



dstny

Managed WiFi

for your company
and guests



What is Managed WiFi?

It is a managed wifi infrastructure service dedicated to companies who want to offer a user-friendly wifi access to their employees and guests without undergoing the maintenance constraints of such environment.

- Do you want to offer an easy to use wifi guest access?
- Do you want to quickly extend your wifi infrastructure to cover new offices/meeting rooms?
- Do you want to maximize the experience of users using voice or video conferencing over the wifi network?

Then, Managed Wi-Fi is a service which will fulfill your expectations. In the following chapters, we will see how Managed WiFi makes the life of the wifi infrastructure admins and users easier.





Why Managed Wi-Fi?

Because it will make the life of both your users and IT admins easier

The Managed Wi-Fi offer is based on Cisco Meraki wifi access points. This one is designed to maximize the user experience: optimizing the quality of commonly used applications (such as Microsoft Teams or Zoom) or making the delivery of wifi guest accounts easy.

It is also a co-managed service: your IT administrators can offload most of the wifi maintenance tasks to the Destiny team but can still implement some urgent changes if it can't wait for few hours.

Because an Access Point is not a switch

Network switches and wifi access points fulfill the same function: they provide a local network access to end-users. However, while switches are rarely the cause of problems, it is quite different with the wifi infrastructure. Radio frequencies are sensitive to interferences, wifi clients (laptops, tablets, smartphones) are fickle, building structures can block waves etc.

The goal of Managed Wi-Fi is to reduce the administration and maintenance costs. A service including incident handling. A technology minimizing the number of incidents and collecting all necessary troubleshooting data.



What value does Managed Wi-Fi offer your company?

A nice user experience

Managed Wi-Fi is based on the Cisco Meraki MR technology which natively supports radio channel optimization for critical traffic prioritization. In this way, quality sensitive applications such as Voice and Video conferencing work properly. Meraki MR also embeds a sponsored guest wifi mechanism which makes guest access management extremely simple.

Visibility

Our wifi infrastructure constantly monitors the wifi clients. We know what applications they

use, how much bandwidth they consume, when and why they are connected and disconnected, what is their radio signal strength etc. Not only do we obtain statistics on network usage, but we also collect all the data necessary to quickly diagnose end user problems.

Security

Our wifi access points comply with the latest security standards (WPA3, wifi6) and are not vulnerable to non-patchable native vulnerabilities of the wifi 5 standard (such as KRACK). In addition, these access points constantly scan the radio channels to detect rogue access points (hacker devices impersonating your APs) and unsecure end user connections. Last but not least, they also recognize unsecure devices (smartphones, tablets etc.) and isolate them from critical internal resources.



Co-management

Your problems are our problems! We offer you a full control on your wifi devices but we still take care of the change management and the incidents. Then, you combine the advantages of an outsourced service and a self-managed platform.

