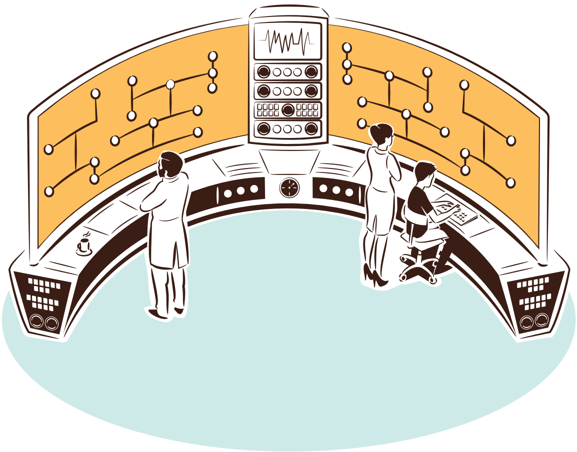
AleFIT MAB Keeper & Office Locator



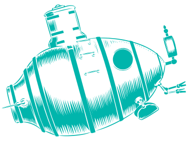
The fundamental objective of network security is safeguarding the local network against unauthorized access of users and devices. For this reason, the IEEE 802.1x standard was created and Cisco offers a product called the Identity Services Engine (Cisco ISE) that oversees network access. ALEF NULA has developed the **AleFIT MAB Keeper** and **AleFIT Office Locator** applications that help fulfill these requirements.

After deploying this restrictive technology, our customers have been asking how to deal with problems stemming from incompatible and non-existent internal processes concerning, for example:

- What to do to if a workstation failed to be properly authenticated with there being no apparent reason for it?
- How to quickly authenticate users if they have been denied access but need to start work immediately?
- How to enable reimaging of a workstation on a secured port?
- How to cut the costs of the administration of the system?
- How to securely designate the management of passive devices (devices that do not support the 802.1x standard) to their administrators?
- How to allow management and system troubleshooting for helpdesk operators who may not be familiar with the used technology?
- Is it possible to wake up workstations on a secured port?

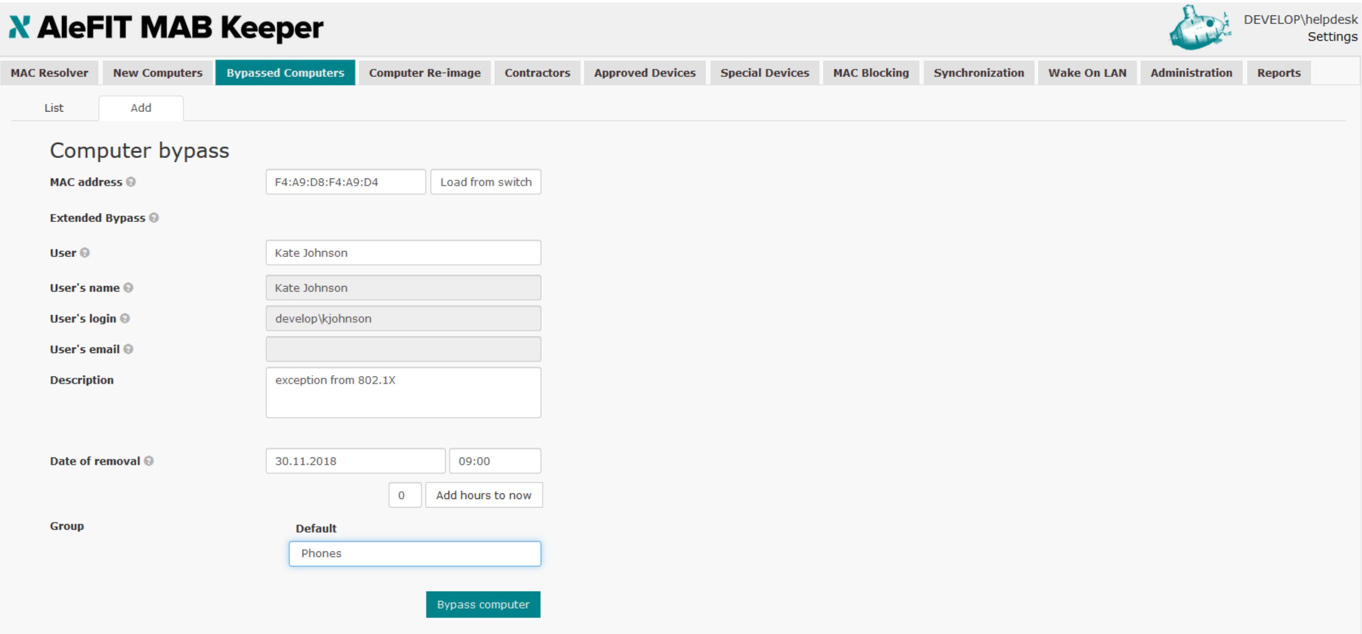
Other questions regarding the implementation (answered on following pages):

