Ubiquiti Unifi CloudKey - Unifi Controller overview and setup

SERVER MANAGEMENT

Managed Service Provider | Network Solutions | Information Systems | IT Projects | www.serman.ee

Overview

> This article is written by Server Management Inc. IT systems administrator Timo Puistaja - 20.12.2016, Tartu, Estonia.

Need help configuring your device? Contact us info@serman.ee

Ubuiquiti Unifi is a set of enterperise Wireless solutions, including AccessPoints - Edu, LongRange, Lite and Pro versions.

For management purposes there are several solutions - downloadable Controller (Windows/Linux/Mac); CloudKey - device/pc/server that acts as Controller and has its own Management interface.

Unifi devices are ment to use when buildin big corporate networks with multiple sites. In this tutorial we are going to show some basic steps to prepare yourself for centralized Wifi management for multiple sites over EU or the world.

Unifi devices support L2 (LAN) and L3 (WAN) management/adoption.

In this article we are prepearing our CloudKey to manage AP´s from different countries all over EU. Our goal is to have proper domain name unifi.mydomain.com with proper wildcard SSL certificate and access/management of Wifi.

Before continuing lets make sure we understand the product names:

Unifi Controller - webpage/service to manage all the Wifi AP´s and sites centralized to one place. It is possible to install Controller software to Linux/Windows and Mac systems **OR** buy a CloudKey that has Controller preinstalled and ready to use.

Unifi CloudKey - a device/pc/server that has Unifi Controller already working inside it. CK also has Management Interface to manage CloudKey itself - firmware updates, static ip; controller update etc.

Installing CloudKey to your LAN

CloudKey can be powered via MicroUSB (minimun 2A) or PoE

Just add power and connect CK to your LAN via ethernet cable.

Check from DHCP server which IP it got and type the IP in your web browser - you are ready to make your initial setup!

Set static IP to your CK either from DHCP server of from CK Management interface.

Now you are ready to manage/adopt your AP´s in local network - thats L2 adoption (only devices in your local subnet can be managed)

Accessing CloudKey (Controller) from public networks

To access your Controller from public networks or make L3 adoption you need to know the basics of port forwarding (firewalls) and domain name systems.

Prerequisites for WAN access to controller using domain name:

1. Public static IP from your ISP
2. DNS settings in your domain name management (for example: unifi.mydomain.com points to 32.32.32.32)

3. Access and knowledge to manage your firewall - port forwards to your CK

By default, the UniFi Controller will operate on the following ports:

- unifi.http.port=8080 (port for UAP to inform controller)
- unifi.https.port=8443 (port for controller GUI / API, as seen in web browser)
- portal.http.port=8880 (port for HTTP portal redirect)
- portal.https.port=8843 (port for HTTPS portal redirect)
- unifi.db.port=27117 (local-bound port for DB server)

Here is a little picture to show you how port forwarding with CloudKey should work:

Installing Wildcard SSL certificate to your Unifi CloudKey(Controller)

1. Intro

Unifi downloadable Controller and CloudKey come with self-signed certificates installed on them. We want to have our trusted SSL certificate on Controller. When accessing your controller unifi.mydomain.com web browsers let you know that the certificate is not trusted and may harm you. We have Wildcard SSL certificate from Comodo - so we need to install them to Cloudkey to get secured and nice green HTTPS://unifi.mydomain.com address in our browsers.

If you want to use **Free Let´s Encrypt certificate** - this is the tutorial for you!

1.1 We need some preparations before we can continue to configure the CK.

1.2 Trusted Certificate

We have ordered wildcard (*.mydomain.com) SSL certificate from Comodo and got these files:

1. STAR_mydomain_com.ca-bundle - **NOT NEEDED FOR CloudKey**
2. STAR_mydomain_com.crt - wildcard certificate, signed by CA
3. wildcard.mycomain.com.key - KEY for wildcard certificate

So we have signed .crt and .key that we are going to use.

Wildcard certificates work the same way as a regular SSL Certificate, allowing you to secure the connection between your website and your customer's Internet browser – with one major advantage. A single Wildcard SSL Certificate covers any and all of the sub-domains of your main domain.

PS! Unifi Controller uses Java keytool to manage certificates - Java Keytool Essentials:

1.3 Software for the work

1. 7zip - archives management tool
2. Putty - tool to access your devices via SSH/telnet etc.
3. WinSCP - tool to access your devices via SFTP/FTP to move files between computers
4. KeyStore Explorer - GUI replacement for the Java command-line utilities keytool and jarsigner.

1.4 How does certificate package look like in CloudKey

Certificates are located in the CloudKey folder /etc/ssl/private

1. cert.tar - this is a tar file contains 3 files below, boot up process will check if they are out of sync
2. cloudkey.crt - *.mydomain.com certificate
3. cloudkey.key - *.mydomain.com key for certificate
4. unifi.keystore.jks - .crt and .key combined together for Java certificate management.

Those files won't be touched during firmware upgrade, but they will be removed if you reset the UniFi Cloudkey back to factory default.

2. Configuration

2.1 Download unifi.keystore.jks from CK

1. Use WinSCP to access your CK
2. Navigate to /etc/ssl/private
3. Download unifi.keystore.jks to your computer
4. Dont close WinSCP connection

2.2 Replace certificates inside unifi.keystore.jks

1. Fire up KeystoreExplorer
2. Open an existing KeyStore - choose the unifi.keystore.jks you downloaded before
3. Password: *aircontrolenterprise*
4. Delete entry "unifi" - now you have empty keystore file
5. Tools - Import Key Pair - OpenSSL
    1. I dont have Encrypted Private Key - **untick**
    2. Import .key (in my case its **wildcard.mycomain.com.key**)
    3. Import .crt (in my case its **STAR_mydomain_com.crt)**
    4. **Import**
    5. Enter Alias: unifi.mydomain.com
    6. **NB! Enter password:** aircontrolenterprise **THIS IS IMPORTANT!**
6. Save your modified **keystore file as "unifi.keystore.jks"** add password

aircontrolenterprise

Now your unifi.keystore.jks file is modified with your own certificates and ready to be uploaded to CK.

2.3 Rename filenames and regenerate cert.tar file

Rename all the files needed for CloudKey and regenerate cert.tar. In my case:

1. STAR_mydomain_com.crt - **cloudkey.crt**
2. wildcard.mycomain.com.key - **cloudkey.key**

Generate new **cert.tar**

1. Open up 7zip
2. Choose files: cloudkey.crt; cloukey.key and unifi.keystore.jks and click Add
3. Name: cert.tar; Archive format: tar
4. Done

2.4 Rename old files inside CloudKey

1. Use Putty to SSH into your CK
2. Navigate to /etc/ssl/private
3. Rename files:
    1. cert.tar - cert.tar.orig
    2. cloudkey.key - cloudkey.key.orig
    3. cloudkey.crt - cloudkey.crt.orig
    4. unifi.keystore.jks - unifi.keystore.jks.orig

2.5 Upload files to CloudKey

1. Continue using WinSCP
2. Upload files you created (cloudkey.crt; cloudkey.key; cert.tar; unifi.keystore.jks) to /etc/ssl/private
3. Reboot CloudKey

2.6 ACCESS YOU CONTROLLER - unifi.mydomain.com

If it works now you have your singed and trusted SSL certificate and web page HTTPS:// is nice solid green. Browsers trust your webpage = profit.

3. Testing - L3 adoption using set-inform as unifi.mydomain.com

Ubiquiti Unifi - L2 and L3 adoption explained

Need help configuring your device? Contact us info@serman.ee

Last update: 22/05/2019