multiOTP® Pro To Enterprise Upgrade Quick Guide

Overview

This Quick Guide explains how to easily upgrade from **multi*OTP*® Pro** to **multi*OTP*® Enterprise** and activate the master/slave feature.

1. Upgrade the firmware of the multi*OTP*® Pro appliance

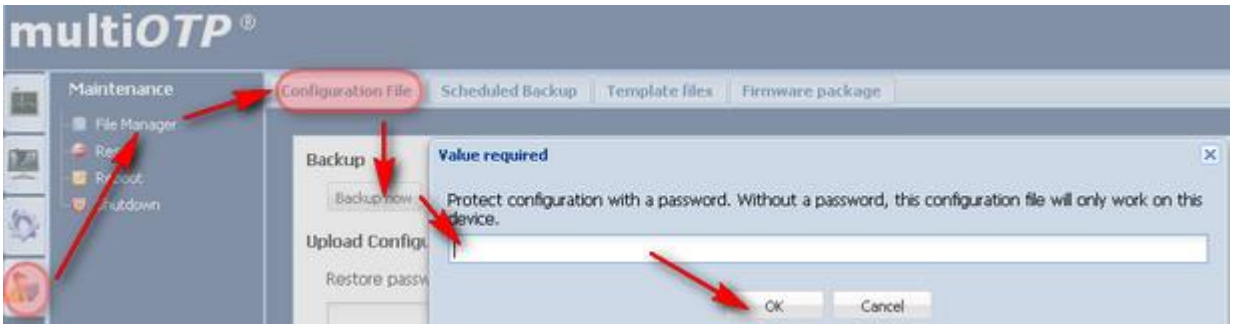
The firmware of the **multi*OTP*® Pro** appliance must be the release 5.0.1.3 or higher. The last firmware can be downloaded from the appliance Web interface, or directly at this address: **http://firmware.multiotp.com/pro/update/**

2. Download the multi*OTP*® Enterprise appliance and upgrade the firmware

The **multi*OTP*® Enterprise** appliance is available as a VMware virtual appliance here: **http://firmware.multiotp.com/enterprise/**
Last firmware can be downloaded from the appliance Web interface, or directly here: **http://firmware.multiotp.com/enterprise/update/**

3. Perform a backup on your multi*OTP*® Pro appliance

Do a backup on your **multi*OTP*® Pro** appliance. Be sure to enter an encryption password, otherwise the restore will only be readable on this appliance.



This will create a **config-xxx-YYYYMMDD-HHMMSS.bin** configuration file.

4. Perform a restore on your multi*OTP*® Enterprise appliance

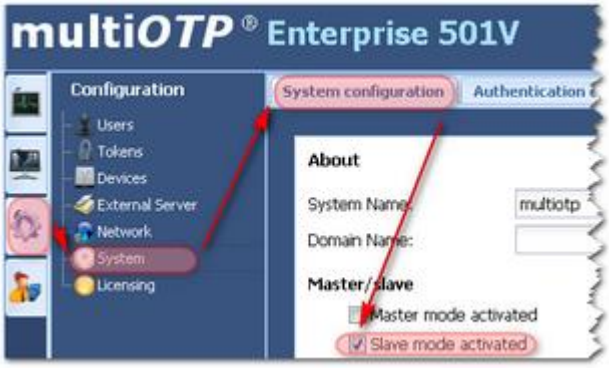
Do a restore on your **multi*OTP*® Enterprise** appliance. You will have to give the same password as for the backup process on the previous appliance. Please note that the network configuration is never restored.

5. Install a slave multi*OTP*® Enterprise appliance

Install a second appliance from scratch based on the downloaded VMware virtual appliance file.

6. Slave: define the multi*OTP*® Enterprise appliance as a slave device

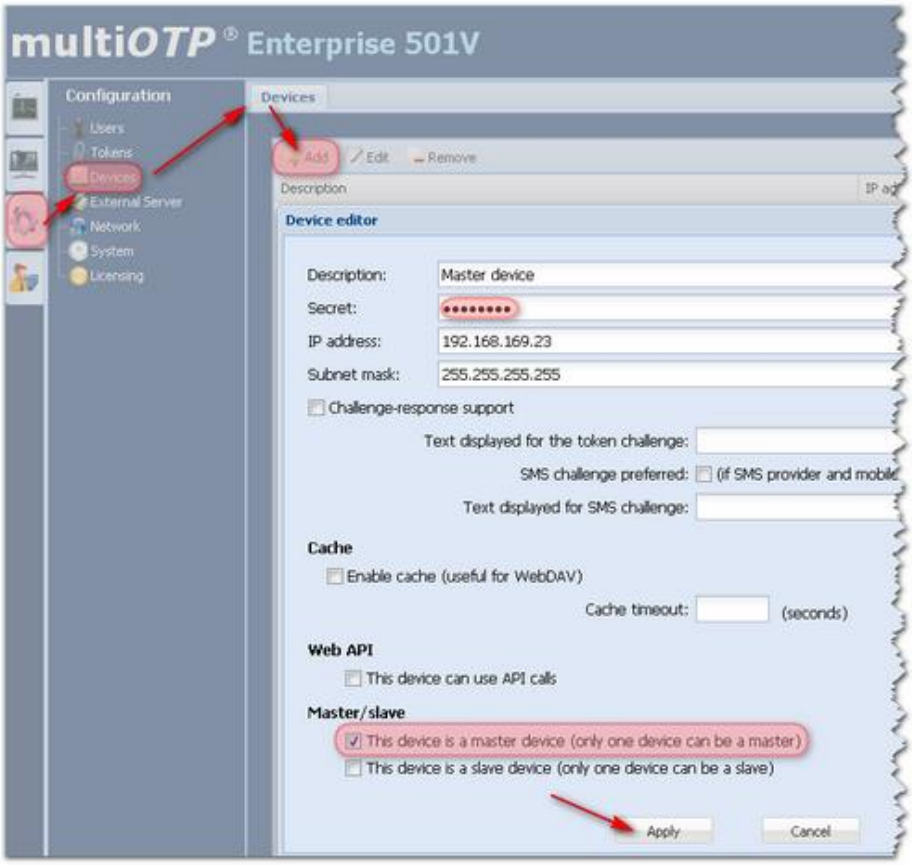
The second appliance must be defined as a slave device.



