy policies.



This template is assigned to 0 devices.

DNS

Primary DNS Server: 0.0.0.0
□ Allow Override

Secondary DNS Server: 0.0.0.0
□ Allow Override

Local Domain Name: ExampleDomain
□ Allow Override

Advanced Options

SNMP

SNMP Agent: ☑ Enable

SNMP v1/v2c

□	Community Name	Queries	Traps
No record found.			

SNMP v3

NTP Server

□ Synchronize with NTP Server

Interface

□	#	Action	Model Match	Detail
□	1	Add Aggregate Interface	FortiGate-40F-3G4G	name: ExampleInterface1;

□	2	Add VLAN Interface	FortiGate-40F-3G4G	interface: lan;
				name: EXAMPLEVLAN;
				vlanid: 1;
				vdom: EXAMPLEVDOM;

Admin Settings

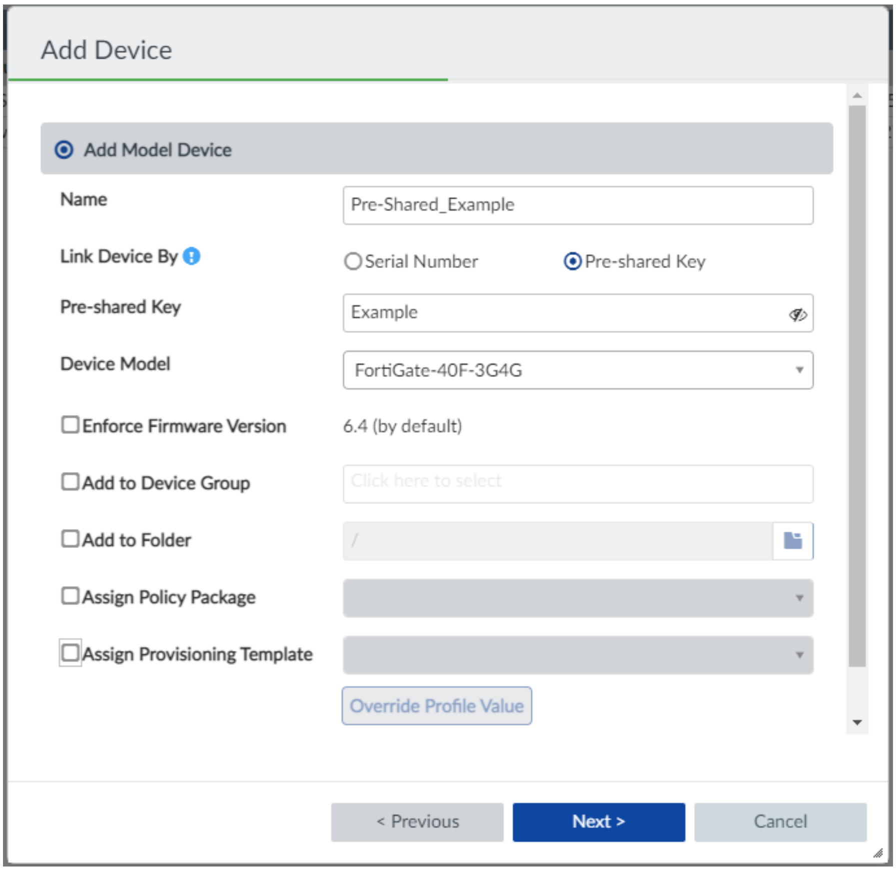
HTTP Port:
☑ Redirects to HTTPS

Figure 9: Provisional template GUI

Provisioning templates are configurations which are pushed to the device, such as VLAN interface settings, SNMP settings, and DNS settings. These templates can also be created via the CLI, but the GUI is easy to use and has all the options needed for the configuration of a device, as can be seen from Figure 9.

6.3.2 With Pre-Shared Key

It is possible to add a model device to FortiManager with a pre-shared key as its linking method. This process is otherwise the same, as laid out in the previous section, but while adding the model device, the pre-shared key option must be chosen. An example of this can be seen from Figure 10.



Add Device

● Add Model Device

Name: Pre-Shared_Example

Link Device By: ○ Serial Number ● Pre-shared Key

Pre-shared Key: Example

Device Model: FortiGate-40F-3G4G

□ Enforce Firmware Version 6.4 (by default)

□ Add to Device Group Click here to select

□ Add to Folder /

□ Assign Policy Package

□ Assign Provisioning Template

Figure 10: Adding a model device with a pre-shared key

From here onwards, the process stays the same as with the setup using a serial number.

The biggest difference with this method is with how much configuration is needed on the customer’s end, in order to bring the Fortinet device to FortiManager. While the Pre-Shared key method is not considerably more complex than the Serial Number method, the user still needs to perform extra steps, and if the user is not comfortable with the CLI interface, this can be uncomfortable.

The end user would need to perform the steps shown in Figure 5, but in addition to that, they would need to input the following command:

```
exe central-mgmt register-device <fmg-serial-number>
    <pre-shared key>
```

Listing 1. Command for adding a pre-shared key.[6]

For this project, priority was put to the idea that the easier it is for the end user to configure the device for usage, the better. With the pre-shared key method, they would also need to be given the serial number to the device, which can cause human errors when inputting the serial number to the command previously mentioned. Thus, it is better to use the serial number method, as mentioned in chapter 6.3.1, with which the customer does not have to configure the device as much, and as such there is less of a risk for human error.