- What to do if a workstation fails to authenticate without any apparent reason?
- Some devices that connect to our network do not support the 802.1x standard. Is it possible to simplify the authentication of such devices without having to use our specialists?
- Is it possible to automatically disconnect a device from the network for which a temporary exception has been granted?
- Is it possible to provide network access to our external suppliers?
- Is controlled access possible for a non-corporate workstation of a corporate user?
- We are used to running updates at night. However, after deploying 802.1x, our existing solutions for remote wake-up on the LAN of workstations do not work. How can we solve this problem?
- What do I do if I need automatic installation of new workstations or so-called “reimaging” of workstations?
- We know the name of the computer or the user. Is it possible to find out where the user/device is connected to the network as well as the status of the authentication session?
- Is it possible to find out who registered a MAC address as well as when and why?



AleFIT MAB Keeper

The AleFIT MAB Keeper application allows the management of certain settings of the authentication system without having access to the configuration GUI of the Cisco ISE. Access rights are assigned based on the administration roles. Thanks to the easy and ergonomic user interface, administrators do not need to have detailed knowledge of the Cisco ISE. Operations can be carried out directly using the GUI or automatically using the built-in REST API. Individual operations are processed in workflows and divided into separate modules.

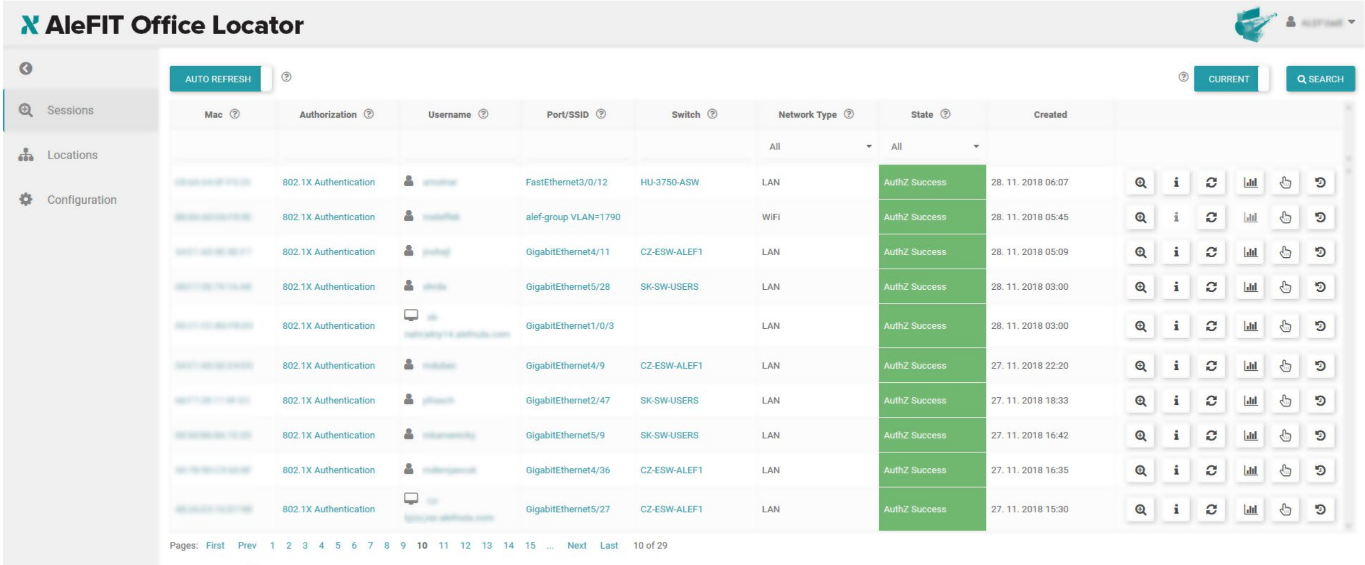


Computer bypass

MAC address	F4:A9:D8:F4:A9:D4
Extended Bypass	
User	Kate Johnson
User's name	Kate Johnson
User's login	develop\kjohnson
User's email	
Description	exception from 802.1X
Date of removal	30.11.2018 09:00
	0
Group	Default Phones