The slave device will **not** synchronize with the defined AD/LDAP server, except if no data are received from the master device for a while.
The slave device will **not** send automatic provisioning emails.

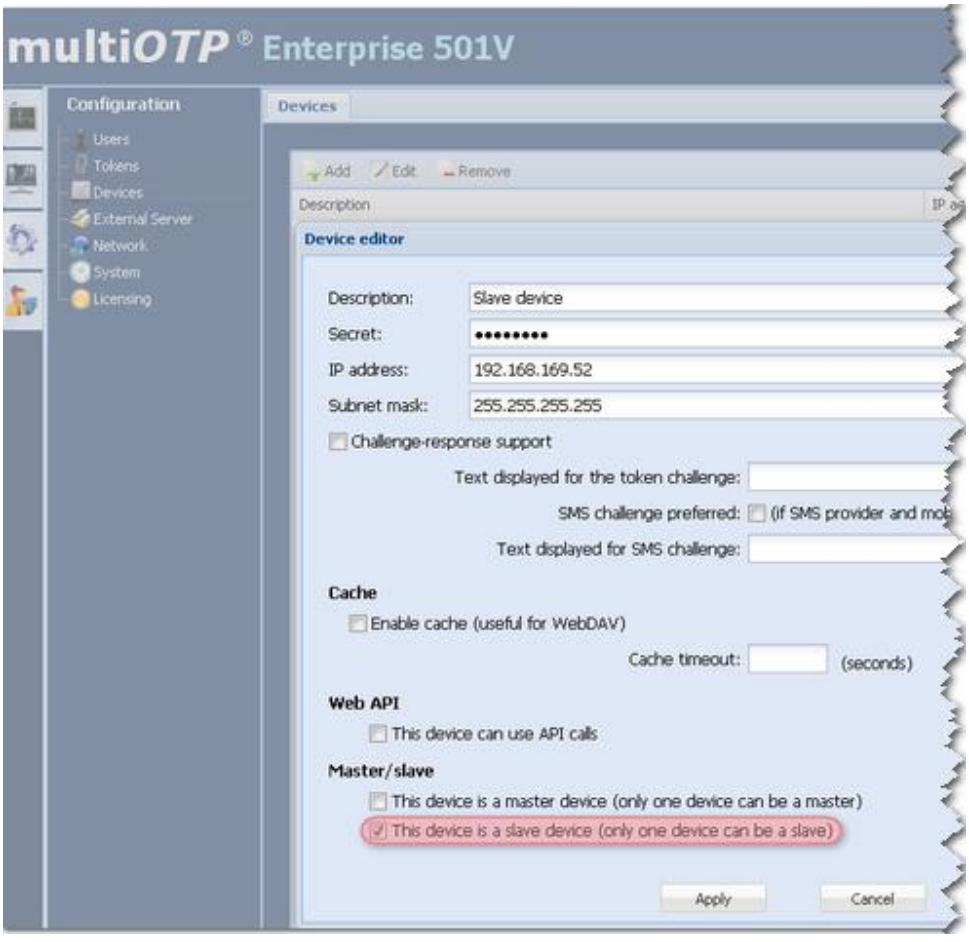
7. Slave: define the shared secret with the master device

On the second device (the slave), declare the IP address (mask 255.255.255.255) and the secret of the master appliance, and set this created device as a master device.



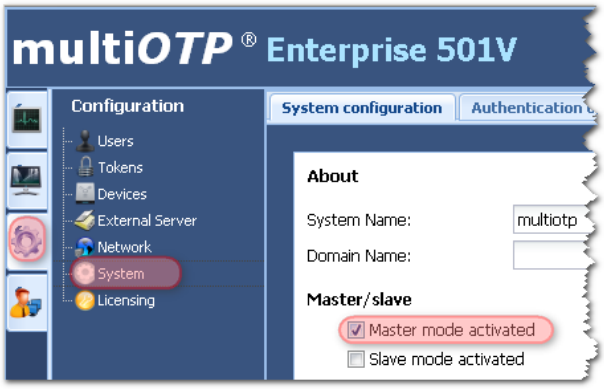
8. Master: define the shared secret with the slave device

On the first device (the master), declare the IP address (mask 255.255.255.255) and the secret of the slave appliance, and set this created device as a slave device.



9. Master: define the multiOTP® Enterprise appliance as the master device

The first appliance must be defined as the master device.



10. Finished!

That's it, you have now a HA master/slave strong two factors authentication.