Pico-UTM 100 FAQ

Next Generation Network Security

Pico-UTM 100 Frequently Asked Questions

01 Login and Start Managing Pico-UTM

Q1. How to log in to Pico-UTM?

Step 1: Connect the WAN port of Pico-UTM to a network where the Pico-UTM can be assigned with a valid IP address automatically from a DHCP server.

Step 2: Connect the LAN port of Pico-UTM to a PC (or a laptop) with an ethernet cable.

Step 3: Launch a web browser on the PC and enter “http://mypico.lionic.com”. Then the Pico-UTM login page displays.

Q2. If the Pico-UTM cannot be assigned with a valid IP address, how to log in to Pico-UTM?

Pico-UTM may not be assigned with a valid IP address due to the following reasons:

1. The network is using static IP addresses (no DHCP server).
2. The network requires getting a valid IP address through PPPoE.
3. The DHCP server is not working.

In such cases, log in to Pico-UTM with the alternative method:

Step 1: Connect the LAN port of Pico-UTM to a PC (or a laptop) with an ethernet cable.

Step 2: Set the IP configuration for the PC manually:

· IP address: 10.254.254.1 (~253) · Netmask: 255.255.255.0

Step 3: Launch a web browser on the PC and enter “http://10.254.254.254”. Then the Pico-UTM login page displays.

Q3. How to manage multiple Pico-UTMs?

A Central Management System (CMS) designed for enterprises and organizations can help IT administrators manage multiple Pico-UTMs. With the CMS, IT administrators can remotely configure security policies for Pico-UTMs, and monitor threats detected by each Pico-UTM. Please contact Pico-UTM sales representatives or resellers in your region for more information about the CMS.

02 Configure Network Settings for Pico-UTM

Q1. Is it necessary to connect to Internet when using Pico-UTM?

Yes, it is necessary to keep Pico-UTM connecting to Internet. While Pico-UTM is operating, it needs Internet to upgrade firmware, update signatures, check the license status, and access Lionic security cloud services, which enhance the protecting ability of Pico-UTM.

Q2. How to deploy Pico-UTMs in an intranet?

When Pico-UTM runs in an intranet, such as smart factories or offices where Pico-UTM cannot reach Internet, firmware upgrading, signature updating and some other services will be not working. In order to keep the full protection of Pico-UTM, it is necessary to build a CMS and a proxy server helping Pico-UTMs access all Lionic cloud services. Please contact Pico-UTM sales representatives or resellers in your region for more information about deploying Pico-UTMs in an intranet.

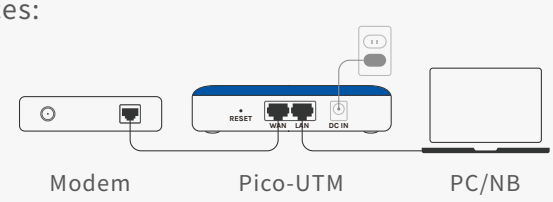
Q3. How to obtain a valid IP address for Pico-UTM?

Based on the network environment, Pico-UTM can obtain a valid IP address by 1 of the 3 methods listed below:
1. Auto (DHCP, default setting) 2. Static IP 3. PPPoE
This [Connection] setting can be configured in [WAN] page after logged in to Pico-UTM.

Q4. I got only 1 valid IP address. How do I configure Pico-UTM?

If your Internet Service Provider (ISP) or IT administrator provides you only 1 valid IP address, you may switch Pico-UTM to [Router Mode] by the following step, so that it can distribute private IP addresses to LAN devices:

Step 1: Connect Pico-UTM and a PC/laptop as shown in the following figure:



Step 2: Set the IP configuration for the PC manually:

· IP address: 10.254.254.1 (~253) · Netmask: 255.255.255.0

Step 3: Launch a web browser on the PC and enter “http://10.254.254.254”. Then the Pico-UTM login page displays.

Step 4: Go to [WAN] page and set the IP configuration based on the instruction from your ISP or IT.

Step 5: Go to [System] > [Device] page, find [Device Settings] and switch [Connection Mode] from [Bridge] to [Router], then click [Apply].

The Pico-UTM would reboot while applying the new setting. After the reboot is done, Pico-UTM connests Internet with the IP address offered by ISP or IT administrator, and assigns private IP addresses to LAN devices with a DHCP server in Pico-UTM. You may replace the PC with a switch, router or Wi-Fi AP if there are more than 1 LAN device to be connected.