6.3.3 FortiDeploy

FortiDeploy is only usable, when the device has been factory reset, and there is the possibility for the use of FortiGate Cloud. FortiGate Cloud is a cloud-based SaaS, with which there is no need for a FortiManager device or virtual machines.

This caused FortiDeploy to be ruled out immediately, as there was already an FortiManager environment set up at Tietokeskus, and not much research was done into deployments with FortiDeploy.

7 Results

Even though the results of this project were not as first anticipated, due to true zero-touch not being achieved, the results were satisfactory, and they will help with the future deployment of devices to customers.

The configuring of the device and the building of the test environment within FortiManager proved to be easier than what was anticipated, which made the process of working on the project virtually painless.

While neither the serial number nor the pre-shared key methods of deployment are truly zero-touch, they are still as close to zero-touch as possible, without using FortiDeploy.

As a result of this project being a success, the project will most likely be used in the future as a reference in some way when it comes to the deployment of Fortinet devices.

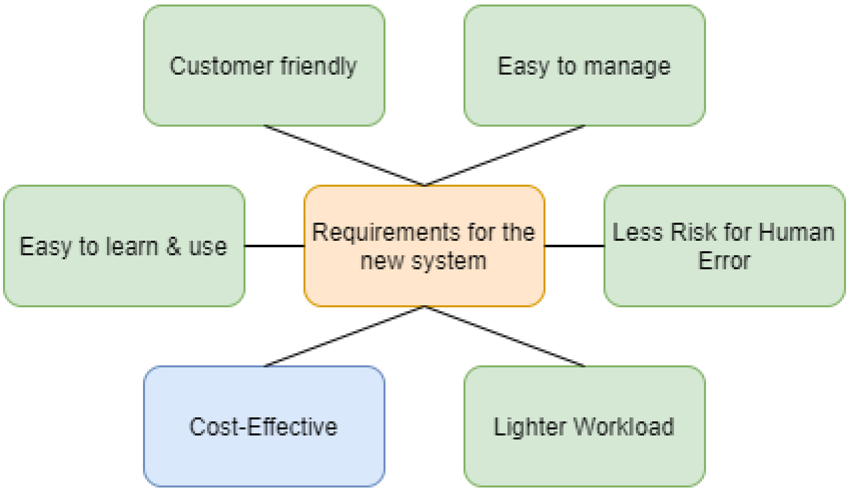


Figure 11: Requirements which were met

Figure 11 above illustrates what requirements were met. All the requirements which are green were met. Cost-effectiveness is marked as blue because it remains to be seen how cost effective this system is in comparison to the old system.

8 Conclusion

This thesis has presented the implementation of zero-touch deployment with Fortinet devices, and all the steps taken to achieve this. Firstly, it was examined why it was necessary to make device deployments easier and more convenient for the customers of Tietokeskus. Then it was examined what requirements Tietokeskus had for the new system, when it comes to deploying new devices. After that, the project was described from start to finish, and lastly the results of the project were presented.

The project itself was straightforward, which was enabled by the fact that the Fortinet Document Library was well updated, as was the internal documentation of Tietokeskus. The project was also helped by meetings with the project supervisor, who was able to give more insight into how deployments worked before Fortinet’s products were put into production and into how they are currently deployed.

The thesis accurately lays out the steps needed in order to set up a method of near zero-touch deployment of Fortinet devices. The results of the project have satisfied the project supervisor. It is still being decided whether this system of deployment will be used for future deployments of Fortinet devices, or whether this project serves as a case study of what possibilities there are for future deployments.

In conclusion, a system was successfully created, with which minimal user input is required for this style of device deployment, meaning that only a few lines of inputs are needed to bring the FortiWiFi device to the FortiManager and to push the configurations automatically to the device once it is connected to FortiManager. The project also showed that true zero-touch deployment is not possible without the FortiDeploy system, which is not accessible to Tietokeskus at the moment. The system which was created was approved by the representative of the commissioning company.

Overall, the project was a success, and the results of this project will most likely be used in the future processes of Tietokeskus when it comes to deploying new Fortinet hardware.

References

1 Tietokeskus Finland Oy. Tietokeskus. Online. <https://www.tietokeskus.fi/tietokeskus>. Accessed 5 March 2021.

2 Picture of Fortimanager Device. Avfirewalls. Online. <https://www.avfirewalls.com/images/FortiManager/fmg-200g.png>. Accessed 21 April 2021.

3 Docs Library. Fortinet. Online. <https://docs.fortinet.com/>. Accessed 10 March 2021.

4 Fortigate & FortiManager. 2021. Company internal documentation. Tietokeskus Finland Oy.

5 Fortinet Document Library. Adding Devices. Fortinet. Online. <https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/632825/adding-devices>. Accessed 20 March 2021.

6 Fortinet Document Library. Example of adding a model device by pre-shared key. Fortinet. Online. <https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/90326/example-of-adding-a-model-device-by-pre-shared-key>. Accessed 30 March 2021.