AleFIT Office Locator

The AleFIT Office Locator application provides comprehensive information concerning the status of the authentication of a device and its location on the specific switch and port. With regard to troubleshooting, the application allows the reading of the authentication logs from the Cisco ISE, the checking of the workstation or user account in the LDAP, the checking of the switch port configuration and the restarting of an authentication session via a CoA message. This information is available to authorized personnel in one location without the need to access other systems (LDAP, Cisco ISE, switches). The AleFIT Office Locator application is fully integrated with the AleFIT MAB Keeper application.



Mac	Authorization	Username	Port/SSID	Switch	Network Type	State	Created
					All	All	
[redacted]	802.1X Authentication	[redacted]	FastEthernet3/0/12	HU-3750-ASW	LAN	AuthZ Success	28. 11. 2018 06:07
[redacted]	802.1X Authentication	[redacted]	alef-group VLAN=1790		WiFi	AuthZ Success	28. 11. 2018 05:45
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet4/11	CZ-ESW-ALEF1	LAN	AuthZ Success	28. 11. 2018 05:09
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet5/28	SK-SW-USERS	LAN	AuthZ Success	28. 11. 2018 03:00
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet1/0/3		LAN	AuthZ Success	28. 11. 2018 03:00
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet4/9	CZ-ESW-ALEF1	LAN	AuthZ Success	27. 11. 2018 22:20
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet2/47	SK-SW-USERS	LAN	AuthZ Success	27. 11. 2018 18:33
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet5/9	SK-SW-USERS	LAN	AuthZ Success	27. 11. 2018 16:42
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet4/36	CZ-ESW-ALEF1	LAN	AuthZ Success	27. 11. 2018 16:35
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet5/27	CZ-ESW-ALEF1	LAN	AuthZ Success	27. 11. 2018 15:30

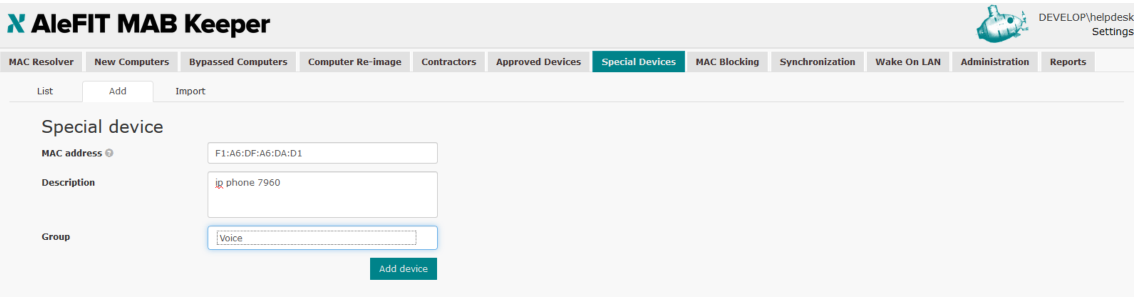
Pages: First Prev 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ... Next Last 10 of 29

1) What to do if a workstation fails to authenticate without any apparent reason?

The standard procedure is to contact the helpdesk or technical support, which will refer the problem to the specialists. They will start to identify the problem and, if the response from the technical support is immediate, the problem is usually solved in a matter of 10 or 20 minutes or so. In most cases however, this is unacceptable. The AleFIT MAB Keeper and Office Locator ensure maximum simplification and automation of the process.

Using the AleFIT Office Locator, the helpdesk or technical support is able to identify the current status of device authentication and verify whether it has been carried out successfully. In the event that authentication is unsuccessful, they can use the AleFIT MAB Keeper to set a temporary exception based on user identification, enabling the user to connect to the network anyway. The problem is subsequently forwarded to the specialists, who then have a few hours to solve the problem.