Note: Disabling the DHCP server in the router or Wi-Fi AP is recommended, in order to avoid double NAT.

03 About the License of Pico-UTM

Q1. Why does Pico-UTM need a license?

A valid license keeps Pico-UTM authorized to access all cloud services provided by Lionic. While the license is valid and Pico-UTM is connected to Internet, Lionic cloud services, such as the firmware and signature update service and the cloud-based virus and malicious website inspecting service, are available, so that the Pico-UTM provides the full protection.

Q2. How to upgrade the firmware for Pico-UTM?

Once a new version of Pico-UTM firmware is released, Pico-UTM will show a notification in [System] > [Firmware Upgrade] page, as long as the license is valid and the Pico-UTM is connected to Internet. After you pressed [Burn] button, the Pico-UTM will start upgrading.

Note: The Pico-UTM will reboot during the upgrading. The Internet connection will be interrupted and resumed after the reboot.

Q3. How to update the signature for Pico-UTM?

The signature will be updated automatically twice a week, as long as the license is valid and the Pico-UTM is connected to Internet.

Q4. What would happen after the license of Pico-UTM expired?

After the license expired, the Pico-UTM will not be able to access all Lionic cloud services, including firmware and signature update service and the cloud-based virus and malicious website inspecting service. Since the remaining protection may be not enough to secure your devices, it is recommended to extend the license by resuming the subscription or contacting Pico-UTM sales representatives or resellers in your region.

Q5. Why does “License Expiration Date” on the dashboard show “Status checking failed”?

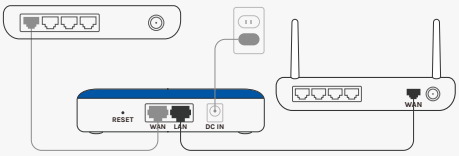
When “License Expiration Date” on the dashboard shows “Status checking failed”, it means that the Pico-UTM is not able to connect to Lionic License Server successfully. Please check if the Pico-UTM is able to access Internet. If there is no network connection issue, please contact Pico-UTM sales representatives, resellers or technical support in your region.

04 About the Protection of Pico-UTM

Q1. How do I know if my device is protected by Pico-UTM?

As long as your device accesses Internet through Pico-UTM, it is protected by Pico-UTM. In the other words, if the upward (to Internet) or downward (from Internet) packet goes through Pico-UTM, the packet would be inspected and your device would be protected.

Note: If the ISP provides you a modem router, combined with modem, router or even Wi-Fi AP, all devices directly connected to the modem router would not be protected, since these devices does not access Internet “through” Pico-UTM. In order to be protected, you would need to add another router or Wi-Fi AP at the LAN port of Pico-UTM as shown in the following figure:



Q2. Why does the Internet speed seem slower after Pico-UTM is installed?

It would take some time for Pico-UTM to inspect packets and match the content with the signature of viruses or attacks. Thus, the Internet speed may be slower while Pico-UTM is protecting your devices. Depending on the protocol or application you are using, the actual Internet speed may differ.

Q3. How many devices can 1 Pico-UTM protect?

Generally, 1 Pico-UTM can protect 50 devices. The actual device number may be different depending on how many sessions are used on each device.

Q4. What would Pico-UTM do once a threat is detected?

The 3 security features of Pico-UTM would do different actions to the threat:
1. Anti-Virus: “Log and Destroy File” (default) or “Log Only”
2. Anti-Intrusion: “Log and Block” (default) or “Log Only”
3. Anti-WebThreat: “Log and Block” (default) or “Log Only”

To configure the action, go to [Policy] > [Anti-Virus] or [Anti-Intrusion] or [Anti-WebThreat] page and select in [Action] drop-down menu.

Q5. What can I do if Pico-UTM destroyed a trusted file or blocked a trusted connection?

Since the packet may be similar to a part of viruses or attacks in rare cases, Pico-UTM would consider it as a threat. If Pico-UTM destroyed a file or blocked a connection you trust, you can add it into the whitelist by the following steps:

Step 1: Log in to Pico-UTM.

Step 2: Go to [Threats] and find the event in [Anti-Virus], [Anti-Intrusion] or [Anti-Web Threat] page. You may identify the event with the file name or IP address.

Step 3: Click [+ Add] button at the end of the event (in the last column of each row) to add it into the whitelist.

Step 4: Download the file or connect the site again.

Furthermore, you can also report this issue via our website:
https://www.lionic.com/reportfp_lc