Flexibility

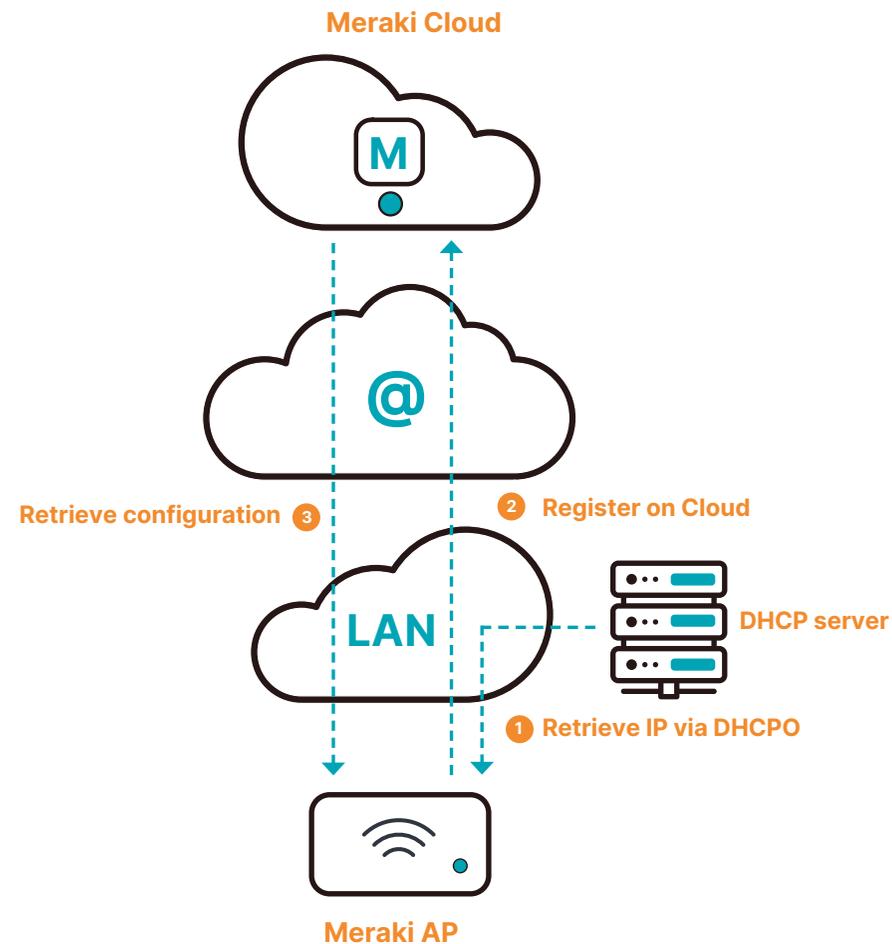
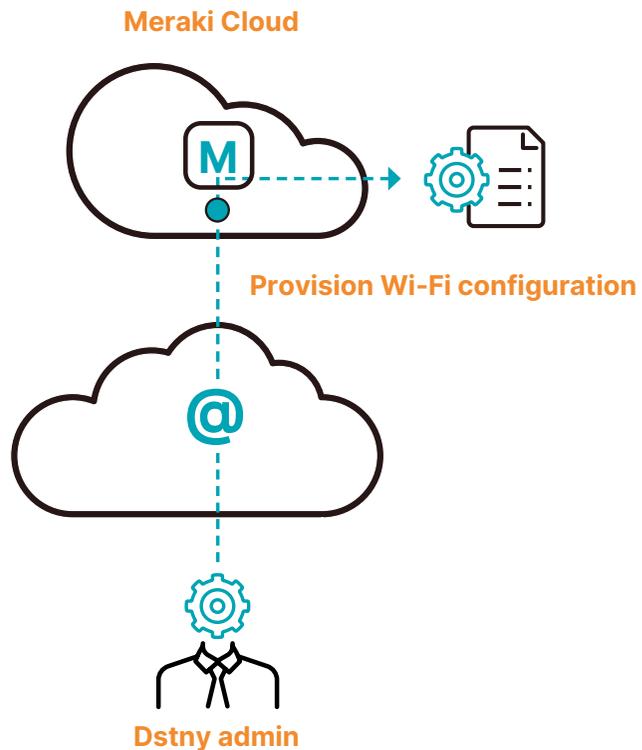
You can resize your architecture whenever you want. Need to cover a new office? Is it as easy as making a phone call! We ship devices on site (no need for pre-staging, this is a zero touch deployment technology), you connect them on the network and...that's all! Dstny charges you per month and per access point.



How does it work?

Central configuration

Dstny creates a central configuration on the Cisco Meraki cloud. We don't need to create one configuration scheme per access point. Instead, we create a configuration template which is applied everywhere. It simplifies the deployment of new parameters when these need to be applied globally.



Zero touch provisioning

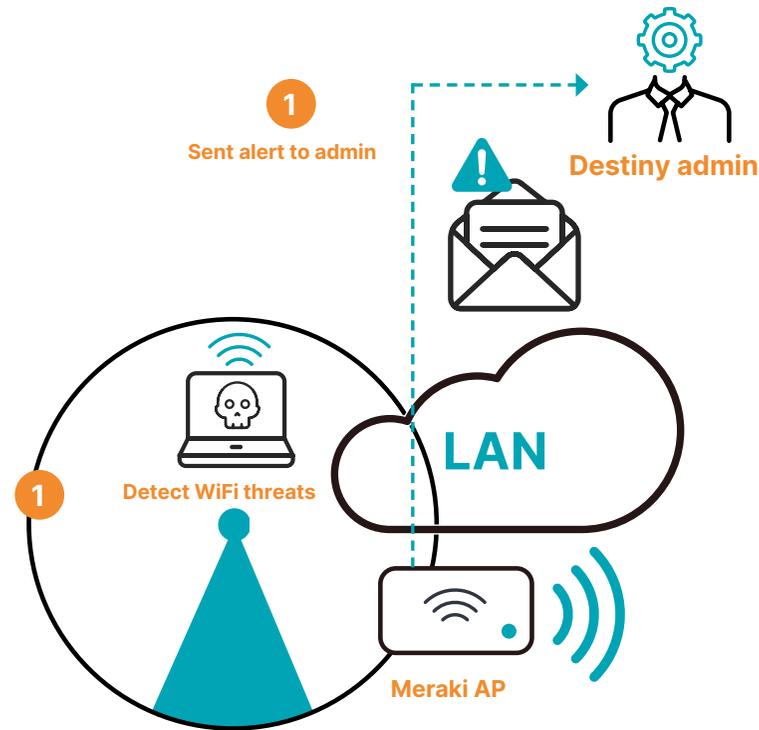
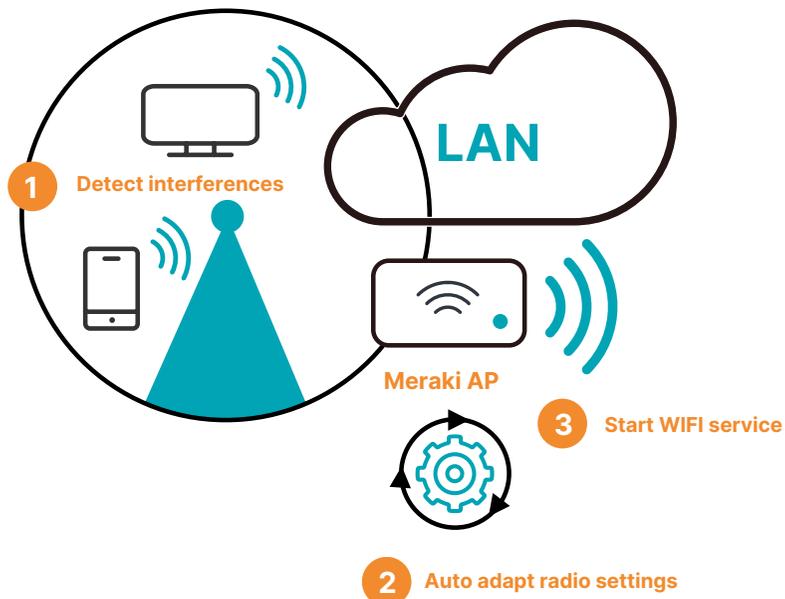
The access points are collected from our stock and sent to the sites. No staging phase is required. Once connected to the local network, the access point retrieves an IP via DHCP and connects to the Cisco Meraki Cloud to retrieve its configuration.