2



Special device

MAC address: F1:A6:DF:A6:DA:D1

Description: ip phone 7960

Group: Voice

2) Some devices that connect to our network do not support the 802.1x standard. Is it possible to simplify the authentication of such devices without having to use our specialists?

The AleFIT MAB Keeper is an application that controls not only the access rights to individual modules and functions, but can also deal with access rights to a specific group of devices. So, if your printers are administered by an external company or a dedicated internal team of administrators, it is possible to allow them access to the AleFIT MAB Keeper. After logging in, the user can register a new MAC address in the system but only to the group for which the rights have been assigned – for example, only to the group for printers.

3) Is it possible to automatically disconnect a device from the network for which a temporary exception has been granted?

Yes, in fact this is one of the key features of the AleFIT MAB Keeper application. Unlike the Cisco ISE, the AleFIT MAB Keeper allows exception activation, i.e. authentication using the MAC address of the device for a specified time period after which the record automatically expires and is automatically removed. In the event that the cause of the problem cannot be solved in the meantime, subsequent authentication of the user or device will be unsuccessful.

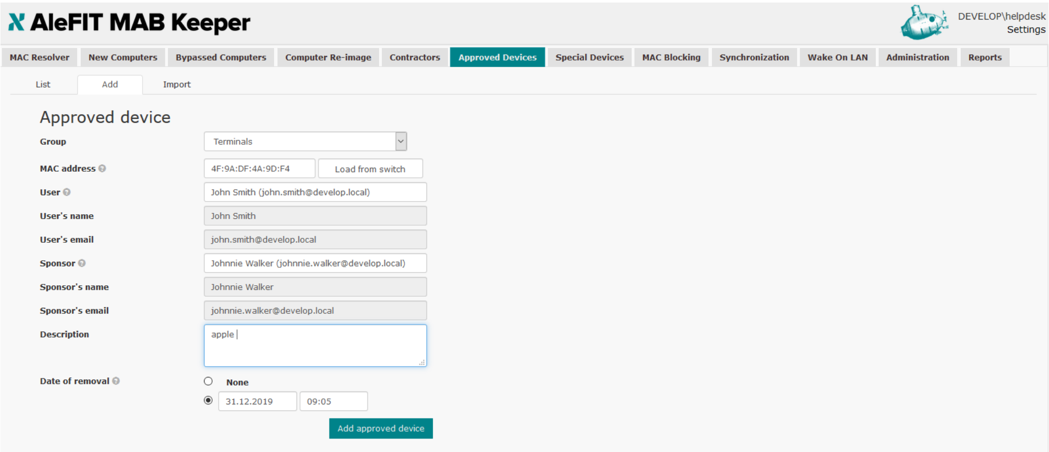
4) Is it possible to provide network access to our external suppliers?

This is another advantage of our solution. We are able to identify the rights of the sponsors and temporarily assign the same rights to their visitors by authenticating the MAC address of their laptops. Each sponsor is informed about the assignment of rights by email, which is sent automatically. Once the account expires, the access is automatically cancelled.

5) Is controlled access possible for a non-corporate workstation of a corporate user?

Yes, the AleFIT MAB Keeper makes it possible to establish short-term access for external suppliers as well as to provide long-term access for private workstations of internal employees. The AleFIT MAB Keeper allows these workstations, among other things, to register their MAC address and the date of access termination. Users are then authenticated via the 802.1x protocol and the MAC address of the workstation they use to log on is also verified. Network access is automatically cancelled on the date of expiration. The sponsor is informed of the assignment of rights by email.

5



Approved device

Group: Terminals
MAC address: 4F:9A:DF:4A:9D:F4
User: John Smith (john.smith@develop.local)
User's name: John Smith
User's email: john.smith@develop.local
Sponsor: Johnnie Walker (johnnie.walker@develop.local)
Sponsor's name: Johnnie Walker
Sponsor's email: johnnie.walker@develop.local
Description: apple
Date of removal: ○ None ● 31.12.2019 09:05

