

Overview

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

1. Upgrade the firmware of the multiOTP® Pro appliance

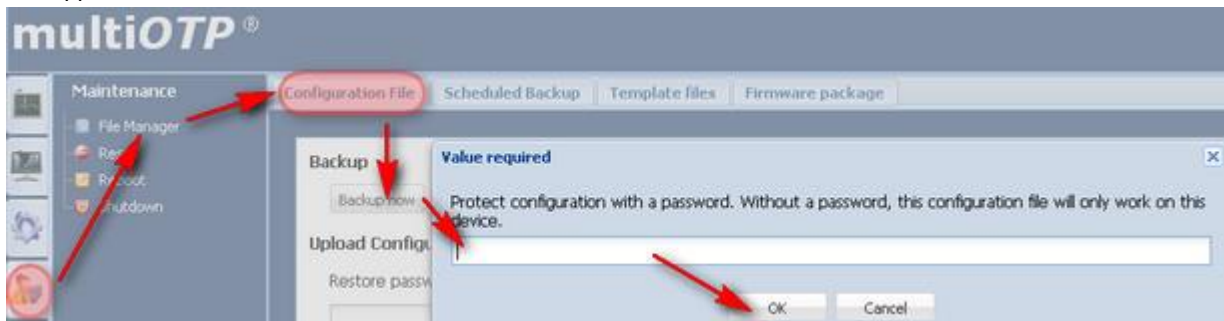
The firmware of the multiOTP® Pro appliance must be the release 5.0.1.3 or higher. The last firmware can be downloaded from the appliance Web interface, or directly at this address: <http://firmware.multip.com/pro/update/>

2. Download the multiOTP® Enterprise appliance and upgrade the firmware

The multiOTP® Enterprise appliance is available as a VMware virtual appliance here: <http://firmware.multip.com/enterprise/>
Last firmware can be downloaded from the appliance Web interface, or directly here: <http://firmware.multip.com/enterprise/update/>

3. Perform a backup on your multiOTP® Pro appliance

Do a backup on your multiOTP® 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 multiOTP® Enterprise appliance

Do a restore on your multiOTP® 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 multiOTP® Enterprise appliance

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

6. Slave: define the multiOTP® 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.

The screenshot shows the 'multiOTP Enterprise 501V' configuration interface. The left sidebar contains a 'Configuration' menu with options: Users, Tokens, Devices, External Server, Network, System, and Licensing. The 'Devices' menu item is highlighted with a red circle and a red arrow. The main area is titled 'Devices' and contains an 'Add' button (circled in red), 'Edit', and 'Remove' buttons. Below this is a 'Device editor' form with the following fields and options:

- Description: Master device
- Secret: [Redacted]
- IP address: 192.168.169.23
- Subnet mask: 255.255.255.255
- Challenge-response support
- Text displayed for the token challenge: [Empty field]
- SMS challenge preferred: (if SMS provider and mobile number are provided)
- Text displayed for SMS challenge: [Empty field]
- Cache
 - Enable cache (useful for WebDAV)
 - Cache timeout: [Empty field] (seconds)
- Web API
 - This device can use API calls
- Master/slave
 - This device is a master device (only one device can be a master)
 - This device is a slave device (only one device can be a slave)

At the bottom of the form are 'Apply' and 'Cancel' buttons. A red arrow points to the 'Apply' button.

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.

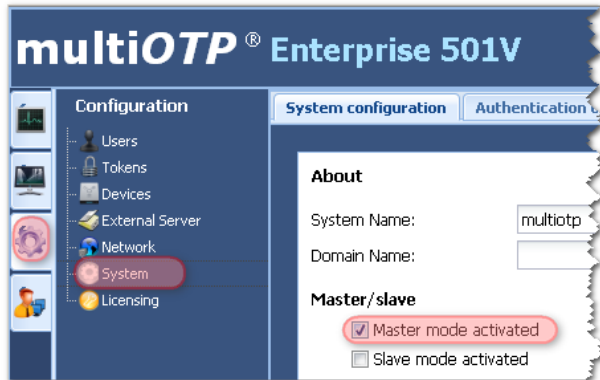
The screenshot shows the 'multiOTP Enterprise 501V' configuration interface. The left sidebar contains a 'Configuration' menu with options: Users, Tokens, Devices, External Server, Network, System, and Licensing. The 'Devices' menu item is highlighted with a red circle and a red arrow. The main area is titled 'Devices' and contains an 'Add' button (circled in red), 'Edit', and 'Remove' buttons. Below this is a 'Device editor' form with the following fields and options:

- Description: Slave device
- Secret: [Redacted]
- IP address: 192.168.169.52
- Subnet mask: 255.255.255.255
- Challenge-response support
- Text displayed for the token challenge: [Empty field]
- SMS challenge preferred: (if SMS provider and mobile number are provided)
- Text displayed for SMS challenge: [Empty field]
- Cache
 - Enable cache (useful for WebDAV)
 - Cache timeout: [Empty field] (seconds)
- Web API
 - This device can use API calls
- Master/slave
 - This device is a master device (only one device can be a master)
 - This device is a slave device (only one device can be a slave)

At the bottom of the form are 'Apply' and 'Cancel' buttons.

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.