How does Managed Wi-Fi work?

Wireless access

Once the access point has configured itself, it starts to scan the wifi channels to discover other access points and potential interferences. The access point dynamically adapts its own frequency and cell size according to scan data. Finally, it starts to deploy the different SSIDs (the different wifi segments, corporate, guest etc.) according to the central configuration.



Air Marshal

All access points continuously monitor the radio frequencies to detect both interferences and attack attempts (such as a rogue AP). In case of a threat is detected, the AP immediately alerts the administrators.

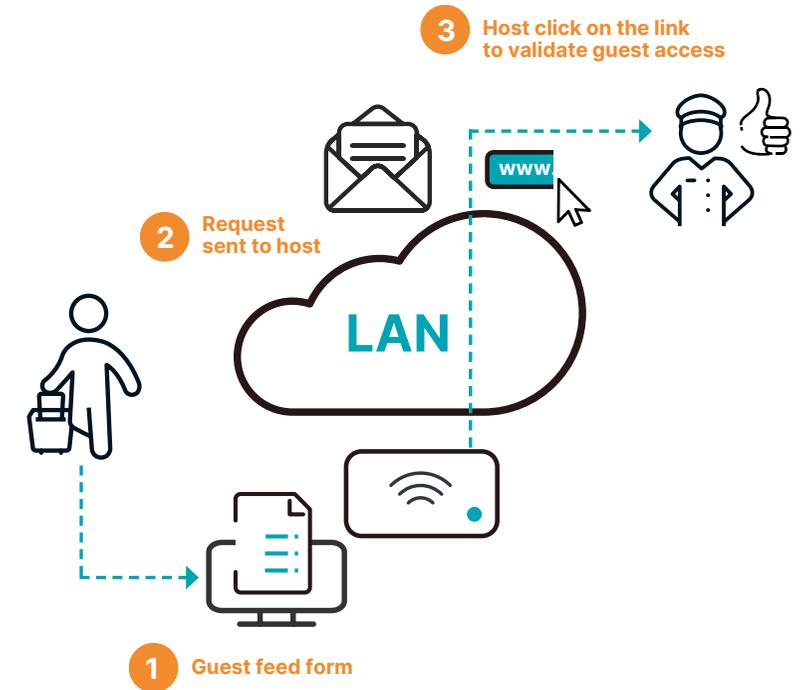




How does Managed Wi-Fi work?

Guest Access

Our wifi infrastructure natively embeds a guest access management system based on “sponsorship”. The potential guests are redirected on a WEB form and mention the email of their host. This one receives an email with a link and just need to click on it to create the guest account.



What does the Dstny service include?

Dstny both offers a Wireless infrastructure and a managed service:

- We take care of the initial configuration, we customize and secure it according to your needs.
- We take care of wifi configuration changes.
- We take over the change requests and the incidents.
- We offer you an access to the Cloud platform so you can co-manage it (if you want) and read the wifi activity reports.

Wifi Standards wifi-6 (802.3ax), 2,4 and 5 GHz bands, WPA3

Alimentation PoE/802.3af compatible (PoE switch is not included in our offer)

Specific features L7 (application layer) traffic optimization, wifi guest sponsorship, mobile device security (tablets smartphones), network (L7 and L3) usage reporting

Contact us

T +32 (0)2 401 97 00

F +32 (0)2 401 97 44

E-mail sales@dstny.be

Destiny NV/SA

Excelsiorlaan 89

1930 Zaventem

dstny