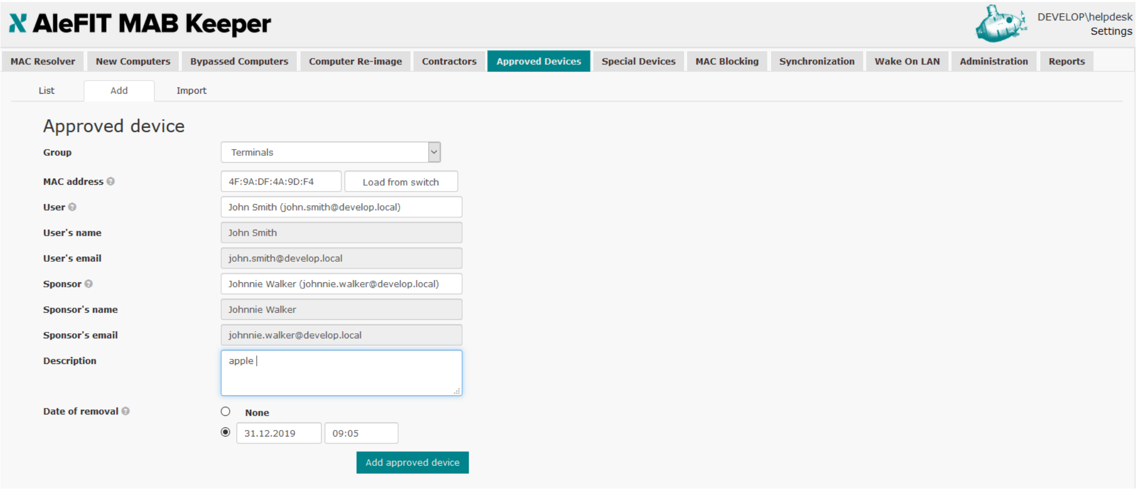
6) We are used to running updates at night. However, after deploying 802.1x, our existing solutions for remote wake-up on the LAN of workstations do not work. How can we solve this problem?

For these purposes, we provide remote wake-up via the WakeOnLAN function. The application identifies the VLAN in which the computer is located and wakes it up. This feature is accessible via the web interface and through the REST API when wake-up is performed from external applications.

7) What do I do if I need automatic installation of new workstations or so-called “reimaging” of workstations?

When installing or reinstalling an operating system, it is often necessary to have the required network resources – such as installation media, device drivers, installation files for additional applications or a previously prepared disc image – readily available. The installation process is automated and requires the workstation to be authenticated. With the utilities supplied with the AleFIT MAB Keeper, it is possible to modify the installation scripts in such a way as to automatically activate your computer's MAC address and authenticate it, thus providing the required network resources.

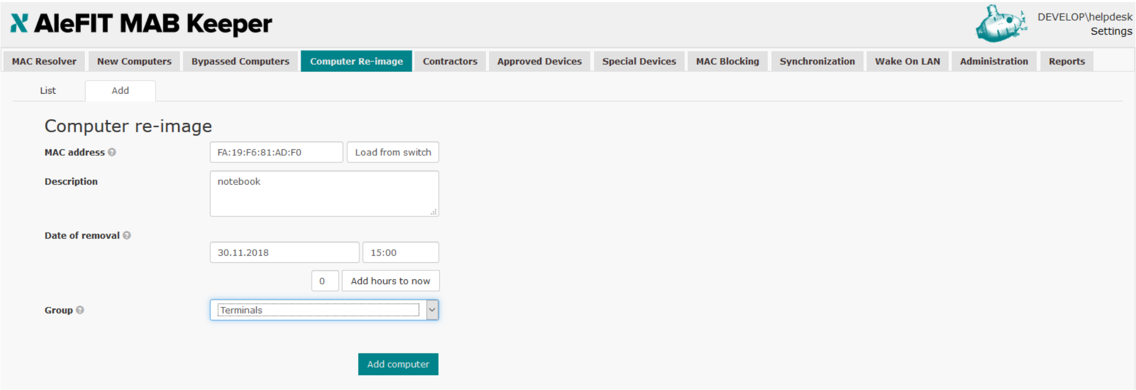
6



Approved device

Group: Terminals
MAC address: 4F:9A:DF:4A:9D:F4
User: John Smith (john.smith@develop.local)
User's name: John Smith
User's email: john.smith@develop.local
Sponsor: Johnnie Walker (johnnie.walker@develop.local)
Sponsor's name: Johnnie Walker
Sponsor's email: johnnie.walker@develop.local
Description: apple
Date of removal: ○ None ● 31.12.2019 09:05

7



Computer re-image

MAC address: FA:19:F6:81:AD:F0
Description: notebook
Date of removal: 30.11.2018 15:00
0 Add hours to now
Group: Terminals

8) We know the name of the computer or the user. Is it possible to find out where the user/device is connected to the network as well as the status of the authentication session?

The AleFIT Office Locator is able to automatically detect the end device (its MAC address and the network name) and based on this information, to provide information about the switch and port to which the device is connected. The application also records the history of events on that port. The application displays information concerning the status of the authentication session of the given device or user and allows the checking of the status of the device/user LDAP account. It further allows the display of the details of the authentication from the Cisco ISE or from the network switch.

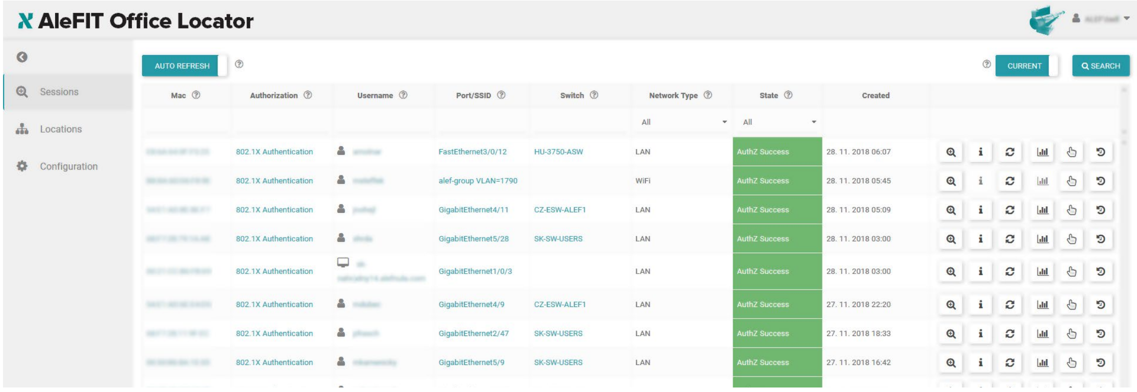
9) Is it possible to find out who registered a MAC address as well as when and why?

Yes, the AleFIT MAB Keeper enables you to view the records of actions that were performed using the application. The log clearly indicates the MAC addresses concerned, who performed the action and when, and whether it involved the granting of an exception, its cancellation or modification.

—

If you do not find the answers to your questions in this leaflet, please contact our sales representative who will provide you with the required information.

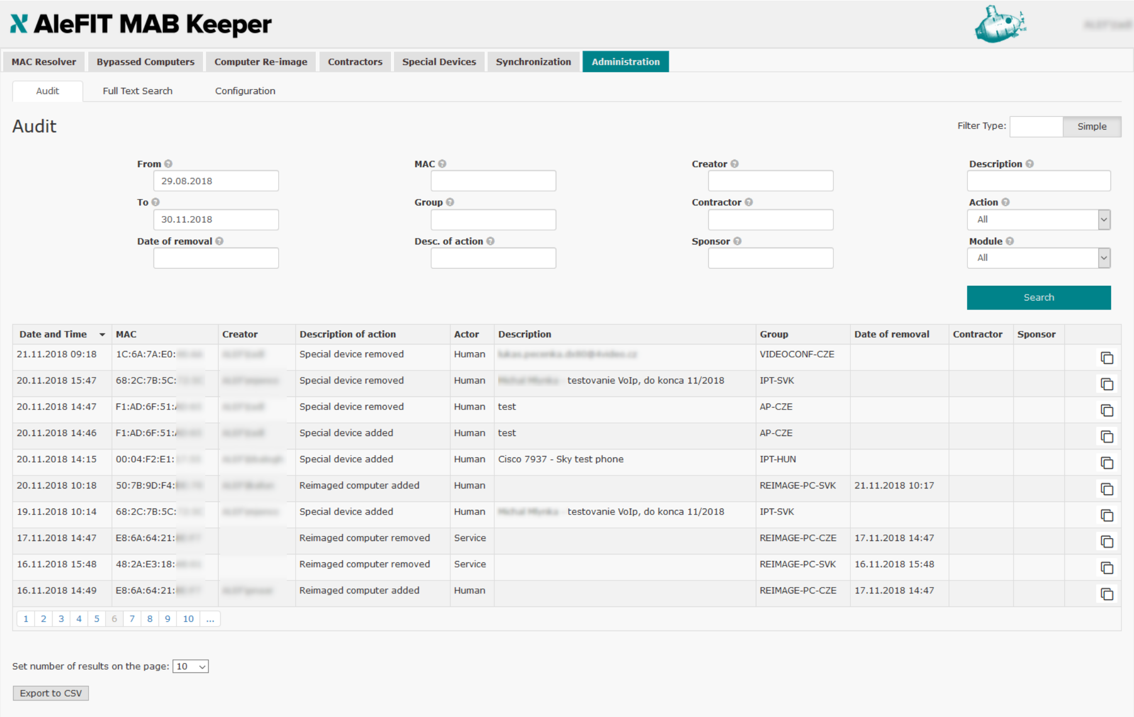
8



AleFIT Office Locator

Mac	Authorization	Username	Port/SSID	Switch	Network Type	State	Created
					All	All	
[redacted]	802.1X Authentication	[redacted]	FastEthernet3/0/12	HU-3750-ASW	LAN	AuthZ Success	28. 11. 2018 06:07
[redacted]	802.1X Authentication	[redacted]	alef-group VLAN=1790		WiFi	AuthZ Success	28. 11. 2018 05:45
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet4/11	CZ-ESW-ALEF1	LAN	AuthZ Success	28. 11. 2018 05:09
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet5/28	SK-SW-USERS	LAN	AuthZ Success	28. 11. 2018 03:00
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet1/0/3		LAN	AuthZ Success	28. 11. 2018 03:00
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet4/9	CZ-ESW-ALEF1	LAN	AuthZ Success	27. 11. 2018 22:20
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet2/47	SK-SW-USERS	LAN	AuthZ Success	27. 11. 2018 18:33
[redacted]	802.1X Authentication	[redacted]	GigabitEthernet5/9	SK-SW-USERS	LAN	AuthZ Success	27. 11. 2018 16:42

9



AleFIT MAB Keeper

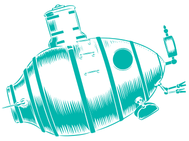
Audit

Filter Type: Simple

From: 29.08.2018
To: 30.11.2018
Date of removal:
MAC:
Group:
Desc. of action:
Creator:
Contractor:
Sponsor:
Description:
Action: All
Module: All

Date and Time	MAC	Creator	Description of action	Actor	Description	Group	Date of removal	Contractor	Sponsor
21.11.2018 09:18	1C:6A:7A:E0:[redacted]	[redacted]	Special device removed	Human	[redacted]	VIDEOCONF-CZE			
20.11.2018 15:47	68:2C:7B:5C:[redacted]	[redacted]	Special device removed	Human	[redacted] testovanie VoIp, do konca 11/2018	IPT-SVK			
20.11.2018 14:47	F1:AD:6F:51:[redacted]	[redacted]	Special device removed	Human	test	AP-CZE			
20.11.2018 14:46	F1:AD:6F:51:[redacted]	[redacted]	Special device added	Human	test	AP-CZE			
20.11.2018 14:15	00:04:F2:E1:[redacted]	[redacted]	Special device added	Human	Cisco 7937 - Sky test phone	IPT-HUN			
20.11.2018 10:18	50:7B:9D:F4:[redacted]	[redacted]	Reimaged computer added	Human		REIMAGE-PC-SVK	21.11.2018 10:17		
19.11.2018 10:14	68:2C:7B:5C:[redacted]	[redacted]	Special device added	Human	[redacted] testovanie VoIp, do konca 11/2018	IPT-SVK			
17.11.2018 14:47	E8:6A:64:21:[redacted]		Reimaged computer removed	Service		REIMAGE-PC-CZE	17.11.2018 14:47		
16.11.2018 15:48	48:2A:E3:18:[redacted]		Reimaged computer removed	Service		REIMAGE-PC-SVK	16.11.2018 15:48		
16.11.2018 14:49	E8:6A:64:21:[redacted]	[redacted]	Reimaged computer added	Human		REIMAGE-PC-CZE	17.11.2018 14:47		

Set number of results on the page: 10



Trust the Strong

ALEF NULA, a.s. | Pernerova 691/42, 186 00 Praha 8,
Česká republika | Phone: +420 225 090 240
cz-sales@alefnula.com | www.alefnula.com

CISCO Partner
Gold Certified